CONTRIBUTIONS TO THE ESSENTIAL DIMENSION OF FINITE AND ALGEBRAIC GROUPS

Inauguraldissertation

zur

Erlangung der Würde eines Doktors der Philosophie

vorgelegt der

Philosophisch-Naturwissenschaftlichen Fakultät
der Universität Basel

von

Roland Lötscher

aus

Ruswil LU

Basel, 2010

genehmigt von der Philosophisch-Naturwissenschaftlichen Fakultät
auf Antrag von

Prof. Dr. H. Kraft

Prof. Dr. Z. Reichstein

Basel, den 30. März 2010

Prof. Dr. E. Parlow, Dekan

creative commons

Namensnennung-Keine kommerzielle Nutzung-Keine Bearbeitung 2.5 Schweiz

---

Sie dürfen:

das Werk vervielfältigen, verbreiten und öffentlich zugänglich machen

Zu den folgenden Bedingungen:

Namensnennung. Sie müssen den Namen des Autors/Rechteinhabers in der von ihm festgelegten Weise nennen (wodurch aber nicht der Eindruck entstehen darf, Sie oder die Nutzung des Werkes durch Sie würden entlohnt).

Keine kommerzielle Nutzung. Dieses Werk darf nicht für kommerzielle Zwecke verwendet werden.

Keine Bearbeitung. Dieses Werk darf nicht bearbeitet oder in anderer Weise verändert werden.

- Im Falle einer Verbreitung müssen Sie anderen die Lizenzbedingungen, unter welche dieses Werk fällt, mitteilen. Am Einfachsten ist es, einen Link auf diese Seite einzubinden.
- Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.
- Diese Lizenz lässt die Urheberpersönlichkeitsrechte unberührt.

Quelle: http://creativecommons.org/licenses/by-nc-nd/2.5/ch/ Datum: 3.4.2009

Contents

Overview

Essential dimension, introduced by Joe Buhler and Zinovy Reichstein and in its most general form by Alexander Merkurjev, is a measure of complexity of algebraic structures such as quadratic forms, hermitian forms, central simple algebras, étale algebras etc. which are defined over fields. Informally, the essential dimension of an algebraic structure is the number of parameters needed to define its objects up to isomorphism. The objects of algebraic structures are often classified by cohomology sets $H^1(K, G)$ (with respect to the fppf topology) of an algebraic group G. The set $H^1(K, G)$ can be seen as the set of isomorphy classes of G-torsors over K. The essential dimension of G-torsors (called essential dimension of G) gives an invariant of algebraic groups, which will be of primary interest in this thesis.

The text is subdivided into four chapters as follows:

Chapter I+II: Multihomogenization of covariants and its application to covariant and essential dimension
The essential dimension of a linear algebraic group G can be expressed via G-equivariant rational maps $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$, so called covariants, between generically free G-modules V and W. In these two chapters we explore a new technique for dealing with covariants, called multihomogenization. This technique was jointly introduced with Hanspeter Kraft and Gerald Schwarz in an already published paper [**KLS**], which forms the second chapter.

Applications of the multihomogenization technique to the essential dimension of algebraic groups are given by results on the essential dimension of central extensions, direct products, subgroups and the precise relation of essential dimension and covariant dimension (which is a variant of the former with polynomial covariants). Moreover the multihomogenization technique allows one to extend a twisting construction introduced by Matthieu Florence from the case of irreducible representations to completely reducible representations. This relates Florence's work on the essential dimension of cyclic p-groups to recent stack theoretic approaches by Patrick Brosnan, Angelo Vistoli and Zinovy Reichstein and Nikita Karpenko and Alexander Mekurjev.

A portion of the first chapter is accepted for publication in Transformation groups [**L2**]. An earlier and larger version with the same title is published on Arxiv [**L1**].

Chapter III: Faithful and p-faithful representations of minimal dimension
The study of essential dimension of finite and algebraic groups is closely related to the study of its faithful resp. generically free representations. In general the essential dimension of an algebraic group is bounded above by the least dimension of a generically free representation minus the dimension of the algebraic group. In some prominent cases this upper bound or a variant of it is strict.

In this chapter we are guided by the following general questions: What do faithful representations of the least possible dimension look like? How can they be constructed? How are they related to faithful representations of minimal dimension of subgroups?

In particular we investigate representations of an extension G of a p-group by a torus (over an algebraically closed field). We will show that such an algebraic group G has a finite p-subgroup F such that the least dimension of a representation of G with kernel finite and of order prime to p is equal to the least dimension of a faithful representation of

F. This result has been established in a combined effort with Zinovy Reichstein and Mark MacDonald.

Along the way we also compute the minimal number of irreducible representations needed to construct a faithful representation and therewith generalize a classical theorem of Wolfgang Gaschütz (*Endliche Gruppen mit treuen absolut-irreduziblen Darstellungen*, Math. Nachr. **12** (1954), 253-255).

Chapter IV: Essential p-dimension of algebraic tori
This chapter is joint work with Mark MacDonald, Aurel Meyer and Zinovy Reichstein and is submitted for publication [**LMMR**]. We study a variant of essential dimension which is relative to a prime number p. This variant, called essential p-dimension, disregards effects resulting from other primes than p. In a recent paper Nikita Karpenko and Alexander Merkurjev have computed the essential dimension of p-groups. We extend their result and find the essential p-dimension for a class of algebraic groups, which includes all algebraic tori and twisted finite p-groups.

Acknowledgments

I would like to thank my adviser Hanspeter Kraft for introducing me to the subject of covariant and essential dimension and for guiding me during my thesis. He carefully read this manuscript and several preprints for publication. I wish to thank him for his tremendous support and for sharing his insights both into the mathematical and non-mathematical world. While I was away in Vancouver for one month he took over my duties as a teaching assistant. Thanks a lot!

Many thanks go to Zinovy Reichstein from whom I learnt a lot about essential dimension and who agreed to referee this thesis. He greatly helped me to organize my stay in Vancouver and to reach the frontiers of the research in essential dimension. I would also like to thank the hosting math department of the University of British Columbia and to Kay Behrend, who allowed me to use his office during my stay in Vancouver.

During my thesis I received financial support from a Schweizer Nationalfonds grant. My stay in Vancouver was funded by the Freie Akademische Gesellschaft (FAG) of Basel.

It was a great pleasure to collaborate with Gerald Schwarz and Hanspeter Kraft and with Aurel Meyer, Mark MacDonald and Zinovy Reichstein. I found it very motivating to do mathematics together, be it at the blackboard or via email. Special thanks go to Aurel, with whom I had lots of useful discussions ever since.

I enjoyed to take part in two conferences related to essential dimension, one in Lens in 2008, the other in Banff in 2009. I want to thank the organisers for inviting me and taking care of everything. Moreover I am grateful for useful conversations with some of the participants, especially with Grégory Berhuy, Alexander Merkurjev and Alexander Duncan.

Many thanks go to all my colleagues from Basel with whom I had a great time. Especially I want to thank Giordano Favi, Jonas Budmiger, Immanuel Stampfli, Christian Graf, Martin Widmer and Philippe Habegger for stimulating mathematical discussions and problem solving.

Finally, I wish to thank my parents and to my wife Lauryna for their great confidence in me and for the wonderful time spent together.

List of publications in peer-reviewed journals and on arxiv.org including material of this thesis

[KLS] H. Kraft, R. Lötscher, G. Schwarz: *Compression of finite group actions and covariant dimension, II*, J.Algebra **322**(1) (2009), 94–107.

[L1] R. Lötscher: *Application of multihomogeneous covariants to the essential dimension of finite groups*, Arxiv:0811.3852 (2008).

[L2] R. Lötscher: *Application of multihomogeneous covariants to the essential dimension of finite groups*, (2009), accepted for publication in Transform. Groups.

[LMMR] R. Lötscher, M. MacDonald, A. Meyer, Z. Reichstein: *Essential p-dimension of algebraic tori* (2009), Arxiv:0910.5574.

CHAPTER I

Multihomogeneous covariants and the essential dimension of algebraic groups

1. Preliminaries

The purpose of this section is to introduce terminology, notation and recall several equivalent definitions of essential dimension that will be used in the sequel.

Throughout this chapter we work over a base field k which will be assumed to be infinite for simplicity. Unadorned tensor products will be taken over k. Sometimes we will extend scalars to a larger field K/k. We will denote by $\bar{k}$ (resp. $k_{\text{sep}} \subseteq \bar{k}$) an algebraic (resp. separable) closure of k. All vector spaces and representations in consideration are finite dimensional over the base field. All schemes in consideration will be of finite type over the base field. We reserve the word *variety* for a geometrically integral separated scheme defined over the base field. We define *algebraic group* to be an affine group scheme over the base field. A G-module is a vector space V endowed with a morphism $G \to \mathrm{GL}(V)$ of algebraic groups. A *G-variety* for an algebraic group G is a variety X with a regular algebraic G-action $G \times X \to X, x \mapsto gx$ on it. Rational and regular maps between varieties will always be defined over the base field. Finite groups will be considered as constant algebraic groups over k. We will write *finite algebraic group* for a finite but not necessarily constant algebraic group. An *étale algebraic group* is a smooth finite algebraic group.

The *essential dimension of G* was originally introduced by Buhler and Reichstein [**BR97, Re00**] (for k of characteristic 0, assumed to be algebraically closed in the second reference) in terms of *compressions* of generically free varieties: A G-variety X is called *generically free* if there exists a G-invariant dense open subscheme U of X such that the (scheme theoretic) stabilizer in G of every point $x \in U(\bar{k})$ is trivial. A G-module V is called generically free if the variety $\mathbb{A}(V)$ representing the functor $A \mapsto V \otimes A$ from commutative k-algebras to sets is generically free. A *compression* of a generically free G-variety Y is a dominant G-equivariant rational map $\varphi\colon Y \dashrightarrow X$, where X is another generically free G-variety. The *essential dimension of G* is then defined as the minimal value of $\dim X - \dim G$ taken over all compressions $\varphi\colon \mathbb{A}(V) \dashrightarrow X$ of a generically free G-module V.

Later the essential dimension of G was reformulated by Merkurjev [**BF03, Me09**] in the more general setting of algebraic groups G over arbitrary fields in terms of fields of definition of G-torsors: A *G-torsor* (over a scheme Y) is a scheme X with a right action by G and a G-invariant morphism $X \to Y$ such that locally on X in the finitely presented faithfully flat (fppf) topology X is G-equivariantly isomorphic to $Y \times G$ (cf. [**BF03**, Definition 4.5]). The essential dimension of G is the least transcendence degree of a field of definition of a *generic G-torsor* (see [**BF03**, Definition 6.3]).

We mainly take the following point of view: A *covariant* of G is a G-equivariant rational map $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$, where V and W are G-modules. The covariant φ is

called *faithful* the image closure $\overline{\varphi(\mathbb{A}(V))}$ is a faithful G-variety. The covariant φ is called *generically free* if its image closure is a generically free G-variety. We denote by $\dim\varphi$ the dimension of the closure of the image of φ. In terms of covariants the essential dimension can be defined as the minimal value of $\dim\varphi - \dim G$ taken over all generically free covariants φ of G.

These three notions of essential dimension are shown to be equivalent in the following lemma, which is a variant of [**Fl08**, Proposition 2.5]. For its formulation we need the notion of a friendly open subset $U \subseteq X$, whose existence for every generically free G-variety X is provided by a result of Gabriel (see [**BF03**, Theorem 4.7 and Definition 4.8]).

DEFINITION 1.1. A *friendly open subset* of a generically free G-variety X is a G-invariant dense open subvariety $U \subseteq X$ which is the total space of a G-torsor $U \to Y$.

LEMMA 1.2. *Let V and W be generically free G-modules. Let $U \subseteq \mathbb{A}(V)$ be a friendly open subset and T be the G-torsor over $k(Y)$ given by the generic fiber of a torsor $U \to Y$. The following values coincide:*

- $e_1 := \min\{\dim\varphi - \dim G \mid \varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ *generically free covariant of* $G\}$.
- $e_2 := \min\{\dim X - \dim G \mid$ *there exists a compression* $\mathbb{A}(V) \dashrightarrow X\}$.
- $e_3 := \min\{\operatorname{trdeg}_k K \mid K$ *a field of definition of* $T\}$.

PROOF. Clearly $e_2 \leq e_1$ since a generically free covariant $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ induces a compression $\mathbb{A}(V) \dashrightarrow X := \overline{\varphi(\mathbb{A}(V))}$.

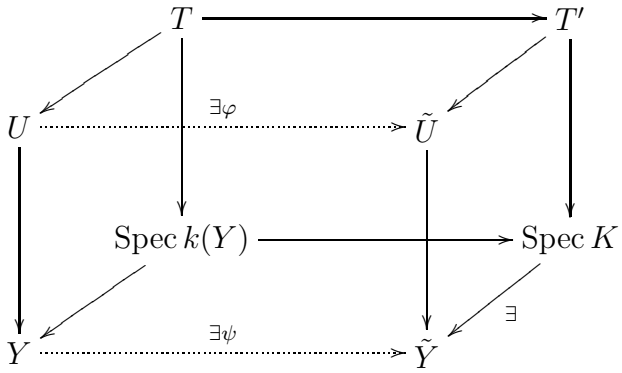
In the next step we show $e_3 \leq e_2$. Let $\varphi\colon \mathbb{A}(V) \dashrightarrow X$ be a compression with $e_2 = \dim X - \dim G$. Let $U' \subseteq X$ be a friendly open subset and T' be the generic fiber of a torsor $U' \to Y'$. We consider φ as a rational map $U \dashrightarrow U'$. We get an induced rational map $Y \dashrightarrow Y'$ making the diagram

$$\begin{array}{ccc} U & \dashrightarrow & U' \\ \downarrow & & \downarrow \\ Y & \dashrightarrow & Y' \end{array}$$

commute. This implies that the torsor T is obtained from T' by pull back (cf. [**BF03**, Lemma 6.11]). Hence $e_3 \leq \operatorname{trdeg}_k k(Y') = \dim X - \dim G = e_2$.

It remains to show $e_1 \leq e_3$. Let $\tilde{U} \subseteq \mathbb{A}(W)$ be a friendly open subset and let $\tilde{U} \to \tilde{Y}$ be a G-torsor. This torsor is *versal* for G (see [**BF03**, Definition 6.1, Remark 6.2] for the case G is smooth or [**Me09**, Theorem 4.1] for the general case). Hence any G-torsor T' over an infinite field K is the pullback of $\tilde{U} \to \tilde{Y}$ by a K-rational point $\operatorname{Spec} K \to \tilde{Y}$ of $\tilde{Y}$. Now choose for T' a G-torsor over a subfield $K \subseteq k(Y)$ of transcendence degree $\operatorname{trdeg}_k K = e_3$ such that T is obtained from T' by scalar extension to $k(Y)$ (note that K is infinite as required, since we assume k to be infinite). This implies the existence of a G-equivariant rational map $\varphi\colon U \dashrightarrow \tilde{U}$ and a rational map $\psi\colon Y \to \tilde{Y}$ completing a

commutative cube (cf. [**BF03**, Lemma 6.11]):



Moreover we may consider φ as a generically free covariant $\mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ with $e_1 \leq \dim \varphi - \dim G \leq \operatorname{trdeg}_k K = e_3$. □

Remark 1.3. The statement of Lemma 1.2 also holds over a finite field k as long as $e_3 > 0$, which is equivalent to G not being special [**Me09**, Proposition 4.4]. An algebraic group is called *special* if G has no non-trivial torsors over any field extensions of k. For example $G = \mathrm{GL}_n$ is special and for $V = W = M_n$ the space of $n \times n$ square matrices with left multiplication of G the values $e_1 = e_2 = e_3$ are equal.

The statement holds in particular for finite algebraic groups (the only special finite algebraic group is the trivial group, but in that case $e_1 = e_2 = e_3 = 0$ are equal as well). Hence as long as we only consider essential dimensions of finite algebraic groups we might as well drop the assumption on k being infinite. The only other place where we need k to be infinite is in section 10 and in Remark 6.3 where the essential dimension of elementary abelian p-groups is considered.

Definition 1.4. We denote by $\operatorname{ed}_k G$ the common value $e_1 = e_2 = e_3$ from Lemma 1.2 and call it the *essential dimension of* G.

Remark 1.5. Note that our definition of essential dimension differs from [**BF03**, Definition 2.1], which uses Galois cohomology (or, equivalently, torsors in the étale topology). The two definitions become equivalent, however, if G is smooth (cf. [**BF03**, Corollary 6.16]). The definition we use appears in more recent articles on essential dimension [**BS08, Me09, TV10**].

The value e_3 from Lemma 1.2 depends neither on the choice of a generically free G-module V [**BF03**] nor on the choice of a generically free G-module W. This has the following consequence:

Lemma 1.6. *For any generically free G-modules V and W there exists a generically free covariant $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ such that $\dim \varphi = \operatorname{ed}_k G + \dim G$.*

2. Introduction

In this chapter we will develop a multihomogenization technique for covariants and invariants of algebraic groups and give applications thereof to the essential dimension

of algebraic groups G. Given G-stable gradings $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$ of generically free G-modules V and W a covariant $\varphi = (\varphi_1, \dots, \varphi_n)\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ is called multihomogeneous if the identities

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

hold true for all i, j and suitable m_{ij}. Here s is an indeterminate and the m_{ij} are integers, forming some matrix $M_\varphi \in \mathrm{Mat}_{m\times n}(\mathbb{Z})$. Thus multihomogeneous covariants generalize homogeneous covariants. A whole matrix of integers takes on 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 5.2 states that if each V_i and W_j is irreducible then the rank of the matrix M_φ is bounded from below by the rank of the largest central diagonalizable subgroup $Z(G, k)$ (the k-center, see Definition 4.4). Moreover if the rank of M_φ exceeds the rank of $Z(G, k)$ by $\Delta \in \mathbb{N}$ then $\mathrm{ed}_k G \leq \dim \varphi - \Delta$. This observation will be useful for several application, in particular for proving upper bounds to $\mathrm{ed}_k G$.

The rest of this chapter is structured as follows. In sections 3, 4 and 5 we give the construction of multihomogenization and derive its basic properties. Then we proceed to applications. Section 6 relates essential dimension with the so called covariant dimension $\mathrm{cdim}_k G$ of étale algebraic groups G, which is an analogue of essential dimension with covariants assumed to be regular. It is well known that the two differ at most by 1 (for a proof see [**Re04**]). We obtain the precise relationship between covariant and essential dimension in case that G has a completely reducible faithful representation. Namely Theorem 6.2 says that $\mathrm{cdim}_k G = \mathrm{ed}_k G$ if and only if G (is trivial or) has a nontrivial k-center, otherwise $\mathrm{cdim}_k G = \mathrm{ed}_k G + 1$.

In section 7 a generalization of a result from [**BR97**] about central extensions is obtained. For a finite group G and a central cyclic subgroup H which intersects the commutator subgroup $[G, G]$ of G trivially Buhler and Reichstein deduced the relation

$$\mathrm{ed}_k G = \mathrm{ed}_k G/H + 1$$

(over a field k of characteristic 0) under some further assumptions on H [**BR97**, Theorem 5.3]. We give a complete generalization for étale algebraic groups given by the identity

$$\mathrm{ed}_k G = \mathrm{ed}_k G/H + \mathrm{rank}\, Z(G, k) - \mathrm{rank}\, Z(G, k)/H,$$

where we only assume that G/H has a completely reducible faithful representation and that H embeds into a diagonalizable direct factor of $G/[G, G]$. For details see Theorem 7.1.

Section 8 contains two results about the essential dimension of subgroups and direct products, both obtained easily with the use of multihomogeneous covariants.

In section 9 we will use multihomogeneous covariants to generalize Florence's twisting construction from [**Fl08**]. This generalization gives a substitute to the use of algebraic stacks in the proof of the theorem of Karpenko and Merkurjev about the essential dimension of p-groups and previous work by Brosnan, Reichstein and Vistoli [**BRV07, BRV08**]. The twisting construction relates the essential dimension of G with generic splitting fields of certain central simple algebras. For a class of algebraic groups G which includes finite p-groups, this relation will be exploited to give a precise formula for the essential dimension of G.

In section 10 we consider the situation when a finite group G does not admit a faithful completely reducible representation. That can only happen if $\operatorname{char} k = p > 0$ and G contains a nontrivial normal elementary abelian p-subgroup A. Proposition 10.1 relates the essential dimension of G and G/A by $\operatorname{ed}_k G/A \leq \operatorname{ed}_k G \leq \operatorname{ed}_k G/A + 1$ when A is central.

3. The multihomogenization technique

3.1. Multihomogeneous maps and multihomogenization. Multihomogenization has been introduced in [**KLS09**] (see Chapter II) for covariants of finite groups over $\mathbb{C}$. We give a more direct and general approach here.

Denote by $X = \operatorname{Hom}_k(*, \mathbb{G}_{\mathbf{m}})$ the contravariant functor from the category of diagonalizable algebraic groups (over k) to the category of abelian groups, which takes a diagonalizable algebraic group G to the set $X(G) = \operatorname{Hom}_k(G, \mathbb{G}_{\mathbf{m}})$ of characters defined over k. For example $X(T) = \mathbb{Z}^r$ if $T = \mathbb{G}_{\mathbf{m}}^r$ is a split torus of rank $r = \dim T$. In particular $X(\mathbb{G}_{\mathbf{m}}) = \mathbb{Z}$.

Let $T = \mathbb{G}_{\mathbf{m}}^m$ and $T' = \mathbb{G}_{\mathbf{m}}^n$ be split tori. The homomorphisms $D \in \operatorname{Hom}_k(T, T')$ defined over k correspond to linear maps $X(D)\colon X(T') \to X(T)$ and to matrices $M_D \in \operatorname{Mat}_{m\times n}(\mathbb{Z})$ under the canonical isomorphisms

$$\operatorname{Hom}_k(T, T') \cong \operatorname{Hom}(X(T'), X(T)) = \operatorname{Hom}(\mathbb{Z}^n, \mathbb{Z}^m) \cong \operatorname{Mat}_{m\times n}(\mathbb{Z})$$

In terms of the matrix $M_D = (m_{ij})_{1\leq i\leq m, 1\leq j\leq n}$ the homomorphism D is then given by

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

The above isomorphisms are compatible with composition of homomorphisms $D \in \operatorname{Hom}_k(T, T'), D' \in \operatorname{Hom}_k(T', T'')$ on one hand and multiplication of matrices $M \in \operatorname{Mat}_{m\times n}(\mathbb{Z})$, $M' \in \operatorname{Mat}_{n,r}(\mathbb{Z})$ on the other hand (where $T'' := \mathbb{G}_{\mathbf{m}}^r$ is another split torus). That means that $M_{D'\circ D} = M_D \cdot M_{D'}$.

Let V be a graded vector space, $V = \bigoplus_{i=1}^m V_i$. We associate with V the torus $T_V \subseteq \operatorname{GL}(V)$ consisting of those linear automorphisms which act by multiplication of scalars on each V_i. We identify T_V with $\mathbb{G}_{\mathbf{m}}^m$ 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 $T_W \subseteq \operatorname{GL}(W)$ its associated torus.

Definition 3.1. 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 $M \in \operatorname{Mat}_{m,n}(\mathbb{Z})$ if

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

for all i and j.

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

$$\begin{array}{ccc} T_V \times \mathbb{A}(V) & \xrightarrow{(t,v)\mapsto tv} & \mathbb{A}(V) \\ \downarrow{\scriptstyle D\times\varphi} & & \downarrow{\scriptstyle \varphi} \\ T_W \times \mathbb{A}(W) & \xrightarrow{(t',w)\mapsto t'w} & \mathbb{A}(W) \end{array} \tag{2}$$

commutes.

Example 3.2. Let $V = \bigoplus_{i=1}^m V_i$ be a graded vector space. If $h_{ij} \in k(V_i)^*$ for $1 \le i, j \le m$ are homogeneous rational functions of degree $r_{ij} \in \mathbb{Z}$ then the map

$$\psi_h \colon \mathbb{A}(V) \to \mathbb{A}(V), \quad v \mapsto (h_{11}(v_1)\dots h_{m1}(v_m)v_1, \dots, h_{1m}(v_1)\dots h_{mm}(v_m)v_m)$$

is multihomogeneous with degree matrix equal to $M = (r_{ij} + \delta_{ij})_{1\le i,j\le m}$, where δ_{ij} is the Kronecker delta.

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 $D \in \mathrm{Hom}_k(T_V, T_W)$ is uniquely determined by condition (2). We shall write D_φ, X_φ and M_φ for D, $X(D)$ and M_D, respectively. If $\varphi_j = 0$ for some j then the matrix entries m_{ij} of M_φ, for $i = 1, \cdots, m$, do not give any information. For simplicity we will always assume that all components φ_j are nonzero. There are various ways for dealing with zero components φ_j. For example one can make the convention $m_{ij} = 0$ for such j and each i. Then all results in this chapter go through, but some of the proofs would become more technical.

Given an arbitrary rational map $\varphi \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ we produce 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 $\lambda \in \mathrm{Hom}_k(\mathbb{G}_\mathbf{m}, T_V)$. In section 5 this procedure will be applied to covariants for a group G.

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 $f = \frac{p}{q}$ with polynomials p, q where $s \nmid q$. For such f we define $\lim f \in k(V)$ by $(\lim f)(v) = \frac{p(v,0)}{q(v,0)}$. 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 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 $\psi = (f_1, \dots, f_d)$ where $d = \dim W$ and $f_1, \dots, f_d \in O_s$ we shall write $\lim \psi$ for the rational map $(\lim f_1, \dots, \lim f_d) \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$.

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

$$\tilde{\varphi} \colon \mathbb{A}(V) \times \mathbb{G}_\mathbf{m} \dashrightarrow \mathbb{A}(W), \quad (v, s) \mapsto \varphi(\lambda(s)v)$$

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

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

The limit $H_\lambda(\varphi) = (H_\lambda(\varphi)_1, \dots, H_\lambda(\varphi)_n)$ depends only on φ and the choice of λ. By construction and since we assume $\varphi_j \neq 0$ for all j we have $(H_\lambda(\varphi))_j \neq 0$ for all j as well.

Our construction enjoys the following property:

LEMMA 3.3. *For any one-parameter subgroup $\lambda \in \mathrm{Hom}_k(\mathbb{G}_{\boldsymbol{m}}, T_V)$ we have*

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

PROOF. Choose a basis in each W_j and take their union for a basis of W. Let $d = \dim W$ and write $\varphi = (f_1, \dots, f_d)$ with respect to the chosen basis, where $f_j \in k(V)$. Then $H_\lambda(\varphi)$ is of the form $(\lim \hat{f}_1, \dots, \lim \hat{f}_d)$ where each $\hat{f}_j \in O_s \subset k(V \times k)$ is given by

$$\hat{f}_j(v, s) = s^{\gamma_j} f_j(\lambda(s)v)$$

for some $\gamma_j \in \mathbb{Z}$. Choose a maximal subset $S = \{j_1, \dots, j_l\}$ of $\{1, \dots, d\}$ with the property that $\lim \hat{f}_{j_1}, \dots, \lim \hat{f}_{j_l}$ are algebraically independent. It suffices to show that $f_{j_1}, \dots, f_{j_l}$ are then algebraically independent, too. Without loss of generality $j_1 = 1, \dots, j_l = l$.

Assume that $f_1, \dots, f_l$ are algebraically dependent. Let $p \in k[x_1, \dots, x_l] \setminus \{0\}$ with $p(f_1, \dots, f_l) = 0$. Since the algebraic independence implies $\lim \hat{f}_j \neq 0$ for $j = 1 \dots l$ we have $\nu(\hat{f}_j) = 0$. Set $\gamma = (\gamma_1, \dots, \gamma_l)$ and write p in the form

$$p = \sum_{i \in \mathbb{Z}} p_i \quad \text{where} \quad p_i = \sum_{\beta \in \mathbb{N}^l \colon \beta \cdot \gamma = -i} c_\beta x_1^{\beta_1} \cdots x_l^{\beta_l}.$$

Let $d = \min\{i \in \mathbb{Z} \mid \exists \beta \in \mathbb{N}^l \colon \beta \cdot \gamma = -i, c_\beta \neq 0\}$. That implies $p_d \neq 0$. For $j = 1 \dots l$ there exists $\delta_j \in O_s \subset k(V \times k)$ such that $\hat{f}_j - \lim \hat{f}_j = s\delta_j$. By construction,

$$\begin{aligned} 0 &= s^{-d} p(f_1, \dots, f_l)(\lambda(s)v) = s^{-d} p(s^{-\gamma_1} \hat{f}_1, \dots, s^{-\gamma_l} \hat{f}_l)(v) \\ &= s^{-d} p\big(s^{-\gamma_1}(\lim \hat{f}_1 + s\delta_1), \dots, s^{-\gamma_l}(\lim \hat{f}_l + s\delta_l)\big)(v) \\ &= p_d\big(\lim \hat{f}_1, \dots, \lim \hat{f}_l\big)(v) + sh(v, s), \end{aligned}$$

where $h \in O_s$. Taking the limit shows $p_d\big(\lim \hat{f}_1, \dots, \lim \hat{f}_l\big) = 0$, which concludes the proof. □

It is quite immediate that $H_\lambda(\varphi)$ is equivariant with respect to the homomorphism of tori $\lambda(\mathbb{G}_{\mathbf{m}}) \to \lambda'(\mathbb{G}_{\mathbf{m}})$ which sends $\lambda(s)$ to $\lambda'(s^{-1})$. However, to get equivariance for the full tori T_V and T_W (i.e., such that $H_\lambda(\varphi)$ is multihomogeneous) we have to choose the one-parameter subgroup λ carefully.

Write φ in the form $\varphi = \frac{1}{f}(\psi_1, \dots, \psi_n)$ where each $\psi_j \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W_j)$ is regular and $f \in k[V]$. The space $\mathrm{Mor}(V, W_j)$ of regular maps $\mathbb{A}(V) \to \mathbb{A}(W_j)$ carries a representation of T_V where W_j is equipped with the trivial action of T_V. It decomposes into a direct sum $\mathrm{Mor}(V, W_j) = \bigoplus \mathrm{Mor}(V, W_j)_\chi$ taken over all $\chi \in X(T_V)$, where

$$\mathrm{Mor}(V, W_j)_\chi = \{\psi \in \mathrm{Mor}(V, W_j) \mid \psi(t^{-1}v) = \chi(t)\psi(v) \text{ for all } t \in T_V(\bar{k}), v \in \mathbb{A}(V)(\bar{k})\}.$$

Thus $\psi_1, \dots, \psi_n$ can be written as sums $\psi_j = \sum_\chi \psi_j^\chi$ where only finitely many ψ_j^χ are different from 0. Similarly $f \in k[V] = \mathrm{Mor}(V, k)$ has a decomposition $f = \sum_\chi f^\chi$ with the same properties. Let

$$S(\psi, f) = \{\chi \in X(T_V) \mid f^\chi \neq 0 \text{ or } \exists j : \psi_j^\chi \neq 0\},$$

which is a finite subset of $X(T_V)$.

LEMMA 3.4. *If T is a split torus and $S \subset X(T)$ is a finite subset then there exists a one-parameter subgroup $\lambda \in \mathrm{Hom}_k(\mathbb{G}_{\boldsymbol{m}}, T)$ such that the restriction of the map $X(T) \to \mathrm{Hom}_k(\mathbb{G}_{\boldsymbol{m}}, \mathbb{G}_{\boldsymbol{m}}), \chi \mapsto \chi \circ \lambda$ to S is injective.*

PROOF. The claim can easily be shown via induction on the rank $r = \dim T$ of the torus. Identifying $X(T) = \mathbb{Z}^r = \mathrm{Hom}_k(\mathbb{G}_{\mathbf{m}}, T)$ and $\mathrm{Hom}_k(\mathbb{G}_{\mathbf{m}}, \mathbb{G}_{\mathbf{m}}) = \mathbb{Z}$ the above map is given by $\mathbb{Z}^r \to \mathbb{Z}, \quad \alpha \mapsto \langle \alpha, \beta \rangle := \sum_{i=1}^r \alpha_i \beta_i$, where $\beta \in \mathbb{Z}^r$ corresponds to λ. □

We will write $\langle \chi, \lambda \rangle$ for the image of $\chi \circ \lambda$ in $\mathbb{Z}$, i.e., $\chi \circ \lambda(s) = s^{\langle \chi, \lambda \rangle}$ for $s \in \mathbb{G}_{\mathbf{m}}(\bar{k})$.

PROPOSITION 3.5. *Let $\lambda \in \mathrm{Hom}_k(\mathbb{G}_{\boldsymbol{m}}, T_V)$ be such that the restriction of the map $X(T_V) \to \mathbb{Z}, \chi \mapsto \langle \chi, \lambda \rangle$ to $S(\psi, f)$ is injective (such λ exists by Lemma 3.4). Then $H_\lambda(\varphi)$ is multihomogeneous.*

PROOF. For notational simplicity set $\psi_0 = f$. There are unique characters $\chi_0, \chi_1, \ldots, \chi_n$ such that $\chi_j \circ \lambda$ is minimal (considered as an integer) amongst all $\chi \circ \lambda$ for which $\psi_j^\chi \neq 0$, for each $j = 0 \ldots n$. The rational map $\mathbb{A}(V) \times \mathbb{A}^1 \dashrightarrow \mathbb{A}(W_j)$ (or $\mathbb{A}(V) \times \mathbb{A}^1 \dashrightarrow \mathbb{A}^1$ for $j = 0$) given by

$$\begin{aligned} s^{-\langle \chi_j, \lambda \rangle} \psi_j(\lambda(s)v) &= s^{-\langle \chi_j, \lambda \rangle} \sum_\chi \psi_j^\chi(\lambda(s)v) \\ &= s^{-\langle \chi_j, \lambda \rangle} \sum_\chi \chi \circ \lambda(s) \psi_j^\chi(v) \\ &= \sum_\chi s^{\langle \chi - \chi_j, \lambda \rangle} \psi_j^\chi(v) \end{aligned}$$

has limit $\psi_j^{\chi_j}$, which implies that $H_\lambda(\varphi) = \frac{1}{f^{\chi_0}}(\psi_1^{\chi_1}, \ldots, \psi_n^{\chi_n})$. Define the homomorphism $D \in \mathrm{Hom}_k(T_V, T_W)$ by

$$D = (\chi_1 \chi_0^{-1}, \ldots, \chi_n \chi_0^{-1}).$$

Then $H_\lambda(\varphi)(tv) = D(t) H_\lambda(\varphi)(v)$, showing the claim. □

3.2. Existence of minimal multihomogeneous covariants. We now go over to the case where the graded vector spaces $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$ are furnished with a representation of an algebraic group G. We assume that the subspaces V_i and W_j are G-invariant. For $\lambda \in \mathrm{Hom}_k(T_V, T_W)$ as in Proposition 3.5 the rational map $H_\lambda(\varphi)\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ is multihomogeneous and has dimension $\dim H_\lambda(\varphi) \leq \dim \varphi$. Moreover, the rational map $H_\lambda(\varphi)$ is again G-equivariant as a limit of G-equivariant rational maps.

In general the covariant $H_\lambda(\varphi)$ does not have to be generically free if the covariant φ is. We will sidestep this difficulty with the following definition.

DEFINITION 3.6. We call an algebraic group G *friendly* if every faithful G-variety is generically free.

For example étale algebraic groups are friendly ([**FF07**, Lemma 1.1]). In contrast GL_n is not friendly for $n > 1$, since its natural faithful action on $\mathbb{A}^n$ is not generically free. Moreover we have the following result:

PROPOSITION 3.7. *Let G be an algebraic group. Assume that one of the following conditions is satisfied:*

(A) $G_{\bar{k}}$ is a direct product of a finite group and a torus
(B) G is finite and $(G_{\bar{k}})^0$ has only finitely many closed subgroups.

Then G is friendly.

PROOF. Since both freeness and generic freeness can be tested over an algebraic closure (cf. Lemma 7.1 of Chapter IV) we may and will assume that k is algebraically closed.

(A) Case A: Here G is a direct product $G = T \times F$ of a (split) torus T and a finite group F.

We first consider the case $G = T$. Let X be a faithful T-variety. Replacing X by its normalization we may assume that X is normal (note that the T-action on X can be lifted to its normalization and X is faithful or generically free if and only if its normalization is). By [**Su74**, Introduction a)] X is covered by affine open T-invariant sub-varieties. Hence we may assume that X embeds in $\mathbb{A}(V)$ for a T-module V. We choose V such that X does not embed in $\mathbb{A}(W)$ for a proper submodule $W \subseteq V$. Now let U be the intersection of X with the complement of $\bigcup \mathbb{A}(W)$ where W runs through all proper submodules of V formed by direct sums of character spaces. This is a T-invariant dense open subset of X with free T-action. Hence the claim follows.

The general case where $G = T \times F$ can be reduced to the case $G = T$ with a similar argument as in Chapter IV, Lemma 7.1.

(B) Case B: Here G is finite and G^0 has only finitely many closed subgroups. We have an exact sequence

$$1 \to G^0 \to G \to \bar{G} \to 1,$$

where $\bar{G}$ is étale. Note that G has only finitely many étale subgroups. Let X be a faithful G-variety and set

$$U := X \setminus (\bigcup X^H)$$

where H runs over all non-trivial closed subgroups which are either étale or contained in G^0. Clearly U is open, since each X^H is closed and the union is finite. Moreover by irreducibility and faithfulness of X the subset U is dense. We want to show that every $x \in U(\bar{k})$ has trivial stabilizer in G. The intersection $G_x \cap G^0$ is trivial by construction of U. Hence G_x maps isomorphically onto a closed subgroup of $\bar{G}$, which is étale. Hence G_x is étale, too. Again this is only possible if G_x is trivial. Replacing U by $\bigcap_{g \in G(k)} gU \subseteq U$ we may assume that U is G-invariant (cf. [**Sk02**, p. 344]). Then U is a G-invariant dense open subset of X with free G-action. This proves the claim.

□

Similarly as in [**KS07**, Lemma 4.1] we can prove the following result:

LEMMA 3.8. *Let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a faithful covariant between graded G-modules $V = \bigoplus_{i=1}^m V_i$, $W = \bigoplus_{j=1}^n W_j$. If $W_1, \dots, W_n$ are all irreducible, then $H_\lambda(\varphi)$ is faithful, i.e., G acts faithfully on the image closure of $H_\lambda(\varphi)$. In particular, if G is friendly then $H_\lambda(\varphi)$ is generically free again.*

PROOF. Let N_j and N_j' denote the stabilizer of the image closure of φ_j and $H_\lambda(\varphi)_j$, respectively. It suffices to show $N_j = N_j'$ for $j = 1 \dots n$. Fix j. Both maps φ_j and $H_\lambda(\varphi)_j$ are nonzero. Since W_j is irreducible it follows from Lemma 3.9 below that N_j and N_j' are both equal to the kernel of the G-action on $\mathbb{A}(W_j)$. The claim follows. □

LEMMA 3.9. *Let W be an irreducible G-module and $X \subseteq \mathbb{A}(W)$ be a G-stable subvariety, which is not contained in $\{0\}$. Then the kernels of the G-action on X and $\mathbb{A}(W)$ coincide.*

PROOF. We may assume that G acts faithfully on $\mathbb{A}(W)$. Let N denote the kernel of the G-action on X. This means $X \subseteq \mathbb{A}(W^N)$. Since N is normal $W^N \subseteq W$ is G-invariant. By irreducibility and since $X \not\subseteq \{0\}$ we have $W^N = W$. Faithfulness of the G-action on $\mathbb{A}(W)$ implies that N is trivial. □

Lemma 3.8 motivates the following definition:

DEFINITION 3.10. G is called *semi-faithful* (over k) if it admits a completely reducible faithful representation (over k).

A finite group G is semi-faithful over a field of $\operatorname{char} k = p > 0$ if and only if it has no nontrivial normal p-subgroups (cf. [**Na47**]). For an algebraic group G we have the following partial characterization of semi-faithful groups:

PROPOSITION 3.11. *If G does not contain any nontrivial normal unipotent closed subgroup then G is semi-faithful. The converse holds under the assumption that $G(k)$ is dense in G.*

PROOF. First assume that G does not have a nontrivial normal unipotent closed subgroup. Let V be a faithful G-module. Then the kernel of the G-action on the direct sum of the irreducible decomposition factors of V is a normal unipotent closed subgroup, hence trivial. This implies that G is semi-faithful.

Conversely assume that G has a faithful completely reducible module V and that $G(k)$ is dense in G. Let H be a normal unipotent closed subgroup. Then by [**Ja87**, Proposition 6.16] the restriction of V to H is completely reducible as well. Since every module of a unipotent group contains a nonzero fixed vector it follows that H acts trivially on V. Hence H is trivial, which proves the claim.

□

REMARK 3.12. Semi-faithfulness has been investigated in [**Va05**] for (smooth) reductive algebraic groups G. It is shown that every reductive group G is semi-faithful unless possibly $\operatorname{char} k = 2$. In characteristic 2 the groups SO_{2n+1} for $n \geq 1$ are given as examples of reductive and not semi-faithful algebraic groups. Moreover it is shown in that paper

that a reductive group over a field of charcteristic 2 is semi-faithful if and only if $G_{k_{\mathrm{sep}}}$ does not have a direct factor isomorphic to SO_{2n+1} for any $n \geq 1$.

REMARK 3.13. By a theorem of Rosenlicht the density assumption on $G(k)$ in Proposition 3.11 is satisfied if G is connected and k is perfect (and infinite), see e.g. [**Bo69**, Corollary 18.3]. For reductive algebraic groups G the density assumption in Proposition 3.11 can be dropped as shown in [**Va05**].

DEFINITION 3.14. A covariant $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ of G is called *minimal* if it is generically free and $\dim \varphi = \mathrm{ed}_k G$.

Given completely reducible G-modules $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$ of a friendly semi-faithful algebraic group G we can replace a minimal covariant $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ by its multihomogenization $H_\lambda(\varphi)$ (for suitable one-parameter subgroup λ of T_V as in Proposition 3.5) without loosing minimality, which follows from Lemma 3.3 and Lemma 3.8. This has the following consequence, which we will often use in the sequel:

PROPOSITION 3.15. *Let G be a friendly semi-faithful algebraic group. Then for any completely reducible faithful G-modules $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$ there exists a multihomogeneous minimal covariant $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ of G.*

REMARK 3.16. For the validity of Proposition 3.15 we do not really need that every faithful G-variety is generically free. It suffices that every faithful affine G-variety is generically free. For example the proposition holds for infinite and non-smooth algebraic groups of multiplicative type as well. Non-affine G-varieties will come into play in Theorem 5.2 of section 5.

4. Multihomogeneous invariants

Let $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$ be graded G-modules. The primary goal of this section is to find all possible degree matrices M_φ associated to multihomogeneous covariants $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$. To achieve this goal we have to study multihomogeneous invariants of V.

An element $f \in k(V)$ is called *multihomogeneous* if it is multihomogeneous regarded as a rational map $\mathbb{A}(V) \dashrightarrow \mathbb{A}^1$. The nonzero multihomogeneous rational invariants of V form a group under multiplication, which we denote by $\mathcal{M}_G(V)$. Note that $\mathcal{M}_G(V)$ depends on the grading of V.

For $f_1, \ldots, f_n \in \mathcal{M}_G(V)$ and a covariant $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ the rational map

$$\tilde{\varphi} = (f_1\varphi_1, \ldots, f_n\varphi_n)\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$$

is again a covariant. This gives us a method of modifying covariants by tuples $(f_1, \ldots, f_n) \in \mathcal{M}_G(V)^n$. Note that the degree matrix of $M_{\tilde{\varphi}}$ is obtained from M_φ by adding to the jth column the degree vector of f_j for $j = 1, \ldots, n$.

We will later make use of the following lemma:

LEMMA 4.1. *The set $\mathcal{M}_G(V) \cap k[V]^G$ generates $k[V]^G$ additively. If $k(V)^G = \mathrm{Quot}(k[V]^G)$ (which happens in particular if G is étale) then $\mathcal{M}_G(V)$ generates $k(V)^G$ as a field.*

PROOF. The first claim follows from the fact that $k[V]^G$ decomposes into a direct sum of G-invariant weight spaces for the T_V-action. The second claim follows easily from the first claim. □

In order to see what effect the above modification of covariants by n-tuples of invariants has on degree matrices, we need to study the possible degree vectors of multihomogeneous invariants.

DEFINITION 4.2. Let $V = \bigoplus_{i=1}^n V_i$ be a graded G-module. The *degree module* $\mathrm{DM}_G(V)$ of V is the submodule of $X(T_V) \simeq \mathbb{Z}^m$ formed by the degrees of multihomogeneous invariants, i.e., the image of the group homomorphism $\deg\colon \mathcal{M}_G(V) \to X(T_V), \quad f \mapsto X_f(\mathrm{Id}_{\mathbb{G}_\mathbf{m}})$. Equivalently it is the image of the group homomorphism

$$\prod_{f\in S} X(\mathbb{G}_\mathbf{m}) \to X(T_V)$$

induced by the homomorphisms $X_f\colon X(\mathbb{G}_\mathbf{m}) \to X(T_V)$, where S is any finite subset of $\mathcal{M}_G(V)$ whose degrees generate $\mathrm{DM}_G(V)$.

In the sequel we aim to relate the degree module of V to a certain subgroup of G. It is well known that every algebraic group G has a largest closed central subgroup of multiplicative type, see [**SGA3**] where it is called *centre réductif*. The following central subgroup of G is a split analogue and will play an important role in the sequel:

LEMMA 4.3. *There exists a (unique) largest closed central diagonalizable subgroup of G.*

PROOF. By [**SGA3**, Théorème 4.4] G admits a (unique) largest central subgroup A of multiplicative type. Its subgroup $\mathrm{Split}_k(A)$ constructed in Chapter IV, section 4 is the (unique) largest central diagonalizable subgroup of G. □

DEFINITION 4.4. We call the largest closed central diagonalizable subgroup from Lemma 4.3 the *k-center* of G and denote it by $Z(G,k)$.

EXAMPLES 4.5.
- The k-center of an algebraic group G of multiplicative type coincides with $\mathrm{Split}_k(G)$.
- If G is a finite group then

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

- The k-center of SL_2 is μ_2, which is smooth if and only if $\operatorname{char} k \neq 2$. This example shows that the k-center of a smooth (and even semi-simple) algebraic group can be non-smooth. Similarly if T is a one-dimensional non-split torus over a field of $\operatorname{char} k = 2$ then $Z(T,k) \simeq \mu_2$ is non-smooth.

If G is semi-faithful then $Z(G,k)$ is the largest closed subgroup of G which acts by scalars on every irreducible representation of G over k:

LEMMA 4.6. *Let $V = \bigoplus_{i=1}^m V_i$ be a completely reducible faithful G-module and $\rho\colon G \to \mathrm{GL}(V)$ the corresponding homomorphism. Then $\rho(Z(G,k)) = T_V \cap \rho(G)$.*

PROOF. By definition of $Z(G,k)$ and faithfulness of ρ the closed subgroup $\rho(Z(G,k))$ can be characterized as the largest closed central diagonalizable subgroup of $\rho(G)$. Since $\rho(G) \cap T_V$ is central and diagonalizable it is contained in $\rho(Z(G,k))$. For the reverse inclusion we must show that $\rho(Z(G,k))$ is contained in T_V. It suffices to show that $Z(G,k)$ acts by multiplication by scalars on every irreducible G-module W. As $Z(G,k)$ is diagonalizable we may write $W = \bigoplus_{\chi\in\Lambda} W_\chi$ where Λ is a finite set of characters of $Z(G,k)$ defined over k and $Z(G,k)$ acts on $\mathbb{A}(W_\chi)$ via χ. Since $Z(G,k)$ is central G preserves each $\mathbb{A}(W_\chi)$. Therefore $W = W_\chi$ for some $\chi \in \Lambda$ by irreducibility of W and the claim follows. □

The following relationship between the degree module and the k-center of an étale algebraic group G shows, that the possible degree vectors of multihomogeneous invariants are only restricted by the influence of the k-center of G:

PROPOSITION 4.7. *Assume that G is étale and that $V = \bigoplus_{i=1}^m V_i$ is a completely reducible faithful G-module. Then the sequence*

$$\mathcal{M}_G(V) \xrightarrow{\deg} X(T_V) \to X(Z(G,k)) \to 1$$

is exact. In particular $\mathrm{DM}_G(V) = \{\chi \in X(T_V) \mid \chi|_{Z(G,k)} = 1\}$ *and* $X(T_V)/\mathrm{DM}_G(V) \simeq X(Z(G,k))$.

PROOF. Choose a finite subset $S \subseteq \mathcal{M}_G(V)$ such that the degrees of the elements of S generate $\mathrm{DM}_G(V)$. We may replace the homomorphism $\deg\colon \mathcal{M}_G(V) \to X(T_V)$ by the homomorphism $X(\prod_{f\in S} \mathbb{G}_{\mathbf{m}}) \to X(T_V)$, since they both have image $\mathrm{DM}_G(V)$. Now the claim becomes equivalent to exactness of the sequence

$$1 \to Z(G,k) \xrightarrow{\rho} T_V \to \prod_{f\in S} \mathbb{G}_{\mathbf{m}}\,.$$

Exactness at $Z(G,k)$ follows directly from the faithfulness of V. Denote by Q the kernel of the last map, which is the intersection of the kernels of the maps $D_f\colon T_V \to \mathbb{G}_{\mathbf{m}}$ taken over all multihomogeneous invariants $f \in S$. Clearly $\rho(Z(G,k)) \subseteq Q$ because each $f \in S$ is G-invariant. On the other hand let $\tilde{G} = \rho(G)\cdot Q$ be the subgroup of $\mathrm{GL}(V)$ generated by $\rho(G)$ and Q, defined as the image of the morphism $\rho(G) \times Q \to \mathrm{GL}(V), (g,h) \mapsto gh$ of algebraic groups. This is again a finite algebraic group defined over k and contains $\rho(G)$ as a normal subgroup. The quotient $\tilde{G}/\rho(G) \simeq Q/(Q \cap \rho(G))$ is diagonalizable. By construction we have $\mathcal{M}_G(V) = \mathcal{M}_{\tilde{G}}(V)$ and Lemma 4.1 implies $\bar{k}(V)^G = \mathrm{Quot}(\bar{k}[V]^G) = \mathrm{Quot}(\bar{k}[V]^{\tilde{G}}) \subseteq \bar{k}(V)^{\tilde{G}} \subseteq \bar{k}(V)^{\rho(G)}$, hence $\bar{k}(V)^G = \bar{k}(V)^{\tilde{G}}$. By [**Sk02**] we get $|G| = \max(G : G_x) = [\bar{k}(V) : \bar{k}(V)^G] = [\bar{k}(V) : \bar{k}(V)^{\tilde{G}}] = \max(\tilde{G} : \tilde{G}_x)$, where the maxima are taken over all $x \in V \otimes \bar{k}$, and G_x (resp. $\tilde{G}_x$) denotes the stabilizer of x in G (resp. $\tilde{G}$). By Lemma 3.7 $V \otimes \bar{k}$ contains a point x with trivial stabilizer in $\tilde{G}$ (note that $(\tilde{G}_{\bar{k}})^0$ is finite and diagonalizable, hence contains only finitely many closed subgroups). Hence $|G| = |\tilde{G}|$ and Lemma 4.6 implies $Q = \rho(Z(G,k))$. □

DEFINITION 4.8. For graded G-modules $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$ we denote by $\mathrm{mCov}(V,W)$ the space of multihomogeneous covariants $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$.

The formula

$$(f_1, \dots, f_n) \cdot \varphi = (f_1\varphi_1, \dots, f_n\varphi_n) \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$$

for $(f_1, \dots, f_n) \in \mathcal{M}_G(V)^n$ induces an action of the group $\mathcal{M}_G(V)^n$ on $\mathrm{mCov}(V, W)$, which respects faithfulness when all W_j are irreducible. Furthermore we get an action of $\mathcal{M}_G(V)^n$ on the set $S = \{X_\varphi \colon \varphi \in \mathrm{mCov}(V, W)\} \subseteq \mathrm{Hom}(X(T_W), X(T_V))$ of all degrees associated to multihomogeneous covariants. We will identify $\mathcal{M}_G(V)^n$ with the group $\mathrm{Hom}(X(T_W), \mathcal{M}_G(V))$ by associating with an element $\gamma \in \mathrm{Hom}(X(T_W), \mathcal{M}_G(V))$ the n-tuple $(f_1, \dots, f_n) \in \mathcal{M}_G(V)$ where $f_j = \gamma(\chi_j)$ for the standard basis of $X(T_W)$ formed by the characters $\chi_j \colon T_W \to \mathbb{G}_{\mathbf{m}}, t = (t_1, \dots, t_n) \mapsto t_j$. Then the action on degrees is given by

$$\begin{aligned} \mathrm{Hom}(X(T_W), \mathcal{M}_G(V)) \times S &\to S, \\ (\gamma, s) &\mapsto \gamma s \colon X(T_W) \to X(T_V) \\ \chi &\mapsto (\deg \gamma(\chi)) \cdot s(\chi). \end{aligned}$$

From Proposition 4.7 we get the following result, which says that every possible degree matrix of multihomogeneous covariants of an étale algebraic group can be obtained by modifying an arbitrary multihomogeneous covariant by a suitable tuple of multihomogeneous invariants.

Corollary 4.9. *If G is étale and $V = \bigoplus_{i=1}^m V_i$ is completely reducible and faithful then the group $\mathrm{Hom}(X(T_W), \mathcal{M}_G(V))$ acts transitively on S.*

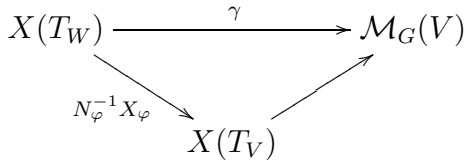
Proof. Let $s, s' \in S$ and choose $\varphi, \varphi' \in \mathrm{mCov}(V, W)$ such that $s = X_\varphi$ and $s' = X_{\varphi'}$. Define $D \in \mathrm{Hom}_k(T_V, T_W)$ by $D(t) = D_\varphi(t) D_{\varphi'}(t^{-1})$ for $t \in T_V(\bar{k})$. Then $D|_{\rho(Z(G,k))} = 1$, since D_φ and $D_{\varphi'}$ are both the identity on $\rho(Z(G, k))$. By Proposition 4.7 this is equivalent to saying that $X(D) \in \mathrm{Hom}(X(T_W), \mathrm{DM}_G(V))$. Therefore $X(D)$ comes from some homomorphism $\gamma \in \mathrm{Hom}(X(T_W), \mathcal{M}_G(V))$. By construction $\gamma s' = s$, finishing the proof. □

In general modifying a minimal faithful multihomogeneous covariant $\varphi \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ by a tuple of multihomogeneous invariants $(f_1, \dots, f_n) \in \mathcal{M}_G(V)^n$ will increase the dimension of the covariant. In the rest of this section we show that certain tuples of multihomogeneous invariants do not have this effect at all, whereas in general the increase in dimension is not as large as it could be expected.

Let $\varphi \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a faithful multihomogeneous covariant. Let $N_\varphi \in \mathbb{N}$ be the greatest common divisor of the entries of the elements of $\operatorname{im} X_\varphi \subseteq X(T_V) \cong \mathbb{Z}^m$, where $m = \dim T_V$. Then $N_\varphi^{-1} X_\varphi \colon X(T_W) \to X(T_V)$ is well defined and its image has a complement in $X(T_V)$. We distinct between two types of elements of $\mathrm{Hom}(X(T_W), \mathcal{M}_G(V))$ relative to φ:

Definition 4.10. A homomorphism $\gamma \colon X(T_W) \to \mathcal{M}_G(V)$ is called of

- *type I relative to* φ if it factors through $N_\varphi^{-1}X_\varphi\colon X(T_W) \to X(T_V)$, i.e., if there exists a commutative diagram of the form



- *type II relative to* φ if the image of γ equals the image of $\ker X_\varphi \hookrightarrow X(T_W) \to \mathcal{M}_G(V)$.

PROPOSITION 4.11. *Every homomorphism* $\gamma\colon X(T_W) \to \mathcal{M}_G(V)$ *decomposes as* $\gamma = \alpha \cdot \beta$ *where* $\alpha\colon X(T_W) \to \mathcal{M}_G(V)$ *is of type I relative to* φ *and* $\beta\colon X(T_W) \to \mathcal{M}_G(V)$ *is of type II relative to* φ.

PROOF. Choose decompositions $X(T_W) = \ker X_\varphi \oplus A$ and $X(T_V) = \operatorname{im} N_\varphi^{-1}X_\varphi \oplus B$. Define the homomorphisms $\alpha, \beta\colon X(T_W) \to \mathcal{M}_G(V)$ by

$$\alpha|_{\ker X_\varphi} = 1,\ \beta|_{\ker X_\varphi} = \gamma|_{\ker X_\varphi} \quad \text{and} \quad \alpha|_A = \gamma|_A,\ \beta|_A = 1.$$

Clearly β is of type II relative to φ and $\alpha\beta = \gamma$.

Note that the homomorphism $N_\varphi^{-1}X_\varphi\colon X(T_W) \to X(T_V)$ induces an isomorphism from A to its image in $X(T_V)$. Thus we may define $\varepsilon\colon X(T_V) \to \mathcal{M}_G(V)$ by $\varepsilon|_B = 1$ and $\varepsilon(N_\varphi^{-1}X_\varphi(\chi)) = \gamma(\chi)$ for $\chi \in A$. This shows that α is of type I relative to φ, finishing the proof. □

PROPOSITION 4.12. *If* γ *is of type I relative to* φ *then* $\overline{(\gamma\varphi)(V \otimes \bar{k})} \subseteq \overline{\varphi(V \otimes \bar{k})}$ *and in particular* $\dim(\gamma\varphi) \leq \dim \varphi$. *For arbitrary* γ *the dimension of* $\gamma\varphi$ *is at most* $\dim \varphi + (\operatorname{rank} X(T_W) - \operatorname{rank} M_\varphi)$.

PROOF. Let γ be of type I relative to φ. Then there exists $\varepsilon\colon X(T_V) \to \mathcal{M}_G(V)$ such that $\gamma = \varepsilon \circ N_\varphi^{-1}X_\varphi$. We have rational evaluation maps $\mathrm{ev}_\gamma\colon \mathbb{A}(V) \dashrightarrow T_W$ and $\mathrm{ev}_\varepsilon\colon \mathbb{A}(V) \dashrightarrow T_V$, such that $(\gamma\varphi)(v) = \mathrm{ev}_\gamma(v)\varphi(v)$ and similarly for ε. Now let $v \in V \otimes \bar{k}$ such that ev_ε and φ are defined at v. Choose $t \in T_V(\bar{k})$ such that $t^{N_\varphi} = \mathrm{ev}_\varepsilon(v)$. Then one checks easily that $\mathrm{ev}_\gamma(v) = D_\varphi(t)$, whence

$$(\gamma\varphi)(v) = \mathrm{ev}_\gamma(v)\varphi(v) = D_\varphi(t)\varphi(v) = \varphi(tv).$$

This proves the first claim.

The second claim follows from the first, since the image of $\ker X_\varphi \hookrightarrow X(T_W) \to \mathcal{M}_G(V)$ is generated by $r := \operatorname{rank}(\ker X_\varphi) = \operatorname{rank} X(T_W) - \operatorname{rank} M_\varphi$ functions. □

5. Properties of multihomogeneous covariants

5.1. The rank of the degree-matrix of a multihomogeneous covariant.

DEFINITION 5.1. For a diagonalizable group D we denote by $\operatorname{rank} D$ the minimal number of generators of the character group $X(D)$ and call it the *rank of* D. Equivalently this number can be expressed as the least dimension of a split torus in which D embeds.

For a faithful multihomogeneous covariant $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ of a friendly semi-faithful algebraic group we will prove the following inequality relating the rank of M_φ and the rank of the k-center $Z(G,k)$ (see Definition 4.4):

THEOREM 5.2. *Let G be a friendly semi-faithful algebraic group and let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a faithful multihomogeneous covariant between completely reducible faithful G-modules $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$. Then* $\operatorname{rank} M_\varphi \geq \operatorname{rank} Z(G,k)$ *and*

$$\operatorname{ed}_k G + \dim G - \operatorname{rank} Z(G,k) \leq \dim \varphi - \operatorname{rank} M_\varphi.$$

In particular if φ is minimal then

$$\operatorname{rank} M_\varphi = \operatorname{rank} Z(G,k).$$

REMARK 5.3. The case when G is a finite group with trivial center (and $k = \mathbb{C}$) is Proposition 3.4 of Chapter II.

PROOF OF THEOREM 5.2. Let $\rho_V\colon G \to \mathrm{GL}(V)$ and $\rho_W\colon G \to \mathrm{GL}(W)$ denote the representation homomorphisms. By Lemma 4.6 we have $\rho_V(Z(G,k)) \subseteq T_V$. Since φ is equivariant with respect to both the tori- and G-action, $\rho_W(Z(G,k)) = D_\varphi(\rho_V(Z(G,k))) \subseteq D_\varphi(T_V)$. Hence $\operatorname{rank} M_\varphi = \operatorname{rank} D_\varphi(T_V) \geq \operatorname{rank} \rho_W(Z(G,k)) = \operatorname{rank} Z(G,k)$.

The second inequality follows from the Proposition 5.4 below, 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 $\overline{\varphi(\mathbb{A}(V))}$ by a free action of a torus S of dimension $\operatorname{rank} M_\varphi - \operatorname{rank} Z(G,k)$. □

PROPOSITION 5.4. *Let $\varphi = (\varphi_1, \ldots, \varphi_n)\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a faithful multihomogeneous covariant between completely reducible G-modules $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$. Then there exists a sub-torus $S \subseteq D_\varphi(T_V)$ of dimension* $\operatorname{rank} M_\varphi - \operatorname{rank} Z(G,k)$ *and a G-invariant dense open subset $W' \subseteq \mathbb{A}(W)$ on which $D_\varphi(T_V)$ acts freely such that the geometric quotient $(\overline{\varphi(\mathbb{A}(V))} \cap W')/S$ exists as a variety and its induced G-action is faithful.*

In the sequel we use the following notation:

DEFINITION 5.5. Let $V = \bigoplus_{i=1}^m V_i$ be a graded vector space. Define the variety $\mathbb{PP}(V)$ by

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

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

For the proof of Proposition 5.4 we need Lemma 5.6 below. A special case is shown in Chapter II, Lemma 3.3. A similar argument can be used to prove the more general statement.

LEMMA 5.6. *Let $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$ be graded G-modules with each W_j irreducible and let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a faithful multihomogeneous covariant. Let $\pi_W\colon \mathbb{A}(W) \dashrightarrow \mathbb{PP}(W)$ be the obvious G-equivariant rational map. Then the kernel of the action of G on $\pi_W(\overline{\varphi(\mathbb{A}(V))})$ equals $Z(G,k)$.*

PROOF OF PROPOSITION 5.4. The torus $D_\varphi(T_V)$ contains $Z(G,k)$ and has dimension $d := \operatorname{rank} M_\varphi \geq r := \operatorname{rank} Z(G,k)$. By the elementary divisor theorem there exist a non-negative integer $a \leq r$, integers $c_1, \dots, c_a > 1$ and a basis $\chi_1, \dots, \chi_d$ of $X(D_\varphi(T_V))$ such that

$$Z(G,k) = \bigcap_{i=1}^{a} \ker \chi_i^{c_i} \cap \bigcap_{j=r+1}^{d} \ker \chi_j.$$

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

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 $X := \overline{\varphi(\mathbb{A}(V))}$ and also the open subset $X' := X \cap W'$ of X. The S-action on X' is free in the sense of [**MFK94**, Definition 0.8] and in particular separated. In the notation of [**MFK94**] X' coincides with $(X')^s(\mathrm{Pre})$. By [**MFK94**, Proposition 1.9] a (uniform) 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 5.6. Since $Z(G,k) \cap S = \{1\}$ it is trivial. □

REMARK 5.7. Theorem 5.2 does not hold for non-friendly algebraic groups (with faithful replaced by generically free) in general. For example the identity map of $\mathrm{Mat}_{2\times 2}$ is a generically free covariant of GL_2, which is a special algebraic group (hence $\operatorname{ed}_k \mathrm{GL}_2 = 0$). It is multihomogeneous and has degree matrix $M = 1_{\mathrm{Mat}_{2\times 2}}$ of rank 2. The k-center of GL_2 is isomorphic to $\mathbb{G}_\mathbf{m}$. However

$$\operatorname{ed}_k \mathrm{GL}_2 + \dim \mathrm{GL}_2 - \operatorname{rank} Z(\mathrm{GL}_2, k) = 3 \not\leq 2 = \dim \mathrm{Id}_{\mathrm{Mat}_{2\times 2}} - \operatorname{rank} M.$$

To illustrate the usefulness of the existence of minimal multihomogeneous covariants and Lemma 5.6 we give a simple corollary.

COROLLARY 5.8. *Let G be a friendly semi-faithful algebraic group. Then* $\operatorname{ed}_k G + \dim G \geq \operatorname{rank} Z(G,k)$. *Moreover*

- $\operatorname{ed}_k G + \dim G = \operatorname{rank} Z(G,k)$ *if and only if $G = Z(G,k)$, i.e., if and only if G is diagonalizable.*
- *If* $\operatorname{ed}_k G + \dim G \leq \operatorname{rank} Z(G,k) + 1$, *then $G/Z(G,k)$ acts faithfully on a projective rational curve. If moreover $G/Z(G,k)$ is smooth then G is an extension of a closed subgroup of* PGL_2 *by $Z(G,k)$.*

PROOF. By assumption G has a faithful completely reducible module $V = \bigoplus_{i=1}^{m} V_i$. Let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a minimal multihomogeneous covariant of G and set $X := \overline{\varphi(\mathbb{A}(V))}$. Then $D_\varphi(T_V)$ acts generically freely on X. From this we deduce $\operatorname{ed}_k G + \dim G = \dim X \geq \dim D_\varphi(T_V) = \operatorname{rank} M_\varphi$, which is equal to $\operatorname{rank} Z(G,k)$ by Theorem 5.2. By Lemma 5.6 the group $G/Z(G,k)$ acts faithfully on the projective variety $Y := \overline{\pi_V \circ \varphi(\mathbb{A}(V))} \subseteq \mathbb{PP}(V)$. The non-empty fibers of the restriction $X \dashrightarrow Y, x \mapsto \pi_V(x)$ of π_V have dimension $\geq \dim D_\varphi(T_V) = \operatorname{rank} Z(G,k)$. Hence $\dim Y \leq \dim X - \dim D_\varphi(T_V) = \dim \varphi - \operatorname{rank} Z(G,k) = \operatorname{ed}_k G + \dim G - \operatorname{rank} Z(G,k)$.

When $\operatorname{ed}_k G + \dim G \leq \operatorname{rank} Z(G,k)$ the variety Y must be a single point, whence $G = Z(G,k)$. Conversely a diagonalizable group G embeds in $\mathbb{G}_{\mathbf{m}}^{\operatorname{rank} G}$, which is special, whence $\operatorname{ed}_k G + \dim G \leq \dim \mathbb{G}_{\mathbf{m}}^{\operatorname{rank} G} = \operatorname{rank} Z(G,k)$. This solves the first case. In the second case when $\operatorname{ed}_k G + \dim G \leq \operatorname{rank} Z(G,k)+1$ the unirational variety Y has dimension ≤ 1 and it follows by Lüroth's theorem that Y is rational. When $G/Z(G,k)$ is smooth it acts faithfully on the normalization of Y, which is either $\mathbb{P}^1$ or a single point. Since the automorphism group of $\mathbb{P}^1$ is PGL_2 it follows in that case that $G/Z(G,k)$ embeds in PGL_2. In other words G is an extension of a closed subgroup of PGL_2 by $Z(G,k)$. □

Remark 5.9. Corollary 5.8 can be used to classify friendly semi-faithful algebraic groups with $\operatorname{ed}_k G + \dim G - \operatorname{rank} Z(G,k) \leq 1$. We conjecture that any finite semi-faithful group G of $\operatorname{ed}_k G \leq 2$ with nontrivial k-center $Z(G,k)$ embeds into $\mathrm{GL}_2(k)$. In case of $k = \mathbb{C}$ this follows from [**KS07**, Theorem 10.2] and the relationship between covariant and essential dimension from [**KLS09**, Theorem 3.1] (see Chapter II).

5.2. Behavior under refinement of the grading. Let $V = \bigoplus_{i=1}^m V_i$ be a graded vector space. For each i let $V_i = \bigoplus_{k=1}^{d_i} V_{ik}$ be a grading of V_i. We call the grading $V = \bigoplus_{i,k} V_{ik}$ a *refinement* of the grading $V = \bigoplus_i V_i$. Let $\varphi = (\varphi_1, \dots, \varphi_n) \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a multihomogeneous rational map. We consider refinements both in V and in $W = \bigoplus_{j=1}^n W_j$ where $W_j = \bigoplus_{l=1}^{e_j} W_{jl}$, and study the behavior of the rank of the degree matrix. Set $d = \sum_{i=1}^m d_i$ and $e = \sum_{j=1}^n e_j$.

Proposition 5.10. *(A) Refinement in V: Let λ be a one-parameter subgroup of $T_V = \mathbb{G}_{\boldsymbol{m}}^d$ such that $H_\lambda(\varphi) \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ is multihomogeneous w.r.t. the refined grading on V and the old grading on W. Then*

$$\operatorname{rank} M_{H_\lambda(\varphi)} \geq \operatorname{rank} M_\varphi.$$

(B) Refinement in W: The map φ can be considered as a multihomogeneous rational map $\varphi' \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ with respect to the old grading on V and the refined grading on W. Then

$$\operatorname{rank} M_{\varphi'} = \operatorname{rank} M_\varphi.$$

(C) Refinement in both V and W: Consider φ' as above and let λ be a one-parameter subgroup of $T_V = \mathbb{G}_{\boldsymbol{m}}^d$ be such that $H_\lambda(\varphi') \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ is multihomogeneous w.r.t. the refined grading on both V and W. Then

$$\operatorname{rank} M_{H_\lambda(\varphi')} \geq \operatorname{rank} M_\varphi.$$

Proof. (A) Let $(a_{i,j}) = M_\varphi \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ and $(b_{ik,j}) = M_{H_\lambda(\varphi)} \in \mathrm{Mat}_{d,n}(\mathbb{Z})$ be the degree matrices of φ and $H_\lambda(\varphi)$, respectively. Since $H_\lambda(\varphi)$ is still multihomogeneous with respect to the old grading on V we have $\sum_{k=1}^{d_i} b_{ik,j} = a_{i,j}$ for $i = 1 \dots m$ and $j = 1 \dots n$. Therefore the span of the rows of $M_{H_\lambda(\varphi)}$ contains the span of the rows of M_φ. Hence $\operatorname{rank} M_{H_\lambda(\varphi)} \geq \operatorname{rank} M_\varphi$.

(B) The maps $\varphi_{jl} \colon V \dashrightarrow W_{jl}$ are still multihomogeneous of the same degree as $\varphi_j \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W_j)$. Thus the column span of M_φ equals the column span of $M_{\varphi'}$ and hence $\operatorname{rank} M_\varphi = \operatorname{rank} M_{\varphi'}$.

(C) follows from (A) and (B).

□

6. Covariant dimension versus essential dimension

In this section G denotes an étale algebraic group. Recall the definition of the *covariant dimension* of G:

Definition 6.1.

$$\operatorname{cdim}_k G := \min\{\dim \varphi \mid \varphi\colon \mathbb{A}(V) \to \mathbb{A}(W) \text{ faithful regular covariant}\},$$

where V and W are faithful G-modules.

Note that this is the analogue of essential dimension with the only difference that the minimum is taken over regular (rather than rational) covariants. Similarly as for essential dimension the following holds: For any faithful G-modules V and W there exists a faithful regular covariant $\varphi\colon \mathbb{A}(V) \to \mathbb{A}(W)$ with $\dim \varphi = \operatorname{cdim}_k G$.

The following result relates essential and covariant dimension of semi-faithful étale algebraic groups. The special case when $k = \mathbb{C}$ is contained in Theorem 3.1 of Chapter II.

Theorem 6.2. *Let G be a non-trivial semi-faithful étale algebraic group. Then* $\operatorname{cdim}_k G = \operatorname{ed}_k G$ *if and only if $Z(G,k)$ is non-trivial. Otherwise* $\operatorname{cdim}_k G = \operatorname{ed}_k G + 1$.

Proof. For the proof we use the modification of multihomogeneous covariants by (tuples of) multihomogeneous invariants from section 4.

Let $V = \bigoplus_{i=1}^n V_i$ be a faithful completely reducible G-module. The case when $Z(G,k)$ is trivial follows from the inequality $\operatorname{cdim}_k G \leq \operatorname{ed}_k G + 1$ (cf. [**Re04**]) and Theorem 5.2, since M_φ cannot be the zero-matrix for any non-constant regular multihomogeneous covariant $\varphi\colon \mathbb{A}(V) \to \mathbb{A}(V)$.

Now assume that $Z(G,k)$ is non-trivial. Let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a minimal multihomogeneous covariant. First assume that there exists a row vector $\beta \in \mathbb{Z}^n$ such that all entries of $\alpha := \beta M_\varphi$ are strictly positive. We may assume that φ is of the form $\varphi = \frac{\psi}{f}$ where $f \in k[V]^G$ is multihomogeneous and $\psi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ is a (faithful) regular multihomogeneous covariant. Consider $\tilde{\varphi} = (f^{\alpha_1}\varphi_1, \ldots, f^{\alpha_n}\varphi_n)$. It is of the form $\gamma\varphi$ where $\gamma \in \operatorname{Hom}(X(T_V), \mathcal{M}_G(V))$ is of type I relative to φ. Since $\alpha_j > 0$ for all j the covariant $\tilde{\varphi}$ is regular. Proposition 4.12 implies

$$\operatorname{cdim}_k G \leq \dim \tilde{\varphi} \leq \dim \varphi = \operatorname{ed}_k G.$$

We reduce to the case above by composing with a covariant as in Example 3.2. Since V is faithful and $Z(G,k)$ is non-trivial M cannot be the zero matrix. Write $M_\varphi = (m_{ij})$ and fix i_0 and j_0 with $m_{i_0 j_0} \neq 0$. Then $\varphi_{j_0} \neq 0$ and we can find a homogeneous $h \in k[W_{j_0}]^G$ of degree $\deg h > 0$ such that $h \circ \varphi_{j_0} \neq 0$. For any $r \in \mathbb{Z}$ consider the covariant

$$\varphi'\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V), \quad v \mapsto h^r(\varphi_{j_0}(v))\varphi(v).$$

Since $h \circ \varphi_{j_0} \neq 0$ and φ is faithful, φ' is faithful, too. Clearly $\dim \varphi' \leq \dim \varphi = \operatorname{ed}_k G$. Moreover φ' is multihomogeneous of degree $M_{\varphi'} = (m'_{ij})$ where $m'_{ij} = m_{ij} + r \deg h m_{ij_0}$. For suitable $r \in \mathbb{Z}$ this yields a matrix $M_{\varphi'}$ where all $m'_{i_0 j}$ for $j = 1 \ldots n$ are strictly

positive. Now for $\beta = e_{i_0}$ the entries of $\alpha = \beta M_\varphi$ are all strictly positive and we are in the case above. □

REMARK 6.3. The statement of Theorem 6.2 also holds in characteristic p for a finite elementary abelian p-group A, which has essential dimension 1 by [**Le07**, Proposition 5], trivial k-center $Z(A,k)$ and covariant dimension 2, as the following argument shows: It is enough to consider the case $A = \mathbb{Z}/p\mathbb{Z}$. Let V denote the 2-dimensional representation of A where a generator $a \in A$ acts as $a(s,t) = (s, s+t)$. Suppose that there exists a regular faithful covariant $\varphi\colon \mathbb{A}(V) \to \mathbb{A}(V)$ with $X = \overline{\varphi(\mathbb{A}(V))}$ of dimension 1. Then the generator a induces an automorphism of order p on the normalization of X, which is isomorphic to $\mathbb{A}^1$. Since in characteristic p no automorphism of $\mathbb{A}^1$ of order p has fixed points we get a contradiction.

7. The central extension theorem

We show the following generalization of the theorem about the essential dimension of central extensions from [**BR97**]:

THEOREM 7.1. *Let G be a friendly algebraic group. Let H be a closed subgroup of $Z(G,k)$ with $H \cap [G,G] = \{e\}$ and assume that G/H is semi-faithful and friendly. 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 H' is diagonalizable. Then*

$$\operatorname{ed}_k G + \dim G - \operatorname{rank} Z(G,k) \leq \operatorname{ed}_k G/H + \dim G/H - \operatorname{rank} Z(G/H,k).$$

Moreover if H is finite then equality holds, i.e.,

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

REMARK 7.2. Theorem 7.1 generalizes the following results about central extensions: [**BR97**, Theorem 5.3], [**Ka08**, Theorem 4.5], [**Le04**, Theorem 8.2.11], [**BRV08**, Theorem 7.1 and Corollary 7.2] and [**BRV07**, Lemma 11.2]. Some special cases of Theorem 7.1 are also contained in Chapter II, see Corollaries 3.7 and 4.7 of Chapter II.

If G is a finite algebraic group of p-power order then Theorem 7.1 can be deduced from Theorem 1.3 of Chapter IV.

REMARK 7.3. Let $\operatorname{rdim}_k G$ denote the least dimension of a faithful representation of an algebraic group G. Under the assumptions of Theorem 7.1 one can show

$$\operatorname{rdim}_k G - \operatorname{rank} Z(G,k) \leq \operatorname{rdim}_k G/H - \operatorname{rank} Z(G/H,k),$$

but equality does not need to hold.

PROOF OF THEOREM 7.1. Embed H' in $\mathbb{G}_{\mathbf{m}}^r$ where $r := \operatorname{rank} H'$. There exist generators $\hat{\chi}_1, \hat{\chi}_2, \ldots, \hat{\chi}_r$ of $X(\mathbb{G}_{\mathbf{m}}^r) = \mathbb{Z}^r$ and non-negative natural numbers $n_1, n_2, \ldots, n_r$ such that

$$H = \bigcap_i \ker \hat{\chi}_i^{n_i}.$$

If H is finite then $n_1, n_2, \ldots, n_r$ are strictly positive and $H \simeq \mu_{n_1} \times \cdots \times \mu_{n_r}$. Denote by χ_i for $i = 1, \ldots, r$ the restriction of $\hat{\chi}_i$ to H'. Then

$$H = \bigcap_i \ker \chi_i^{n_i}.$$

Let C be a direct complement of H' in $G/[G,G]$ and denote by $\pi\colon G \to G/[G,G] = H' \times C \to H'$ the projection onto H'. Let $W = \bigoplus_{i=1}^m W_i$ be a completely reducible faithful G/H-module and denote by k_{χ_i} the one-dimensional G-module where G acts through $\chi_i \circ \pi$ via scalar multiplication. Then

$$V := (\bigoplus_{i=1}^m W_i) \oplus (\bigoplus_{j=1}^r k_{\chi_j})$$

is a completely reducible faithful G-module. We first prove the inequality $\operatorname{ed}_k G + \dim G - \operatorname{rank} Z(G,k) \leq \operatorname{rank} Z(G,k) + \dim G/H - \operatorname{rank} Z(G/H,k)$: Let $\varphi\colon \mathbb{A}(W) \dashrightarrow \mathbb{A}(W)$ be a minimal multihomogeneous covariant of G/H. Define a faithful covariant of G by

$$\Phi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V), \quad (w, t_1, \ldots, t_r) \mapsto (\varphi(w), t_1, \ldots, t_r).$$

Clearly Φ is multihomogeneous again with $\operatorname{rank} M_\Phi = \operatorname{rank} M_\varphi + r = \operatorname{rank} Z(G/H,k) + r$, where the last equality comes from Theorem 5.2. Moreover by the same theorem,

$$\begin{aligned}\operatorname{ed}_k G + \dim G &\leq \dim \Phi - (\operatorname{rank} M_\Phi - \operatorname{rank} Z(G,k)) \\ &= \operatorname{ed}_k G/H + \dim G/H - \operatorname{rank} Z(G/H,k) + \operatorname{rank} Z(G,k).\end{aligned}$$

Now assume that H is finite. We must show $\operatorname{ed}_k G/H - \operatorname{rank} Z(G/H,k) \leq \operatorname{ed}_k G - \operatorname{rank} Z(G,k)$. Let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a minimal multihomogeneous covariant of G. Let

$$V' := (\bigoplus_{i=1}^m W_i) \oplus (\bigoplus_{j=1}^r k_{\chi_j^{n_j}})$$

and consider the G-equivariant regular map

$$\pi\colon \mathbb{A}(V) \to \mathbb{A}(V'), \quad (w, t_1, \ldots, t_r) \mapsto (w, t_1^{n_1}, \ldots, t_r^{n_r}).$$

Since $H \simeq \mu_{n_1} \times \cdots \times \mu_{n_r}$ this is the quotient map for the geometric quotient of the H-action on $\mathbb{A}(V)$. The composition $\varphi' := \pi \circ \varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V')$ is H-invariant, hence we get a commutative diagram:

$$\begin{array}{ccc} \mathbb{A}(V) & \overset{\varphi}{\dashrightarrow} & \mathbb{A}(V) \\ {\scriptstyle\pi}\downarrow & \searrow^{\varphi'} & \downarrow{\scriptstyle\pi} \\ \mathbb{A}(V') & \overset{\bar{\varphi}}{\dashrightarrow} & \mathbb{A}(V') \end{array}$$

where $\bar{\varphi}\colon \mathbb{A}(V') \dashrightarrow \mathbb{A}(V')$ is a faithful G/H-covariant. Since π is finite the rational maps φ, φ' and $\bar{\varphi}$ all have the same dimension equal to $\operatorname{ed}_k G + \dim G$. Moreover φ' and $\bar{\varphi}$ are multihomogeneous as well. The degree matrix $M_{\varphi'}$ is obtained from M_φ by multiplying its last r columns by $n_1, n_2, \ldots, n_r > 0$ and from $M_{\bar{\varphi}}$ by multiplying its last r rows by $n_1, n_2, \ldots, n_r > 0$. Hence $\operatorname{rank} M_\varphi = \operatorname{rank} M_{\varphi'} = \operatorname{rank} M_{\bar{\varphi}}$. Application

of Theorem 5.2 yields: $\operatorname{ed}_k G/H + \dim G/H - \operatorname{rank} Z(G/H,k) \leq \dim \bar{\varphi} - \operatorname{rank} M_{\bar{\varphi}} = \operatorname{ed}_k G + \dim G - \operatorname{rank} Z(G,k)$. Since $\dim G/H = \dim G$ this finishes the proof. □

COROLLARY 7.4. *Let G be a friendly semi-faithful algebraic group and A be a smooth finite diagonalizable algebraic group. Then*

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

PROOF. Apply Theorem 7.1 to the central subgroup $\{e\} \times A \subseteq G \times A$. □

Another application of the central extension theorem is the following corollary:

COROLLARY 7.5. *Let $V = \bigoplus_{i=1}^m V_i$ be a faithful completely reducible module of an étale semi-faithful algebraic group G. Let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a minimal multihomogeneous covariant. Then (the image closure of) the rational map $\pi_V \circ \varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{PP}(V)$ has exactly dimension* $\dim \varphi - \operatorname{rank} Z(G,k)$.

PROOF. The inequality $\dim \pi_V \circ \varphi \leq \dim \varphi - \operatorname{rank} Z(G,k)$ was already shown in the proof of Corollary 5.8. To prove the reverse inequality let $p \neq \operatorname{char} k$ be a prime and let $r \in \mathbb{N}$ be such that $Z(G,k)$ has a subgroup of the form μ_p^r but none of the form μ_p^{r+1}. One easily shows that V admits a faithful representation of $\tilde{G} := G \times \mu_p^{n-r}$ where $n = \dim T_V$.

Corollary 4.9 implies the existence of $\gamma \in \operatorname{Hom}(X(T_V), \mathcal{M}_G(V))$ such that $\gamma\varphi$ is D-equivariant for $D = \operatorname{Id}_{T_V}$. This turns $\tilde{\varphi} := \gamma\varphi$ into a faithful (multihomogeneous) covariant for $\tilde{G}$. Corollary 7.4 shows that $\dim \tilde{\varphi} \geq \operatorname{ed}_k \tilde{G} = \operatorname{ed}_k G + (n - \operatorname{rank} Z(G,k))$. Since $\pi_V \circ \tilde{\varphi} = \pi_V \circ \varphi$ we get $\dim \pi_V \circ \varphi = \dim \pi_V \circ \tilde{\varphi} \geq \dim \tilde{\varphi} - n \geq \dim \varphi - \operatorname{rank} Z(G,k)$, showing the claim. □

8. Subgroups and direct products

PROPOSITION 8.1. *Let H be a closed subgroup of an algebraic group G. Assume that H and G are friendly and that G has a completely reducible faithful representation which remains completely reducible when restricted to H. Then*

$$\operatorname{ed}_k H + \dim H - \operatorname{rank} Z(H,k) \leq \operatorname{ed}_k G + \dim G - \operatorname{rank} Z(G,k).$$

PROOF. Let $V = \bigoplus_{i=1}^m V_i$ be a faithful G-module with each V_i irreducible which is completely reducible as H-module and let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a minimal multihomogeneous covariant. By Theorem 5.2 $\operatorname{rank} M_\varphi = \operatorname{rank} Z(G,k)$. Now consider φ as a covariant for H. When replacing φ by a multihomogenization $H_\lambda(\varphi)$ with respect to a refinement into irreducible H-submodules we have $\operatorname{rank} M_{H_\lambda(\varphi)} \geq \operatorname{rank} M_\varphi$ by Proposition 5.10. Hence again by Theorem 5.2 $\operatorname{ed}_k H + \dim H - \operatorname{rank} Z(H,k) \leq \dim H_\lambda(\varphi) - \operatorname{rank} M_{H_\lambda(\varphi)} \leq \dim \varphi - \operatorname{rank} M_\varphi = \operatorname{ed}_k G + \dim G - \operatorname{rank} Z(G,k)$. □

REMARK 8.2. There exist pairs (H,G) of a finite group G with subgroup H such that both H and G are semi-faithful over k, but none of the completely reducible faithful representations of G restricts to a completely reducible representation of H. We found some examples using the computer algebra system [**MAGMA**], the smallest (in terms of the order of G) is a pair of the form $H = S_3$, $G = C_2 \ltimes (C_3 \ltimes (C_3 \times C_3))$ in characteristic 2. Also there are examples in order 72 with $G = Q_8 \ltimes (C_3 \times C_3)$ or $G = C_8 \ltimes (C_3 \times C_3)$.

PROPOSITION 8.3. *Let G_1 and G_2 be friendly semi-faithful algebraic groups such that $G_1 \times G_2$ is friendly as well. Then*

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

PROOF. Let $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$ be faithful completely reducible modules of G_1 and G_2, respectively. Let $\varphi_1 \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ and $\varphi_2 \colon \mathbb{A}(W) \dashrightarrow \mathbb{A}(W)$ be minimal multihomogeneous covariants for G_1 and G_2. Then $\operatorname{rank} M_{\varphi_1} = \operatorname{rank} Z(G_1, k)$ and $\operatorname{rank} M_{\varphi_2} = \operatorname{rank} Z(G_2, k)$ by Theorem 5.2. 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 $\operatorname{rank} M_\varphi = \operatorname{rank} M_{\varphi_1} + \operatorname{rank} M_{\varphi_2} = \operatorname{rank} Z(G_1, k) + \operatorname{rank} Z(G_2, k)$. Thus, by Theorem 5.2,

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

Since $\dim \varphi_1 = \operatorname{ed}_k G_1 + \dim G_1$ and $\dim \varphi_2 = \operatorname{ed}_k G_2 + \dim G_2$ this implies the claim. □

REMARK 8.4. We do not know of an example where the inequality in Proposition 8.3 is strict.

EXAMPLE 8.5. Let k be a field which admits a cyclic extension of degree 6. Let l_2 and l_3 be intermediate fields with $[l_i : k] = i$. Let $T_i := R^{(1)}_{l_i/k}(\mathbb{G}_{\mathbf{m}l_i})$ denote the kernels of the norm morphisms $R_{l_i/k}(\mathbb{G}_{\mathbf{m},l_i}) \to \mathbb{G}_{\mathbf{m},k}$. Here $R_{l/k}(\mathbb{G}_{\mathbf{m},l})$ is the algebraic group representing the functor $A \mapsto \mathbb{G}_{\mathbf{m},l}(A \otimes l) = (A \otimes l)^\times$ from commutative k-algebras to groups, called *Weil restriction* of $\mathbb{G}_{\mathbf{m},l}$ to k, and the maps $(A \otimes l)^\times \to A^\times$ send an element $x \in (A \otimes l)^\times$ to the determinant of the k-linear map on $(A \otimes l)$ given by left-multiplication by x.

The (quasi-split) tori $R_{l_i/k}(\mathbb{G}_{\mathbf{m},l_i})$ are well known to be special, i.e., $\operatorname{ed}_k R_{l_i/k} = 0$ (see e.g. [**FF07**, p. 3892]). Moreover T_2 and T_3 have essential dimension 1 by [**BF03**, Theorem 2.5]. We have $\mu_i \simeq Z(T_i, k) \subset Z(R_{l_i/k}(\mathbb{G}_{\mathbf{m},l}), k) \simeq \mathbb{G}_{\mathbf{m},k}$. Hence T_2, T_3 and $T_2 \times T_3$ all have k-center of rank 1. Proposition 8.3 implies $\operatorname{ed}_k T_2 \times T_3 \leq 1$ and since $\operatorname{ed}_k T_2 \times \operatorname{ed}_k T_3 \geq \operatorname{ed}_k T_2 = 1$ [**BF03**, Remarks 1.16] it follows that $\operatorname{ed}_k T_2 \times T_3 = 1$.

The inequality $\operatorname{ed}_k T_2 \times T_3 \leq 1$ also follows from Proposition 8.1 considering $T_2 \times T_3$ as a closed subgroup of the torus $R_{l_2/k}(\mathbb{G}_{\mathbf{m},l_2}) \times R_{l_3/k}(\mathbb{G}_{\mathbf{m},l_3})$, which has essential dimension 0.

9. A generalization of Florence' twisting construction

Twisting of quasi-projective varieties by torsors and its functorial properties have been used by MATHIEU FLORENCE in his computation of the essential dimension of cyclic p-groups [**Fl08**]. He starts with a faithful irreducible representation V of minimal dimension of a cyclic p-group $G = \mathbb{Z}/p^r\mathbb{Z}$ and a faithful homogeneous covariant $\varphi \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$. By homogeneity and since $Z(G, k)$ acts trivially on $\mathbb{P}(V)$ the covariant φ induces a $H := G/Z(G, k)$-equivariant rational map $\psi \colon \mathbb{P}(V) \dashrightarrow \mathbb{P}(V)$. The twist of $\mathbb{P}(V)$ by a generic H-torsor is shown to be the Severi Brauer variety $\mathrm{SB}(D)$ associated with a central division algebra D of p-power degree. The functorial properties of the twist construction yield a rational map $\hat{\psi} \colon \mathrm{SB}(D) \dashrightarrow \mathrm{SB}(D)$ with $\dim \hat{\psi} \leq \dim \psi$. By a result of NIKITA KARPENKO every rational map $\mathrm{SB}(D) \dashrightarrow \mathrm{SB}(D)$ is dominant. Florence concludes that φ is dominant as well.

We will use the twisting construction for completely reducible modules of arbitrary semi-faithful algebraic groups G and connect this construction with the stack-theoretic approach used in [**KM08, BRV07, BRV08**]. Assume now that $V = \bigoplus_{i=1}^m V_i$ is a faithful completely reducible module of an algebraic group G and let $\varphi = (\varphi_1, \dots, \varphi_m)\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a multihomogeneous covariant of G with $\varphi_j \neq 0$ for all j (we do not assume that φ is generically free). Since φ is multihomogeneous the composition $\pi_V \circ \varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{PP}(V) = \prod_{j=1}^m \mathbb{P}(V_i)$ is T_V-invariant. Hence there exists a rational map $\psi\colon \mathbb{PP}(V) \dashrightarrow \mathbb{PP}(V)$ making the diagram

$$\begin{array}{ccc} \mathbb{A}(V) & \overset{\varphi}{\dashrightarrow} & \mathbb{A}(V) \\ \downarrow{\scriptstyle \pi_V} & & \downarrow{\scriptstyle \pi_V} \\ \mathbb{PP}(V) & \overset{\psi}{\dashrightarrow} & \mathbb{PP}(V) \end{array}$$

commute. Let C be any closed central diagonalizable subgroup of G. We view ψ as an $H := G/C$-equivariant rational map. Let K/k be a field extension and E be an H-torsor over K. We twist the H-equivariant rational map ψ (after scalar extension to K) by the H-torsor E and obtain a rational map

$${}^E\psi_K\colon {}^E\mathbb{PP}(V \otimes K) \dashrightarrow {}^E\mathbb{PP}(V \otimes K).$$

Here the twist of a quasi-projective H-variety X by a H-torsor E is the categorical quotient $(E \times X)/H$ where H acts on $E \times X$ by $h(e, x) = (eh^{-1}, hx)$. For details of the twist construction and its properties we refer to [**Fl08**, section 2] and [**FF07**].

In the sequel we use the connecting map

$$\delta\colon H^1(K, H) \to H^2(K, C)$$

in non-abelian cohomology (with respect to the fppf-topology) associated to the exact sequence

$$1 \to C \to G \to H \to 1$$

(see [**Gi71**]) and compose it with the map

$$\chi_*\colon H^2(K, C) \to H^2(K, \mathbb{G}_\mathbf{m}) \simeq \mathrm{Br}(K)$$

induced by some character $\chi \in X(C)$, where $\mathrm{Br}(K)$ is the Brauer group of K. Now fix an H-torsor E over K. Since $H^1(K, H)$ classifies H-torsors we can look at the image of the class $[E] \in H^1(K, H)$ of E under the map $\chi_* \circ \delta\colon H^1(K, H) \to \mathrm{Br}(K)$. This yields a map

$$\beta^E\colon X(C) \to \mathrm{Br}(K), \chi \to \beta^E(\chi) := \chi_* \circ \delta([E]),$$

which is easily seen to be a group homomorphism. The twisted variety is now described as follows:

Lemma 9.1. ${}^E\mathbb{PP}(V \otimes K) \simeq \prod_{i=1}^m \mathrm{SB}(A_i)$. *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* $\beta^E(\chi_i)$ *where* $\chi_i \in X(C)$ *is the character of* C *through which* C *acts on* $\mathbb{A}(V_i)$*.*

Proof. The first claim follows from [**Fl08**, Lemma 3.1]. For the second claim see [**KM08**, Lemma 4.3]. □

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 9.3.

DEFINITION 9.2. Let X be a K-variety and $D \subseteq \mathrm{Br}(K)$ 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**, section 1.4]) of X (resp. D). It is denoted by $\mathrm{cd}(X)$ (resp. $\mathrm{cd}(D)$).

LEMMA 9.3 ([**KM06**, Corollary 4.6]). *Let $X = \prod_{i=1}^{n} \mathrm{SB}(A_i)$ be a product of Severi Brauer varieties of central simple K-algebras $A_1, \dots, A_n$. Then $e(X) = \mathrm{cd}(X) = \mathrm{cd}(D)$, where $D \subseteq \mathrm{Br}(K)$ is the subgroup generated by the classes of $A_1, \dots, A_n$.*

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

THEOREM 9.4. *Let G be a semi-faithful algebraic group and $V = \bigoplus_{i=1}^{m} V_i$ a faithful completely reducible G-module. Let E be a G/C-torsor over an extension K of k where C is any closed subgroup of $Z(G,k)$. Then*

$$\mathrm{ed}_k G + \dim G - \operatorname{rank} Z(G,k) \geq e\left({}^{E}\mathbb{PP}(V \otimes K)\right) = \mathrm{cd}(\operatorname{im} \beta^{E}).$$

PROOF. Replacing V by a direct sum of enough copies of V we may assume that V is generically free. Let $\tilde{\varphi}\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a minimal covariant and denote by $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ its multihomogenization (which is faithful, but not necessarily generically free). Let $\psi\colon \mathbb{PP}(V) \dashrightarrow \mathbb{PP}(V)$ be associated to φ as in the beginning of this section. Lemma 3.3 implies $\dim \varphi \leq \dim \tilde{\varphi} = \mathrm{ed}_k G + \dim G$. Let us write $\dim \theta$ for the dimension of the image closure of a rational map θ like in the case of covariants. Since the image closure of ${}^{E}\psi_K$ is the twist of the image closure of ψ_K by E we have $\dim {}^{E}\psi_K = \dim \psi_K$. Hence

$$e\left({}^{E}\mathbb{PP}(V \otimes K)\right) \leq \dim {}^{E}\psi_K \leq \dim \psi_K = \dim \psi.$$

We now show that $\dim \psi \leq \dim \varphi - \operatorname{rank} Z(G,k)$. Let $X := \overline{\varphi(\mathbb{A}(V))} \subseteq \mathbb{A}(V)$. 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 or equal to $\operatorname{rank} Z(G,k)$, 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 V is faithful restricted to C the characters $\chi_1, \dots, \chi_m$ generate $X(C)$. Lemma 9.3 and Lemma 9.1 imply $e\left({}^{E}\mathbb{PP}(V \otimes K)\right) = \mathrm{cd}\left({}^{E}\mathbb{PP}(V \otimes K)\right) = \mathrm{cd}\operatorname{im} \beta^{E}$, hence the claim. □

REMARK 9.5 (The choice of the subgroups $C \subseteq Z(G,k)$). Karpenko and Merkurjev work with the subgroup of elements of exponent p in $Z(G,k)$. In their setting G is a p-group and k contains a primitive pth root of unity, so C is the smallest subgroup of $Z(G,k)$ with the same rank as $Z(G,k)$. In general the best lower bound is obtained with the maximal choice, i.e., with the subgroup $C = Z(G,k)$. This is seen as follows: Set $Z = Z(G,k)$. For a G/C-torsor E' over K let E denote its image under $H^1(K, G/C) \to H^1(K, G/Z)$. Then

for any $\chi \in X(Z)$ we have a commutative diagram:

$$\begin{array}{ccccccc} H^1(K, G/C) & \longrightarrow & H^2(K, C) & \xrightarrow{(\chi|_C)_*} & H^2(K, \mathbb{G}_{\mathbf{m}}) & \longrightarrow & \mathrm{Br}(K) \\ \downarrow & & \downarrow & & \| & & \| \\ H^1(K, G/Z) & \longrightarrow & H^2(K, Z) & \xrightarrow{\chi_*} & H^2(K, \mathbb{G}_{\mathbf{m}}) & \longrightarrow & \mathrm{Br}(K) \end{array}$$

Since every element of $X(C)$ is the restriction of some character $\chi \in X(Z)$ this shows that $\mathrm{im}(\beta^E) = \mathrm{im}(\beta^{E'})$, hence their canonical dimensions coincide.

We now go further to prove a generalization of Karpenko and Merkurjev's [**KM08**, Theorem 4.1]. This however involves two key results from their work:

THEOREM 9.6 ([**KM08**, Theorem 2.1 and Remark 2.9]). *Let p be a prime, K be a field and $D \subseteq \mathrm{Br}(K)$ be a finite p-subgroup of rank $r \in \mathbb{N}$. Then* $\operatorname{cd} D = \min\{\sum_{i=1}^{r}(\operatorname{Ind} a_i - 1)\}$ *taken over all generating sets $a_1, \ldots, a_r$ of D. Here* $\operatorname{Ind} a_i$ *denotes the index of a_i.*

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

THEOREM 9.7 ([**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 a generic H-torsor E over some field extension K/k such that for all $\chi \in X(C)$:*

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

We have the following result:

COROLLARY 9.8 (cf. [**KM08**, Theorem 4.1]). *Let G be a finite group whose socle C is a central p-subgroup for some prime p and let k be a field containing a primitive p-th root of unity. Assume that for all $\chi \in X(C)$ the equality*

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

holds. Then $\operatorname{ed}_k G$ *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 $\operatorname{ed}_k G \leq d$ is clear. By the assumption on k we have $\operatorname{rank} C = \operatorname{rank} Z(G, k) = \operatorname{rank} Z(G)$. Hence, by Theorem 9.4, it suffices to show $\operatorname{cd}(\operatorname{im} \beta^E) = d - \operatorname{rank} C$ for a generic $H := G/C$-torsor E over a field extension K of k.

By Theorem 9.6 there exists a basis $a_1, \ldots, a_s$ 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 $\chi_1, \ldots, \chi_r$ of $X(C)$ such that $a_i = \beta^E(\chi_i)$ for $i = 1, \ldots, s$ and $\beta^E(\chi_i) = 1$ for $i > s$ and choose $V_i \in \mathrm{Rep}^{(\chi_i)}(G)$ of minimal dimension. By assumption $\dim V_i = \gcd\left\{\dim V \mid V \in \mathrm{Rep}^{(\chi_i)}(G)\right\}$, which is equal to the index of $\beta^E(\chi_i)$ for the H-torsor E of Theorem 9.7.

Set $V = V_1 \oplus \cdots \oplus V_r$. This is a faithful representation since every normal subgroup of G intersects $C = \operatorname{soc} G$ non-trivially. Then $\operatorname{cd}(\operatorname{im} \beta^E) = \sum_{i=1}^{s}(\operatorname{Ind} a_i - 1) =$

$\sum_{i=1}^{r} \operatorname{Ind} \beta^E(\chi_i) - \operatorname{rank} C = \sum_{i=1}^{r} \dim V_i - \operatorname{rank} C = \dim V - \operatorname{rank} C \geq d - \operatorname{rank} C$. The claim follows. □

We conclude this section with the following conjecture, which is based on Theorem 9.4 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**, section 7].

Conjecture 9.9. *Let G be a finite group whose socle $C := \operatorname{soc} G$ is central and let k be a field containing a primitive p-th root of unity for every prime p dividing $|C|$. Assume that for all $\chi \in X(C)$ of prime order $\min \dim W = \gcd \dim W$ taken on both sides over all $W \in \operatorname{Rep}^{(\chi)}(G)$. Then*

$$\operatorname{ed}_k G = \dim V - \sum_p \operatorname{rank} C(p) + \operatorname{rank} C,$$

where $V = \bigoplus V_p$ is a faithful representation of G, the direct sum being taken over all primes p dividing $|C|$, and V_p is of minimal dimension amongst representations of G whose restriction to $C(p)$ is faithful.

Proof of Conjecture 9.9 assuming the truth of formula (3). "$\leq$": Consider the identity map $\operatorname{Id}\colon \mathbb{A}(V) \to \mathbb{A}(V)$, which is a multihomogeneous covariant. Theorem 5.2 implies $\operatorname{ed}_k G \leq \dim \operatorname{Id} - (\operatorname{rank} M_{\operatorname{Id}} - \operatorname{rank} Z(G,k)) = \dim V - \sum_p \operatorname{rank} C(p) + \operatorname{rank} C$.

"$\geq$": Choose a generic G/C-torsor E. Then $\operatorname{ed}_k G \geq \operatorname{cd}(\operatorname{im} \beta^E) + \operatorname{rank} C$, by Theorem 9.4. The p-Sylow subgroup of the image of the abelian group $C = \bigoplus_p C(p)$ equals $\beta^E(C(p))$. Formula (3) implies that $\operatorname{cd} \operatorname{im} \beta^E = \sum_p \operatorname{cd} \beta^E(C(p))$, which can be computed with the help of Theorems 9.6 and 9.7. Similarly as in the proof of Corollary 9.8 we get the claim, using the replacement of gcd by min. □

Remark 9.10. The conditions $\operatorname{soc} C \subseteq Z(G)$ and $\min \dim W = \gcd \dim W$ for all $W \in \operatorname{Rep}^{(\chi)}(G)$ and χ of prime order are satisfied for nilpotent groups. In that case V_p is simply a faithful representation of minimal dimension of a p-Sylow subgroup of G.

Remark 9.11. Formula (3) was proven in [**CKM07**] in the special case where D is cyclic of order 6 and k contains $\mathbb{Q}(\zeta_3)$, where $\zeta_3 = e^{\frac{2\pi i}{3}}$. 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 $\operatorname{ed}_k G = 4$ for any field k containing $\mathbb{Q}(\zeta_3)$.

Using the computer algebra systems [**MAGMA**] and [**GAP**] (and [**SAGE**] to combine the two) we found several examples of non-nilpotent groups for which [**CKM07**, Theorem 1.3] applies when k is a field containing $\mathbb{Q}(\zeta_3)$. These are groups (of order 432) with $\operatorname{soc} G = Z(G) \simeq C_6$ whose Sylow 2- and 3-subgroup have essential dimension 2 and 3, respectively. We get for their essential dimension $\operatorname{ed}_k G = (2+3) - 2 + 1 = 4$.

10. Normal elementary p-subgroups

Suppose that we are in the case of a non semi-faithful finite group G. Recall from the remark above Proposition 3.11 that this happens precisely when $\operatorname{char} k = p > 0$ and G contains a nontrivial normal p-subgroup A. Replacing A by the elements of $Z(A)$ of exponent p (which is again normal in G) we may assume that A is p-elementary. In particular $\operatorname{ed}_k A = 1$ by [**Le07**, Proposition 5]. We would like to relate $\operatorname{ed}_k G$ and $\operatorname{ed}_k G/A$ and use this iteratively to pass to the semi-faithful case.

PROPOSITION 10.1. *If A is a elementary p-group, which is normal in G and if* $\operatorname{char} k = p$ *then* $\operatorname{ed}_k G/A \leq \operatorname{ed}_k G$. *If furthermore A is central in G then*

$$(*) \qquad \operatorname{ed}_k G/A \leq \operatorname{ed}_k G \leq \operatorname{ed}_k G/A + 1.$$

For the proof of Proposition 10.1 we make use of Merkurjev's notion of the essential dimension of a functor from the category of field extensions of k to the category of sets, see [**BF03**]. Consider the Galois cohomology functor $H^1(*, G)$, which takes a field extension K/k to the Galois cohomology set $H^1(K, G) := H^1(\operatorname{Gal}(K_{\text{sep}}/K), G(K_{\text{sep}}))$. An element $\alpha \in H^1(K, G)$ is said to descend to a subfield $K_0 \subseteq K$ (containing k) if α belongs to the image of $H^1(K_0, G) \to H^1(K, G)$. The essential dimension of α is defined as the least transcendence degree (over k) of a subfield K_0 to which α descends. The essential dimension of G (from Definition 1.4) is then equal to the maximal essential dimension of α taken over all K/k and $\alpha \in H^1(K, G)$.

PROOF OF PROPOSITION 10.1. Since A is normal there is the following exact sequence in Galois cohomology:

$$1 \to H^1(*, A) \to H^1(*, G) \to H^1(*, G/A)$$

[**Se64**, Proposition 58]. For A is an elementary abelian p-group and $\operatorname{char} k = p$ we have $H^2(*, A) = 0$. Moreover by [**TV10**, Lemma 3.2 and Lemma 3.3] $H^2(*, \tilde{A}) = 0$ for any twisted form $\tilde{A}$ of A. Therefore by [**Se64**, Corollary after Proposition 41] $H^1(*, G) \to H^1(*, G/A)$ is a surjection of functors. In particular $\operatorname{ed}_k G/A \leq \operatorname{ed}_k G$ by [**BF03**, Lemma 1.9].

Now suppose that A is central in G. We have an action of $H^1(*, A)$ on $H^1(*, G)$ as follows: Let K/k be a field extension and let $[\alpha] \in H^1(K, A)$ and $[\beta] \in H^1(K, G)$ and set $[\alpha] \cdot [\beta] := [\alpha\beta] \in H^1(K, G)$. Since A is central $\alpha\beta$ satisfies the cocyle condition and its class in $H^1(K, G)$ does not depend on the choice of α and β. Moreover it is well known that two elements of $H^1(K, G)$ have the same image in $H^1(K, G/A)$ if and only if one is transformed from the other by an element of $H^1(K, A)$, see [**Se64**]. Thus we have a transitive action on the fibers of $H^1(K, G) \twoheadrightarrow H^1(K, G/A)$, and this action is natural in K. That means we have a fibration of functors

$$H^1(*, A) \rightsquigarrow H^1(*, G) \twoheadrightarrow H^1(*, G/A).$$

Now [**BF03**, Proposition 1.13] yields $\operatorname{ed}_k G \leq \operatorname{ed}_k G/A + \operatorname{ed}_k A = \operatorname{ed}_k G/A + 1$. □

REMARK 10.2. The inequality $\operatorname{ed}_k G \leq \operatorname{ed}_k G/A + 1$ of Proposition 10.1 also follows from a very recent result [**TV10**, Lemma 3.4] of DAJANO TOSSICI and ANGELO VISTOLI. More generally they show the inequality $\operatorname{ed}_k G \leq \operatorname{ed}_k G/A + \operatorname{ed}_K \tilde{A}$ for an algebraic group

G, a commutative unipotent normal algebraic subgroup A of G, where K is some field extension of k and $\tilde{A}$ is a twisted form of A over K. When A is central, $\tilde{A}$ is $A_K = \operatorname{Spec} F \times_{\operatorname{Spec} k} A$.

REMARK 10.3. If G is a finite p-group and A is a (not necessarily central) elementary abelian p-subgroup contained in the Frattini subgroup of G then [**Le04**] gives the relations $(*)$ as well.

EXAMPLE 10.4. Let G denote the perfect group of order $8! = 40320$ which is a central extension of A_8 by C_2. The socle of this group $\operatorname{soc} G = C_2$ is central.
Claim: $\operatorname{ed}_k G = 8$ if $\operatorname{char} k \neq 2$ and $\operatorname{ed}_k G \in \{2, 3, 4\}$ if $\operatorname{char} k = 2$.

PROOF. First consider the case when $\operatorname{char} k \neq 2$. There exists a faithful irreducible G-module of degree 8. This implies in particular that $\operatorname{ed}_k G \leq 8$. Moreover one may check using a Computer algebra system like [**MAGMA**] or [**GAP**] that the degree of every faithful irreducible representation of G is a multiple of 8. The faithful irreducible representations of G are precisely the elements of $\operatorname{Rep}^{(\chi)}(G)$ where χ is the non-trivial character of $\operatorname{soc} G = C_2$. Hence the claim follows with Corollary 9.8.

Now consider the case of $\operatorname{char} k = 2$. Proposition 10.1 implies that $\operatorname{ed}_k A_8 \leq \operatorname{ed}_k G \leq \operatorname{ed}_k A_8 + 1$. The essential dimension of $A_8 \simeq \mathrm{GL}_4(\mathbb{F}_2)$ is either 2 or 3 [**Ka06**, Lemma 5.5 and Theorem 5.6], and the claim follows. □

Bibliography

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

[Bo69] A. Borel: *Linear Algebraic Groups*, Benjamin (1969).

[BR97] J. Buhler, Z. Reichstein: *On the essential dimension of a finite group*, Compos. 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.

[BS08] P. Brosnan, R. Sreekantan: *Essential dimension of abelian varieties over number fields*, C. R. Acad. Sci. Paris, Ser. I **346**(7-8) (2008), 417–420.

[CKM07] J.-L. Colliot-Thélène, N. Karpenko, A. Merkurjev: *Rational surfaces and canonical dimension of* PGL_6, Algebra i Analiz **19** (2007), no. 5, 159–178, translation in St.Petersburg Math.J. **19** (2008), no. 5, 793–804.

[FF07] G. Favi, M. Florence: *Tori and essential dimension*, J. Algebra **319**(9) (2008), 3885–3900.

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

[GAP] M. Schönert et al.: *GAP Groups, Algorithms, and Programming.* Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, third edition, 1993.

[Gi71] J. Giraud, *Cohomologie non abélienne*, Die Grundlehren der mathematischen Wissenschaften **179** (1971), Springer-Verlag.

[Ja87] J. C. Jantzen, *Representations of Algebraic Groups.* Pure and Applied Mathematics, 131. Academic Press, Orlando, Florida, (1987).

[Ka06] M.C. Kang: *Essential dimensions of finite groups*, Arxiv:math/0611673, 2006.

[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**(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**(1) (2009), 94–107.

[KS07] H. Kraft, G. Schwarz: *Compression of finite group actions and covariant dimension*, J. Algebra **313**(1) (2007), 268–291.

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

[Le07] A. Ledet: *Finite groups of essential dimension one*, J. Algebra **311** (2007), 31–37.

[MAGMA] W. Bosma, J. Cannon, C. Playoust: *The Magma algebra system. I. The user language.* J. Symbolic Comput., **24(3-4)** (1997), 235–265.

[Me09] A. Merkurjev: *Essential dimension*, in Quadratic forms – algebra, arithmetic, and geometry (R. Baeza, W.K. Chan, D.W. Hoffmann, and R. Schulze-Pillot, eds.), Contemp. Math. **493** (2009), 299–326.

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

[Re00] Z. Reichstein: *On the notion of essential dimension for algebraic groups*, Transf. Groups, **5**(3) (2000), 265–304.

[Re04] Z. Reichstein: *Compressions of group actions*, Invariant Theory in all Characteristics, CRM Proc. Lecture Notes vol. **35**, Amer. Math. Soc., Providence, **35** (2004), 199-202.

[SAGE] W. Stein: *Sage: Open Source Mathematical Software (Version 3.0.6)*, The Sage Group, 2008, `http://www.sagemath.org`.

[Se64] J.P. Serre: *Cohomologie Galoisienne*, Lecture Notes in Math., Springer-Verlag, 1964.

[SGA3] Séminaire de géométrie algébrique de lI.H.E.S., 1963-1964, *schémas en groupes*, dirigé par M. Demazure et A. Grothendieck, Lecture Notes in Math. **151–153**, Springer, 1970.

[Sk02] S. Skryabin: *Invariants of finite group schemes*, J. Lond. Math. Soc. **65**(2) (2002), 339–360.

[Su74] H. Sumihiro: *Equivariant completion*, J. Math. Kyoto Univ. **14**(1) (1974), 1–28.

[TV10] D. Tossici, A. Vistoli: *On the essential dimension of infinitesimal group schemes*, Arxiv:1001.3988v2, 2010.

[Va05] A. Vasiu: *Normal, unipotent subgroup schemes of reductive groups*, C. R. Acad. Sci. Paris, Ser. I **341**(2) (2005) 79-84.

CHAPTER II

Compressions of finite group actions and covariant dimension, II

HANSPETER KRAFT, ROLAND LÖTSCHER AND GERALD SCHWARZ

(published in the Journal of Algebra)

Let G be a finite group and $\varphi\colon V \to W$ an equivariant polynomial map between finite dimensional G-modules. We say that φ is faithful if G acts faithfully on $\varphi(V)$. The covariant dimension of G is the minimum of the dimension of $\overline{\varphi(V)}$ taken over all faithful φ. In [**KS07**] we investigated covariant dimension and were able to determine it in many cases. Our techniques largely depended upon finding homogeneous faithful covariants. After publication of [**KS07**], the junior author of this article pointed out several gaps in our proofs. Fortunately, this inspired us to find better techniques, involving multihomogeneous covariants, which have enabled us to extend and complete the results, simplify the proofs and fill the gaps of [**KS07**].

1. Introduction

For simplicity we take our ground field to be the field $\mathbb{C}$ of complex numbers. (Much work has been done in the context of more general fields (see, for example, [**Flo08, JLY02, Led07, KM08**]). In [**Löt08**] our results are extended to this context.) Let G be a finite group. All G-modules that we consider will be finite dimensional. A *covariant* of G is an equivariant morphism (= polynomial map) $\varphi\colon V \to W$ where V and W are G-modules. The *dimension* of φ is defined to be the dimension of the image of φ:

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

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

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

$$\operatorname{ed} G \le \operatorname{cdim} G \le \operatorname{ed} G + 1$$

(see [**Rei04**] or the proof of Theorem 2.5 below).

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

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

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

We thank the referee for helpful comments.

2. Multihomogeneous Covariants

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

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

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

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

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

REMARKS 2.1. (A) If the V_i and W_j are G-modules and φ is equivariant, so are all the $\varphi_j^{(\alpha)}$ and $\varphi_{\max}$. Note that no entry in $\varphi_{\max}$ is zero since the same is true of φ.

(B) If $\varphi\colon V \to W$ is multihomogeneous of degree $A = (\alpha_{ji})$ and $\psi\colon W \to U = \bigoplus_{k=1}^{\ell} U_\ell$ is multihomogeneous of degree $B = (\beta_{kj})$ and all components of $\psi \circ \varphi$ are non-zero, then the composition $\psi \circ \varphi\colon V \to U$ is multihomogeneous of degree BA.

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

LEMMA 2.1. *Let $\varphi\colon V \to W$ be a morphism where no φ_j is zero. Then* $\dim \varphi_{\max} \leq \dim \varphi$.

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

$$\Phi\colon \mathbb{C} \times V \to \mathbb{C} \times W, \quad (t, v) \mapsto (t, {}^t\varphi(v))$$

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

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

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

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

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

COROLLARY 2.2. *Let $p\colon \overline{Y} \to \mathbb{C}$ be as in the proof above. If* $\dim \varphi = \dim \varphi_{\max}$ *and* $\operatorname{im}\varphi$ *is $\mathbb{C}^*$-stable, then $p^{-1}(0)$ is $\mathbb{C}^*$-stable.*

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

THEOREM 2.3. *Let G be a finite group and let $V = \oplus_{i=1}^n V_i$ and $W = \oplus_{j=1}^m W_j$ be faithful representations where the V_i and W_j are irreducible submodules. Then there is a minimal regular multihomogeneous covariant $\varphi\colon V \to W$ all of whose components are nonzero.*

PROOF. Let $\varphi\colon V \to W$ be a minimal covariant. We can always arrange that for given $v \in V$ and $w \in W$, both with trivial stabilizer in G, we have $\varphi(v) = w$ (see [**KS07**, Proposition 2.1]. This is also proved in [**Pop94**, Theorem 7.1.12], cf. [**BR97**, Lemma

3.2a].). Thus we can assume that all components of φ are nonzero. Then $\varphi_{\max}\colon V \to W$ is a multihomogeneous covariant, $\dim \varphi_{\max} \leq \dim \varphi$ and $\varphi_{\max}$ is faithful since all its components are non-zero [**KS07**, Lemma 4.1]. □

COROLLARY 2.4. *Let V_i be a faithful irreducible representation of the group G_i, $i = 1, \ldots, n$. Then $V = \oplus_{i=1}^n V_i$ is a faithful representation of $G := G_1 \times \cdots \times G_n$, and there is a minimal multihomogeneous covariant $\varphi\colon V \to V$.* □

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

THEOREM 2.5. *Let G be a finite group and let $V = \oplus_{i=1}^n V_i$ and $W = \oplus_{j=1}^m W_j$ be faithful representations where the V_i and W_j are irreducible submodules. Then there is a minimal rational multihomogeneous covariant $\psi\colon V \to W$ all of whose components are non-zero and which is of the form $\psi = h^{-1}\varphi$ where h is a multihomogeneous invariant and $\varphi\colon V \to W$ a multihomogeneous minimal regular covariant.*

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

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

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

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

$$\psi_{\max} := (\frac{\varphi_1}{h}, \ldots, \frac{\varphi_m}{h})\colon V \to W$$

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

Now assume that $\dim \varphi = \dim \psi + 1$ so that $\overline{\varphi(V)}$ is $\mathbb{C}^*$-stable. If φ is not minimal then there is a minimal homogeneous regular covariant $\tilde{\varphi}$ of dimension $\leq \dim \psi$ and we are again done. Therefore we can assume that φ is minimal, hence $\dim \varphi_{\max} = \dim \varphi$. Since $\overline{{}^t\varphi(V)}$ is $\mathbb{C}^*$-stable for all $t \neq 0$ it follows from Corollary 2.2 that $\overline{\varphi_{\max}(V)}$ is $\mathbb{C}^*$-stable, too, and so

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

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

3. Covariant dimension and essential dimension

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

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

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

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

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

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

$$\tilde{\varphi}\colon v = (v_1, \dots, v_n) \mapsto (f(v)^{\mu_1} \varphi_1(v), \dots, f(v)^{\mu_m} \varphi_m(v)) \tag{4}$$

is a covariant with $\tilde{\varphi}(V) \subset \varphi(V)$, hence $\dim \tilde{\varphi} \leq \dim \varphi$. Moreover, if φ is faithful and f multihomogeneous, then $\tilde{\varphi}$ is faithful and multihomogeneous of degree $\tilde{A} := \mu \deg f + A$, i.e., $\tilde{\alpha}_{ji} = \mu_j \deg_{V_i} f + \alpha_{ji}$.

This has the following application which will be used later in the proof of Corollary 4.4: *Let p be a prime which does not divide the order of the center of G. Then there is a minimal multihomogeneous covariant $\varphi\colon V \to V$ of degree $A \not\equiv 0 \mod p$.*
(Start with a minimal multihomogeneous covariant $\varphi\colon V \to V$ of degree A and assume that $A \equiv 0 \mod p$. We can choose a $\mu \in A\mathbb{Q}^n \cap \mathbb{Z}^m$ such that $\mu_{j_0} \not\equiv 0 \mod p$ for at least one j_0. Moreover, there is a multihomogeneous invariant f of total degree $\not\equiv 0 \mod p$ (see [**KS07**, Lemma 4.3]). But then $\mu \deg f \not\equiv 0 \mod p$, and so the covariant $\tilde{\varphi}$ given in (4) is minimal and has degree $\mu \deg f + A \not\equiv 0 \mod p$.)

For the next results we need some preparation. Let $\varphi\colon V \to W$ be a multihomogeneous faithful covariant of degree $A = (\alpha_{ji})$ where all components φ_j are non-zero. Define $W' := \{(w_1, \dots, w_m) \in W \mid w_i \neq 0 \text{ for all } i\} = \prod_{j=1}^m (W_j \setminus \{0\})$. The group $\mathbb{C}^{*m}$ acts freely on W' and $W' \to \prod_{j=1}^m \mathbb{P}(W_j)$ is the geometric quotient. Let $X := \overline{\varphi(V)}$ and $\mathbb{P}(X) \subset \prod_{j=1}^m \mathbb{P}(W_j)$ the image of X, and set $X' := X \cap W'$. Finally, denote by $S \subset \mathbb{C}^{*m}$ the image of the homomorphism $T(A)\colon \mathbb{C}^{*n} \to \mathbb{C}^{*m}$. Then we have the following.

LEMMA 3.3. *(A)* $\dim \mathbb{P}(X) \leq \dim X - \dim S \leq \dim X - \operatorname{rank} Z(G)$.
(B) The kernel of the action of G on $\mathbb{P}(X)$ is equal to $Z(G)$.

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

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

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

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

$$\operatorname{ed} G \leq \dim \varphi - \operatorname{rank} A \text{ and } \operatorname{cdim} G \leq \dim \varphi - \operatorname{rank} A + 1.$$

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

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

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

$$\operatorname{cdim} G = \operatorname{ed} G + 1.$$

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

PROPOSITION 3.6. *If G has a non-trivial center, then* $\operatorname{cdim} G = \operatorname{ed} G$.

PROOF. Let $\psi\colon V \to V$ be a multihomogeneous minimal rational covariant of degree $A = (\alpha_{ji})$ which is of the form $h^{-1}\varphi$ where $h \in \mathcal{O}(V)^G$ is a multihomogeneous invariant and $\varphi\colon V \to V$ a multihomogeneous regular minimal covariant (Theorem 2.5).

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

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

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

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

$$\operatorname{ed} G = \operatorname{cdim} G = \operatorname{cdim} G/Z(G) = \operatorname{ed} G/Z(G) + 1.$$

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

4. The image of a covariant

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

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

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

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

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

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

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

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

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

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

PROOF. Since the degree matrix $A = (\alpha_{ji})$ exists, no φ_j is zero. Let $m = \dim V_1 + \cdots + \dim V_k$. By Proposition 4.1 the ideal of $\overline{\varphi(V)}$ is generated by functions of the form $F(y_1, \dots, y_m) t_{k+1}^{r_{k+1}} \cdots t_n^{r_n}$ where F is multihomogeneous. Such a function vanishes on $\operatorname{im}\varphi$ if and only if $F(y_1, \dots, y_m)$ vanishes on the image of $(\varphi_1, \dots, \varphi_k)$. Thus the

ideal $\mathcal{I}(\varphi(V))$ is generated by functions not involving $t_{k+1}, \dots, t_n$. As a consequence, $\overline{\varphi(V)} = \overline{(\varphi_1, \dots, \varphi_k)(V)} \times V_{k+1} \times \cdots \times V_n$. □

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

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

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

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

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

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

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

(A) If p is coprime to $|Z(G)|$, then $\operatorname{cdim}(G \times \mathbb{Z}/p) = \operatorname{cdim} G$.

(B) If p divides all $|Z(G_i)|$, then $\operatorname{cdim}(G \times (\mathbb{Z}/p)^m) = \operatorname{cdim} G + m$.

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

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

PROOF. Let V_i be a faithful irreducible representation of G_i. Then $V := V_1 \oplus \cdots \oplus V_n$ is a faithful representation of G. By Corollary 2.4 there is a minimal multihomogeneous faithful covariant $\varphi = (\varphi_1, \dots, \varphi_k)\colon V \to V$ of degree A. For any $\delta = (\delta_1, \dots, \delta_n) \in \mathbb{Z}^n$ there is a linear action of $\mathbb{Z}/p$ on V where the generator $\bar{1} \in \mathbb{Z}/p$ acts by

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

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

Assume now that p divides all $|Z(G_i)|$. There is a minimal multihomogeneous covariant $\psi\colon V \oplus \mathbb{C}^m \to V \oplus \mathbb{C}^m$ for $G \times (\mathbb{Z}/p)^m$ where $(\mathbb{Z}/p)^m$ acts in the obvious way on $\mathbb{C}^m$. Clearly, no entry of ψ is zero and by Corollaries 4.3 and 4.2, we get $\dim \psi = \dim \varphi + m$

where $\varphi\colon V \oplus \mathbb{C}^m \to V$ is ψ followed by projection to V. Since each component of φ is nonzero, φ is faithful for G [**KS07**, Lemma 4.1]. Thus $\dim \varphi \geq \operatorname{cdim} G$. But clearly, $\operatorname{cdim}(G \times (\mathbb{Z}/p)^m) \leq \operatorname{cdim} G + m$, hence we have equality, proving (2). □

As an immediate consequence we get the following result.

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

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

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

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

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

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

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

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

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

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

Similarly, condition (i) implies that

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

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

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

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

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

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

$$G = \{(g', \xi) \in G' \times \mu_{p^\ell} \mid \chi'(g') = \pi(\xi)\}$$

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

5. Some examples

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6. Faithful Groups

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

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

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

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

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

LEMMA 6.3. *Let $N_1, \dots, N_k$ be the minimal nontrivial normal abelian subgroups of a finite group G. Then*

(A) Each N_i is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$ for some $n \in \mathbb{N}$ and prime p.

(B) Let L be a G-normal subgroup of N_G. There is a direct product M of a subset of $\{N_1, \dots, N_k\}$ such that N_G is the direct product LM.

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

COROLLARY 6.4. *N_G is a direct product of a subset of $\{N_1, \dots, N_k\}$, hence N_G is abelian.* □

PROOF OF COROLLARY 6.2. The subgroup $N_G \cap N_H \subset N_H$ is normal in H. By Lemma 6.3 it has a complement M. Now assume that H is faithful. Then by Proposition 6.1 there exists an element $(c, d) \in N_H = (N_G \cap N_H) \times M$ whose H-conjugacy class generates N_H. Then the H-conjugacy class of c generates $N_G \cap N_H$. Now let N_i be one of the minimal nontrivial normal abelian subgroups of G. By hypothesis, $N_i \subset H$, hence N_i contains a minimal nontrivial H-submodule N'. Then $N' \subset N_G \cap N_H$. The smallest G-stable subspace of N_G containing N' is N_i, hence N_i lies in the G-submodule of N_G generated by the conjugacy class of c. Since N_i is arbitrary, we see that G is faithful. □

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

7. Groups of covariant dimension 2

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

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

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

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

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

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

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

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

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

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

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

Now we can finish the proof. The case that $G = G_2$ is handled in [**KS07**, Lemma 10.2], so we can assume that G' is non-trivial. If G_2 commutes with G', then G_2 is non-commutative and faithful. Moreover, no G_p can be of rank 2, else we have a subgroup which is a product $H := G_2 \times (\mathbb{Z}/p)^2$, and we have $\operatorname{cdim} H \geq 3$ by Corollary 4.4. So G' has rank 1. Then G' is cyclic, hence G is faithful by Remark 6.5, which is a contradiction. Hence we may assume that G_2 acts nontrivially 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 nontrivially 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 nontrivially on N_{G_p}. Since G is not faithful, N_G is not generated by a conjugacy class (Proposition 6.1) and the same holds for the subgroup

$H := \langle g, N_2 \rangle \ltimes N'$ (Corollary 6.2). Thus H is neither faithful nor commutative, so that it must equal G by minimality. It follows that each nontrivial G_p, for $p \neq 2$, is isomorphic to either $\mathbb{Z}/p$ or $(\mathbb{Z}/p)^2$.

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

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

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

8. Errata to [KS07]

First sentence after Definition 4.1. Replace "simple groups." by "nonabelian simple groups."
Proof of Proposition 4.3, second paragraph. Replace "is divisible by m" with "is congruent to 1 mod m."
Proof of Corollary 5.1 last sentence. Replace "Corollary 4.3" by "Proposition 4.3."
Proof of Proposition 6.1 second paragraph. Change "$\varphi|_W$" to $F|_W$."
Proof of Proposition 6.1 first displayed formula. Replace "$F(w,t)$" and "$F_0(w,t)$" by "$F(w,t^m)$" and "$F_0(w,t^m)$."
Top of page 282. Change "trivial stabilizer" to "trivial stabilizer or stabilizer $\pm I$."

Bibliography

[BR97] J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), no. 2, 159–179.

[CLO07] David Cox, John Little, and Donal O'Shea, *Ideals, varieties, and algorithms*, third ed., Undergraduate Texts in Mathematics, Springer, New York, 2007, An introduction to computational algebraic geometry and commutative algebra.

[Flo08] Mathieu Florence, *On the essential dimension of cyclic p-groups*, Invent. Math. **171** (2008), no. 1, 175–189.

[Gas54] Wolfgang Gaschütz, *Endliche Gruppen mit treuen absolut-irreduziblen Darstellungen*, Math. Nachr. **12** (1954), 253–255.

[JLY02] Christian U. Jensen, Arne Ledet, and Noriko Yui, *Generic polynomials*, Mathematical Sciences Research Institute Publications, vol. 45, Cambridge University Press, Cambridge, 2002, Constructive aspects of the inverse Galois problem.

[KM08] Nikita A. Karpenko and Alexander S. Merkurjev, *Essential dimension of finite p-groups*, Invent. Math. **172** (2008), no. 3, 491–508.

[KS07] Hanspeter Kraft and Gerald W. Schwarz, *Compression of finite group actions and covariant dimension*, J. Algebra **313** (2007), no. 1, 268–291.

[Led07] Arne Ledet, *Finite groups of essential dimension one*, J. Algebra **311** (2007), no. 1, 31–37.

[Löt08] Roland Lötscher, *Application of multihomogeneous covariants to the essential dimension of finite groups*, arXiv:0811.3852.

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

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

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

[Stu96] Bernd Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series, vol. 8, American Mathematical Society, Providence, RI, 1996.

HANSPETER KRAFT, ROLAND LÖTSCHER, MATHEMATISCHES INSTITUT DER UNIVERSITÄT BASEL, RHEINSPRUNG 21, CH-4051 BASEL, SWITZERLAND

Email adresses: `Hanspeter.Kraft@unibas.ch, Roland.Loetscher@unibas.ch`

GERALD W. SCHWARZ, DEPARTMENT OF MATHEMATICS, BRANDEIS UNIVERSITY, PO BOX 549110, WALTHAM, MA 02454-9110

Email adress: `Schwarz@brandeis.edu`

CHAPTER III

Faithful and p-faithful representations of minimal dimension

Throughout sections 1-3 of this chapter all groups are finite and k is an arbitrary field (not necessarily infinite). All $\mathbb{Z}G$-modules for a group G will be assumed to be of finite order. In section 1 we relate faithfulness of representations of a group G with the $\mathbb{Z}G$-module structure of a certain abelian subgroup, called the *abelian socle* of G. In section 2 we compute the minimal number of irreducible components needed for a faithful representation of any semi-faithful group. Recall that a group is called semi-faithful (over k) if it admits a faithful completely reducible representation (over k). As a consequence we obtain a characterization of groups, which have a faithful representation with any fixed number of irreducible components. Groups admitting an irreducible faithful representation over an algebraically closed field of characteristic 0 have been characterized in [**Ga54**]. In section 3 we investigate faithful representations of minimal dimension.

In section 4 the letter G denotes an algebraic group over an algebraically closed field of characteristic 0, whose connected component G^0 is a torus and whose component group G/G^0 is a p-group. We study representations with finite kernel of order prime to p and relate these to faithful representations of a finite p-subgroup of G.

1. Faithful representations and the abelian socle

DEFINITION 1.1. A *foot* of G is a minimal nontrivial normal subgroup of G. The subgroup of G generated by the abelian feet of G is called the abelian *socle of* G, denoted by $\mathrm{soc}^{\mathrm{ab}}(G)$. The subgroup of G generated by all feet of G is called the socle of G, denoted by $\mathrm{soc}(G)$.

The following lemma is well known and a generalization to countable groups can be found in [**BH08**].

LEMMA 1.2. $\mathrm{soc}(G) = \mathrm{soc}^{\mathrm{ab}}(G) \times N_1 \times \cdots \times N_r$, *where* $N_1, \ldots, N_r$ *are all the non-abelian feet of* G.

By construction $\mathrm{soc}(G)$ and $\mathrm{soc}^{\mathrm{ab}}(G)$ are normal subgroups of G. The abelian socle has a $\mathbb{Z}G$-module structure induced by the conjugation action of G. Since the abelian feet are simple $\mathbb{Z}G$-modules A is semi-simple. The following result contains the crucial observation for our study of faithful representations and will be used in sections 2 and 3. For a $\mathbb{Z}G$-module A we denote by $A^* := \mathrm{Hom}(A, \bar{k}^*)$ its group of characters over $\bar{k}$, which becomes a $\mathbb{Z}G$-module by endowing $\bar{k}^*$ with the trivial G-action.

PROPOSITION 1.3. *Let* $V = \bigoplus_{i=1}^m V_i$ *be a completely reducible* kG*-module. Let* $A := \mathrm{soc}^{\mathrm{ab}}(G)$ *and choose for every* i *some character* $\chi_i \in A^*$ *appearing in* $V_i|_A \otimes \bar{k}$. *Then* V *is*

faithful if and only if the characters $\chi_1, \ldots, \chi_m$ generate A^* as a $\mathbb{Z}G$-module, $\operatorname{char} k \nmid |A|$, *and no nonabelian foot of G is in the kernel of V.*

In the sequel for a $\mathbb{Z}G$-module A we denote by $\operatorname{rank}_{\mathbb{Z}G}(A)$ the least number of generators:

$$\operatorname{rank}_{\mathbb{Z}G}(A) := \min\{r \in \mathbb{N}_0 \mid \exists a_1, \ldots, a_r \in A : \langle a_1, \ldots, a_r\rangle_{\mathbb{Z}G} = A\} \in \mathbb{N}_0$$

and by $L(A)$ the lattice of $\mathbb{Z}G$-submodules of A, where the meet-operation is given by $B \cap C$ and the join-operation by $B + C$. Note that the word lattice is used here in a different way than elsewhere, where a $\mathbb{Z}G$-lattice is a free abelian group of finite rank with a linear action of G.

For the proof of Proposition 1.3 we work with the lattices $L(A)$ and $L(A^*)$ where $A = \operatorname{soc}^{\mathrm{ab}}(G)$. In general $L(A)$ and $L(A^*)$ are related as follows:

Lemma 1.4. *Let A be a semi-simple $\mathbb{Z}G$-module. Assume that either* $\operatorname{char} k = 0$ *or* $\operatorname{char} k = p > 0$ *and* $p \nmid |A|$.

(A) The map

$$\alpha\colon L(A^*) \to L(A), \quad \mathcal{L} \mapsto \{a \in A \mid \ell(a) = 1\ \forall \ell \in \mathcal{L}\}$$

is an anti-isomorphism between $L(A^*)$ and $L(A)$ with inverse given by $\alpha^{-1}(B) = \{\ell \in A^* \mid \ell(a) = 1\ \forall a \in A\}$.

(B) There exists a (non-canonical) isomorphism of lattices

$$\beta\colon L(A) \xrightarrow{\simeq} L(A^*)$$

which preserves size, i.e. $|\beta(B)| = |B|$ for all $B \in L(A)$.

(C) $\operatorname{rank}_{\mathbb{Z}G}(A) = \operatorname{rank}_{\mathbb{Z}G}(A^*)$.

Proof. (A) The proof is straightforward.

(B) Since A is semi-simple it decomposes into isotypic components. Every submodule of A is isomorphic to the direct sum of its intersections with the isotypic components and it suffices to show the claim for every isotypic component of A. Thus assume $A = (\mathbb{F}_q)^m \otimes V$ for some prime q with $q \neq \operatorname{char} k$, some natural number m and some irreducible $\mathbb{F}_qG$-module V, where $(\mathbb{F}_q)^m$ is equipped with the trivial action of G. We may identify $A^* = (\mathbb{F}_q)^m \otimes V^*$. Every $\mathbb{Z}G$-submodule of A is now of the form $W \otimes V$ for some sub vector-space $W \subset \mathbb{F}_q^m$. Define $\beta\colon L(A) \to L(A^*)$ by $\beta(W \otimes V) = W \otimes V^*$. Then β is an isomorphism of lattices and preserves size, since the assumption $p \nmid |A|$ implies $|V^*| = |V|$.

(C) Let $E_r \subseteq A$ for $r \in \mathbb{N}$ denote the (possibly empty) set of generating r-tuples of the $\mathbb{Z}G$-module A and let $\max(L(A))$ be the set of maximal non-trivial elements of $L(A)$. The two sets are related by:

$$E_r = A^r \setminus \bigcup_{M \in \max(L(A))} M^r.$$

Similarly for $E_r^* \subseteq A^*$ and $\max(L(A^*))$ defined correspondingly with A^* in place of A we have

$$\begin{aligned} E_r^* &= (A^*)^r \setminus \bigcup_{\mathcal{L}\in\max(L(A^*))} \mathcal{L}^r \\ &= (\beta(A))^r \setminus \bigcup_{M\in\max(L(A))} (\beta(M))^r \end{aligned}$$

We claim for any r that $|E_r| = |E_r^*|$. This implies in particular that A is generated by r elements if and only if A^* is, hence $\operatorname{rank}_{\mathbb{Z}G}(A) = \operatorname{rank}_{\mathbb{Z}G}(A^*)$. The claim follows from part (B) and the exclusion principle, which says that for subsets $Y_1, \ldots, Y_t$ of a set Y we have

$$|Y \setminus \cup_{i=1}^t Y_i| = |Y| - \sum_{i=1}^{t} (-1)^{t+1} \sum_{\nu_1<\cdots<\nu_i} |Y_{\nu_1} \cap \cdots \cap Y_{\nu_i}|$$

□

For the case that k is not algebraically closed, we need to deal with irreducible representations which are not absolutely irreducible. Let A be an elementary abelian q-group where q is a prime, $q \neq \operatorname{char} k$. We claim that the group algebra kA decomposes as

$$kA = \bigoplus_{H\subseteq A} V_H$$

where H runs over all cyclic subgroups of A^* and

$$V_{\langle\chi\rangle} := \left\{ \sum_{i\in\mathbb{F}_q^*} \gamma_i \sum_{\chi(a)=i} a \in kA \mid \gamma_i \in k, \sum_{i\in\mathbb{F}_q^*} \gamma_i = 0 \right\}$$

for $\chi \neq 1$ and

$$V_{\langle 1\rangle} = k \sum_{a\in A} a.$$

In fact every V_H is a kA-submodule of kA. Over $\bar{k}$ the group algebra $\bar{k}A$ decomposes into the direct sum of all characters of A. Since $V_{\langle\chi\rangle} \otimes_k \bar{k}$ decomposes into the direct sum of the characters $\chi, \chi^2, \ldots, \chi^{q-1}$ the claim follows.

Now consider an abelian group A, which decomposes as $A = \prod_{i=1}^m A_{q_i}$ where $q_1, \ldots, q_m$ are distinct primes, $q_1, \ldots, q_m \neq \operatorname{char} k$, and A_{q_i} is an elementary abelian q_i group.

LEMMA 1.5. *Let $\chi_1, \ldots, \chi_r$ be the characters appearing in the decomposition over $\bar{k}$ of an irreducible kA-module V. Then $\langle\chi_i\rangle = \langle\chi_j\rangle$ for every $1 \leq i, j \leq r$.*

PROOF. Since the group algebras kA_{q_i} are of coprime dimensions and $kA \simeq kA_{q_1} \otimes \cdots \otimes kA_{q_m}$ the kA-module V is an exterior tensor product of irreducible kA_{q_i}-modules for $i = 1 \ldots m$. Hence it suffices to consider the case $m = 1$. In that case the claim follows from the decomposition $V = \bigoplus V_H$ above. □

In the sequel for a character $\chi \in \operatorname{Hom}(A, \bar{k}^*)$ of a group A we will denote by $\bar{k}_\chi$ the one-dimensional A-module over $\bar{k}$ on which A acts via χ.

PROOF OF PROPOSITION 1.3. Clearly if a non-abelian foot of G is contained in the kernel of V, then V is not faithful. We have $\operatorname{char} k \nmid |A|$ in both sides of the equivalence statement to prove (for the first statement when V is faithful see the remark after Definition 3.10 of Chapter I).

Set $\mathcal{L} := \langle \chi_1, \cdots, \chi_m \rangle_{\mathbb{Z}G} \in L(A^*)$. First suppose that $\mathcal{L} \neq A^*$. We must show that V is not faithful. Let α be the lattice anti-isomorphism from Lemma 1.4(A) and set $B := \alpha(\mathcal{L}) \subseteq A$, which is then a non-trivial normal subgroup of A contained in the kernel of each χ_i and of any power of χ_i. Let W_i be any irreducible sub-representation of $V_i|_A$ containing $\overline{k}_{\chi_i}$ over $\bar{k}$. By Lemma 1.5 $W_i \otimes \bar{k} = \sum \bar{k}_{\chi_i^{\alpha_{ij}}}$ for some $\alpha_{ij} \in \mathbb{N}$. Therefore B acts trivially on W_i. Now since V_i is irreducible, $V_i = \sum_{g \in G} gW_i$ as vector spaces. For $b \in B$ and $w \in W_i$ we have $bgw = g(g^{-1}bg)w = gw$, since B is normal. Thus B acts trivially on V. Hence V is not faithful.

Conversely assume that V is not faithful and no nonabelian foot of G is in the kernel of V. Hence some abelian foot B is in the kernel of V. This implies that B lies in the kernel of each χ_i, whence in the kernel of each element of $\mathcal{L}$. This implies that $\mathcal{L} \neq A^*$. □

2. A generalization of Gaschütz' theorem

Gaschütz's theorem says that a finite group G admits a faithful irreducible complex representation if and only if $\operatorname{soc}^{\mathrm{ab}}(G)$ is generated by the conjugacy class of one of its elements, or equivalently, if and only if $\operatorname{rank}_{\mathbb{Z}G}(\operatorname{soc}^{\mathrm{ab}}(G)) \leq 1$. We have the following generalization:

THEOREM 2.1. *Let G be a semi-faithful group. Then the minimal number of factors of a decomposition series of a faithful representation of G over k equals* $\operatorname{rank}_{\mathbb{Z}G} \operatorname{soc}^{\mathrm{ab}}(G)$ *if* $\operatorname{soc}^{\mathrm{ab}}(G) \neq \{e\}$, *and equals* 1 *otherwise. Moreover the minimum is attained by a completely reducible representation.*

REMARK 2.2. A criterion for a group to admit a faithful representation with any fixed number of irreducible components was given by Shoda [**Sh30**] (in good characteristic) and Nakayama [**NA**] (in positive characteristic). Their criterion is equivalent to Theorem 2.1 but this is not easy to verify directly.

We start with a lemma explaining how to pass from arbitrary to completely reducible representations.

LEMMA 2.3. *Assume that* $\operatorname{char} k = p > 0$. *Let V be a faithful representation of G. If G does not contain any nontrivial normal subgroup of p-power order, then the direct sum of the irreducible decomposition factors of V is faithful as well. Moreover the following conditions are equivalent:*

(i) G is semi-faithful (over k).
(ii) G does not contain any nontrivial normal p-subgroups.
(iii) $p \nmid |\operatorname{soc}^{\mathrm{ab}}(G)|$.

PROOF. The first statement and the equivalence of (i) and (ii) were observed in Chapter I, Proposition 3.11. The implication (iii) $\Rightarrow$ (ii) follows from the fact that every nontrivial p-group has a nontrivial abelian characteristic subgroup. The converse is clear. □

PROOF OF THEOREM 2.1. By Lemma 2.3 the order of $A = \mathrm{soc}^{\mathrm{ab}}(G)$ is not divisible by $\mathrm{char}\, k$ in case $\mathrm{char}\, k > 0$.

Let V be a faithful representation of G over k. We want to show that the number of factors of a decomposition series of V is at least the maximum of $\mathrm{rank}_{\mathbb{Z}G}(A)$ and 1. Clearly it is at least 1. By Lemma 2.3 we may assume that V is completely reducible. Proposition 1.3 implies that the number of irreducible components of V is at least $\mathrm{rank}_{\mathbb{Z}G}(A^*)$, which equals $\mathrm{rank}_{\mathbb{Z}G}(A)$ by Lemma 1.4(C).

Conversely we must construct a faithful representation V over k with at most $\mathrm{rank}_{\mathbb{Z}G}(A)$ irreducible components if A is non-trivial, and a faithful irreducible representation V over k if A is trivial. We first reduce to the case of k being algebraically closed: Assume that $\bigoplus_{i=1}^n V_i$ is a decomposition of a faithful representation into irreducible representations over $\bar{k}$. For each i take any irreducible representation V_i' over k which contains V_i as a decomposition factor over $\bar{k}$. Then $\bigoplus_{i=1}^n V_i'$ is a faithful representation over $\bar{k}$ and has the same number of irreducible components.

Let $N_1, \ldots, N_t$ be the non-abelian feet of G. By Lemma 1.2 the socle of G decomposes as $\mathrm{soc}\, G = A \times N_1 \times \ldots \times N_t$. For each i, since N_i has composite order it has a nontrivial irreducible representation W_i. The (exterior) tensor product $W := W_1 \otimes \cdots \otimes W_t$ is then irreducible (since $k = \bar{k}$) and does not contain any of $N_1, \cdots, N_t$ in its kernel. If A is trivial this gives an irreducible representation of $\mathrm{soc}\, G$ with the property that no foot of G is contained in its kernel. Any irreducible representation whose restriction to $\mathrm{soc}\, G$ contains W (take e.g. an irreducible sub-representation of the induced G-module $\mathrm{ind}_{\mathrm{soc}\, G}^G W$) is then faithful.

From now on assume A to be non-trivial. There exist $r := \mathrm{rank}_{\mathbb{Z}G}(A^*) = \mathrm{rank}_{\mathbb{Z}G}(A)$ characters $\chi_1, \ldots, \chi_r$ of A which generate the $\mathbb{Z}G$-module A^*. For every i choose an irreducible representation V_i of G whose restriction to $\mathrm{soc}\, G$ contains the irreducible representation $k_{\chi_i} \otimes W$. Set $V := \bigoplus_{i=1}^r V_i$. By Proposition 1.3 the representation V is faithful. Moreover it has the required number of irreducible components. This finishes the proof. □

REMARK 2.4. The situation for non-semi-faithful groups is completely different, in so far that the abelian socle tells us nothing about the number of decomposition factors needed for a faithful representation. Take for example a field k of characteristic p and consider the groups $G_n = \mathbb{Z}/p^n\mathbb{Z}$, $n \geq 1$. The abelian socle of G_n is the group of order p with trivial G_n-conjugation action. However $\mathrm{GL}_m(k)$ only admits elements of order p^n when $m \geq p^{n-1} + 1$. Since the only irreducible representation of G_n over k is the trivial representation, this implies that one needs at least $p^{n-1} + 1$ decomposition factors for a faithful representation of G_n.

REMARK 2.5. Let Γ be any subgroup of $\mathrm{Aut}(G)$ containing the inner automorphisms. A representation ρ of G is said to be Γ-faithful if the only Γ-invariant subgroup of $\ker \rho$

is the trivial group. One can define Γ-feet, Γ-socle, abelian Γ-socle (denoted in the sequel by $A^\Gamma(G)$) by replacing normal subgroups by Γ-invariant subgroups (see [**BH08**]) and generalize Theorem 2.1 in the following way: If $\operatorname{char} k = 0$ or $\operatorname{char} k = p > 0$ and $p \nmid |A^\Gamma(G)|$, then the minimal number of irreducible components of a completely reducible Γ-faithful representation of G equals the maximum of $\operatorname{rank}_{\mathbb{Z}\Gamma} A^\Gamma(G)$ and 1. The proof remains basically the same.

There is the following application:

COROLLARY 2.6. *Let $n \in \mathbb{N}$ and $H \subseteq G$ be a subgroup containing $\operatorname{soc}^{\mathrm{ab}}(G)$ and assume that H and G are semi-faithful. If H has a faithful representation over k with n decomposition factors, then G has a faithful representation with n decomposition factors as well.*

PROOF. This is a consequence of Theorem 2.1 and Lemma 2.7 below. □

LEMMA 2.7. *If $H \subseteq G$ is a subgroup containing $\operatorname{soc}^{\mathrm{ab}}(G)$, then $\operatorname{rank}_{\mathbb{Z}H} \operatorname{soc}^{\mathrm{ab}}(H) \geq \operatorname{rank}_{\mathbb{Z}G} \operatorname{soc}^{\mathrm{ab}}(G)$.*

PROOF. Let $h_1, \ldots, h_r$ generate $\operatorname{soc}^{\mathrm{ab}}(H)$ as a $\mathbb{Z}H$-module, where $r = \operatorname{rank}_{\mathbb{Z}H}(\operatorname{soc}^{\mathrm{ab}}(H))$. By semi-simplicity of $\operatorname{soc}^{\mathrm{ab}}(H)$ the $\mathbb{Z}H$-submodule $\operatorname{soc}^{\mathrm{ab}}(H) \cap \operatorname{soc}^{\mathrm{ab}}(G)$ has an H-invariant complement N in $\operatorname{soc}^{\mathrm{ab}}(H)$. Write $h_i = (g_i, n_i)$ where $n_i \in N$ and $g_i \in \operatorname{soc}^{\mathrm{ab}}(H) \cap \operatorname{soc}^{\mathrm{ab}}(G)$. Then $g_1, \ldots, g_r$ generate $\operatorname{soc}^{\mathrm{ab}}(H) \cap \operatorname{soc}^{\mathrm{ab}}(G)$ as a $\mathbb{Z}H$-module. It suffices to show that $g_1, \ldots, g_r$ generate $\operatorname{soc}^{\mathrm{ab}}(G)$ as a $\mathbb{Z}G$-module. Let A be any abelian foot of G. By assumption $A \subseteq \operatorname{soc}^{\mathrm{ab}}(G) \subseteq H$. Let $B \subseteq A$ be a H-foot. By construction $B \subseteq \operatorname{soc}^{\mathrm{ab}}(H) \cap \operatorname{soc}^{\mathrm{ab}}(G)$, which is generated by $g_1, \ldots, g_r$ as a $\mathbb{Z}H$-module. Since A is minimal, the $\mathbb{Z}G$-module generated by B equals A. Hence A is contained in the $\mathbb{Z}G$-module generated by $g_1, \ldots, g_r$. Since this holds for every abelian foot A of G the claim follows. □

3. Minimal dimension of faithful representations

We define the *representation dimension* of G over k as follows:

DEFINITION 3.1. $\operatorname{rdim}_k G := \min\{\dim V \mid V \text{ faithful } G\text{-module over } k\}$.

This numerical invariant gives an upper bound for $\operatorname{ed}_k G$. In certain cases the two invariants of G coincide, e.g. for p-groups when k contains a primitive p-th root of unity [**KM**, Theorem 4.1].

In Chapter I we have defined the notion $\operatorname{Rep}^{(\chi)}(G)$ for characters χ of a central diagonalizable subgroup of an algebraic group G. The following definition is an analog for arbitrary abelian subgroups of a finite group G.

DEFINITION 3.2. Let A be an abelian subgroup of G and $\chi \in A^* := \operatorname{Hom}(A, \bar{k}^*)$.

$$\operatorname{Rep}^{(\chi)}(G) := \{V \text{ irreducible } G\text{-module} \mid (V \otimes \bar{k})|_A \supseteq \bar{k}_\chi\}$$

To every group G and field k we associate the following function:

$$f_{G,k} \colon A^* \to \mathbb{N}_0, \quad \chi \mapsto \min\{\dim V \mid V \in \operatorname{Rep}^{(\chi)}(G)\},$$

where $A = \mathrm{soc}^{\mathrm{ab}}(G)$.

Proposition 1.3 has the following corollary:

COROLLARY 3.3. *If the socle $C = \operatorname{soc} G$ of G is abelian and $\operatorname{char} k \nmid |C|$, then*

$$\operatorname{rdim}_k G = \min\left\{\sum_{i=1}^{r} f_{G,k}(\chi_i)\right\}$$

taken over all $r \in \mathbb{N}$ and all systems of generators $(\chi_1, \ldots, \chi_r)$ of C^* viewed as a $\mathbb{Z}G$-module.

It may happen that G has a faithful representation with d decomposition factors but every faithful representation of minimal dimension has at least $d+1$ decomposition factors. However in the following situation that doesn't occur and we can describe faithful representations of minimal dimension more precisely. Recall the definition of a minimal basis introduced in [**KM**]:

DEFINITION 3.4. Let C be a vector space over some field F of dimension $r \in \mathbb{N}_0$ and let $f\colon C \to \mathbb{N}_0$ be a function. An F-basis $(c_1, \ldots, c_r)$ of C is called *minimal relative to f* if

$$f(c_i) = \min\left\{f(c) \mid c \in C \setminus \langle c_1, \ldots, c_{i-1}\rangle\right\}, \tag{5}$$

for $i = 1, \ldots, r$ where for $i = 1$ we use the convention that the span of the empty set is the trivial vector space $\{0\}$.

PROPOSITION 3.5. *Let G be a group whose socle $C := \operatorname{soc} G$ is a central p-subgroup for some prime p and assume $\operatorname{char} k \neq p$. Let V be any representation of G and let $V_1, V_2, \ldots, V_r$ be its irreducible composition factors where $\dim V_{i+1} \geq \dim V_i$ for all i. Let $\chi_1, \ldots, \chi_r \in C^* = \operatorname{Hom}(C, \bar{k}^*)$ be characters such that $V_i \in \operatorname{Rep}^{(\chi_i)}(G)$. Then V is faithful of dimension $\operatorname{rdim}_k G$ if and only if $r = \operatorname{rank} C$ and $(\chi_1, \ldots, \chi_r)$ forms a minimal basis of $(C^*, f_{G,k})$ with $f_{G,k}(\chi_i) = \dim V_i$. The dimension vector $(\dim V_1, \ldots, \dim V_r)$ does not depend on the choice of a faithful representation V of dimension $\operatorname{rdim}_k G$.*

PROOF. By Lemma 2.3 since $\operatorname{char} k \nmid |C|$ we may replace V by its associated graded representation $V_1 \oplus \ldots \oplus V_r$ without changing faithfulness, decomposition factors and dimension. Thus we will assume that V is completely reducible.

First assume that V is faithful and $\operatorname{rdim}_k G = \dim V$. By Proposition 1.3 faithfulness of V is equivalent to the statement that the characters $\chi_1, \ldots, \chi_r$ generate C^*. Since V has minimal dimension it follows that $r = \operatorname{rank} C$. Let $j \in \{0, \ldots, r\}$ be maximal such that $(\chi_1, \ldots, \chi_r)$ is part of a minimal basis of C^*. We want to show that $j = r$. Assume to the contrary that $j < r$. Hence there exists $\chi \in C^* \setminus \langle \chi_1, \ldots \chi_j\rangle$ and $W \in \operatorname{Rep}^{(\chi)}(G)$ such that $\dim W < \dim V_i$ for all $i > j$. By elementary linear algebra there exists $i > j$ such that $\chi_1, \ldots, \chi_{i-1}, \chi, \chi_{i+1}, \ldots, \chi_r$ generate C^* as well. Let $V' := V_1 \oplus \cdots V_{i-1} \oplus W \oplus V_{i+1} \oplus \cdots \oplus V_r$. Then $\dim V' < \dim V$ and V' is faithful, because V' is faithful restricted to C and every normal subgroup of G intersects $C = \operatorname{soc}(G)$. This contradicts $\dim V = \operatorname{rdim}_k G$.

Now assume that $(\chi_1, \dots, \chi_r)$ and $(\chi'_1, \dots, \chi'_r)$ form two minimal bases of C^*. We show that $f_{G,k}(\chi_i) = f_{G,k}(\chi'_i)$ for all $i = 1 \dots r$. Let $j \in \{0, \dots, r\}$ be the last index where $(f_{G,k}(\chi_1), \dots, f_{G,k}(\chi_j))$ and $(f_{G,k}(\chi'_1), \dots, f_{G,k}(\chi'_j))$ coincide. Assume $j < r$ and $f_{G,k}(\chi'_{j+1}) < f_{G,k}(\chi_{j+1})$. Then $\langle \chi_1, \dots, \chi_j \rangle \neq \langle \chi'_1, \dots, \chi'_j \rangle$. Hence there exists $s \in \{1, \dots, j\}$ such that $\chi'_s \notin \langle \chi_1, \dots, \chi_j \rangle$. Then $f_{G,k}(\chi_{j+1}) > f_{G,k}(\chi'_{j+1}) \geq f_{G,k}(\chi'_s)$, which contradicts the definition of minimal basis. This implies uniqueness of the dimension vector. Moreover it follows that V has dimension $\operatorname{rdim}_k G$ when $(\chi_1, \dots, \chi_r)$ forms a minimal basis of $(C^*, f_{G,k})$ and $\dim V_i = f_{G,k}(\chi_i)$ for all i. □

Corollary 3.6. *Let p be a prime and $G_1, \dots, G_n$ be groups. Assume that* $\operatorname{char} k \neq p$ *and* $\operatorname{soc} G_l$ *is a central p-subgroup of G_l for $l = 1, \dots, n$. Then*

$$\operatorname{rdim}_k \prod_{l=1}^{n} G_l = \sum_{l=1}^{n} \operatorname{rdim}_k G_l.$$

The (statement and the) proof is very similar to [**KM**, Theorem 5.1] and Theorem 8.1 of Chapter IV. Since our situation is more general and we do not require k to contain a primitive p-th root of unity, we include a short proof.

Proof. By induction it suffices to settle the case $n = 2$. Set $G := G_1 \times G_2$. Taking into account the description of minimal faithful representations of Proposition 3.5 it remains to create a minimal basis $(\chi_1, \dots, \chi_r)$ of $(\operatorname{soc} G)^* = (\operatorname{soc} G_1)^* \oplus (\operatorname{soc} G_2)^*$ for $f_{G,k}$ subject to the condition that each χ_i is contained in one of $(\operatorname{soc} G_l)^*$. Here $r = \operatorname{rank} Z(G) = \operatorname{rank} Z(G_1) + \operatorname{rank} Z(G_2)$. Assume that $(\chi_1, \dots, \chi_j)$ is part of a minimal basis such that each χ_i for $i \leq j$ is contained in one of $(\operatorname{soc} G_l)^*$. Choose $\chi \in (\operatorname{soc} G)^* \setminus \langle \chi_1, \dots, \chi_j \rangle$ with $f_{G,k}(\chi)$ minimal. Decompose χ as $\chi^{(1)} \oplus \chi^{(2)}$ where $\chi^{(l)} \in (\operatorname{soc} G_l)^*$ and choose $W \in \operatorname{Rep}^{(\chi)}(G)$ of minimal dimension. The definition of $\operatorname{Rep}^{(\chi)}(G)$ tells us that $\bar{k}_\chi \subseteq W \otimes \bar{k}$. Let ε_1 and ε_2 denote the endomorphism of G sending (g_1, g_2) to (g_1, e) and to (e, g_2), respectively. The module of the representation $\rho_W \circ \varepsilon_i$ contains $\bar{k}_{\chi^{(l)}}$ over $\bar{k}$ and has the same dimension as W. Now replace χ by $\chi^{(l)}$ with l such that $\chi^{(l)}$ lies outside the subgroup of $(\operatorname{soc} G)^*$ generated by $\chi_1, \dots, \chi_j$. This proves the claim. □

4. Minimal p-faithful representations of extensions of p-groups by tori

Throughout this section we fix a prime p and work over an algebraically closed field k of characteristic 0. The symbol ζ_m for $m \in \mathbb{N}$ denotes a primitive root of unity in k of order m. We assume that

$$\zeta_{rm}^r = \zeta_m$$

for $r \in \mathbb{N}$. For a commutative algebraic group G we write $G[m]$ for the m-torsion subgroup $G[m] := \{g \in G \mid g^m = e\}$. If G is diagonalizable we write $X^*(G)$ and $X_*(G)$ for the character (resp. co-character)-group of G.

We consider an algebraic group G which fits into an exact sequence

$$1 \to T \to G \xrightarrow{\pi} H \to 1,$$

where T is a torus and H is a (finite) p-group. In other words G is an extension of a p-group H by a torus T. We will always consider T as a closed subgroup of G.

A (rational) representation $\rho\colon G \to \mathrm{GL}(V)$ is called *p-faithful* if its kernel is finite and has order prime to p.

The class of p-faithful representations of extensions G of p-groups by tori (over more general fields) will play an important role in Chapter IV as well. In fact the discussion of this section is related to section 5 of Chapter IV where we show that for every irreducible G-module V there exists a (finite) p-subgroup F of G such that the restriction of V to F is irreducible. In this section we will find F such that every F-module W can be lifted to G after modifying W with the help of suitable characters of $T \cap F$. In the sequel we will denote by G a fixed extension of a p-group H by a torus T. Our goal is to prove the following result:

THEOREM 4.1. *There exists a (finite) p-subgroup $F \subseteq G$ such that the least dimension of a faithful representation of F equals the least dimension of a p-faithful representation of G.*

REMARK 4.2. Theorem 4.1 implies the lower bound on the essential dimension of G formulated in Theorem 1.3(a) of Chapter IV in case k is algebraically closed and of characteristic 0.

We have another description of p-faithfulness for extensions of p-groups by tori, which will become useful later:

LEMMA 4.3. *A closed normal subgroup N of G is finite of order prime to p if and only if its intersection with $Z(G)[p]$ is trivial.*

PROOF. This is a special case of Proposition 4.4 of Chapter IV. □

We need some group-theoretic preliminaries:

LEMMA 4.4. *Let $r \in \mathbb{N}$ be such that $p^r \geq |H|$. Then there exists a set-theoretic section $s\colon H \to G$ of π such that the associated cocycle $\alpha_s\colon H \times H \to T$ given by $\alpha_s(h, h') = s(hh')^{-1}s(h)s(h')$ has values in $T[p^r]$. Moreover in that case the subgroup G_r of G generated by $T[p^r]$ and $s(H)$ fits into a commutative diagram with exact rows:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & T & \longrightarrow & G & \longrightarrow & H & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \| & & \\ 1 & \longrightarrow & T[p^r] & \longrightarrow & G_r & \longrightarrow & H & \longrightarrow & 1 \end{array}$$

where $T[p^r] \hookrightarrow T$ and $G_r \hookrightarrow G$ are the inclusion morphisms. In particular G_r is a p-subgroup of G.

PROOF. This follows from the fact that the cohomology group $H^2(H, T)$ classifying extensions of H by the H-module T is $|H|$-torsion. See [**CGR**, page 4] and cf. Lemma 5.4 of Chapter IV. □

LEMMA 4.5. *Let Q be a p-group acting on T and let T^Q denote the closed subgroup of T formed by the fixed points under Q. For $\ell \in \mathbb{N}$ define a homomorphism*

$$\mu_\ell \colon (X_*(T) \otimes \mathbb{Z}/\ell\mathbb{Z})^Q \to T^Q/(T^Q)^0 \quad \text{by} \quad \mu_\ell(\lambda \otimes (i + \ell\mathbb{Z})) := [\lambda(\zeta_\ell^i)].$$

Then for $m, \ell \in \mathbb{N}$ with the divisibility relations $\exp(T^Q/(T^Q)^0) \mid \ell \mid m$ we have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & X_*(T^Q) \otimes_{\mathbb{Z}} \mathbb{Z}/\ell\mathbb{Z} & \longrightarrow & (X_*(T) \otimes_{\mathbb{Z}} \mathbb{Z}/\ell\mathbb{Z})^Q & \xrightarrow{\mu_\ell} & T^Q/(T^Q)^0 & \longrightarrow & 1\,, \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & X_*(T^Q) \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} & \longrightarrow & (X_*(T) \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z})^Q & \xrightarrow{\mu_m} & T^Q/(T^Q)^0 & \longrightarrow & 1 \end{array}$$

where the vertical homomorphisms are induced by the injection

$$\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathbb{Z}/m\mathbb{Z},\ a + \ell\mathbb{Z} \mapsto a\frac{m}{\ell} + m\mathbb{Z}.$$

Moreover $T^Q/(T^Q)^0$ is a p-group.

PROOF. The commutativity of the diagram follows from the construction and our choice of compatible roots of unity ζ_m and ζ_ℓ. The injectivity of the first horizontal map is clear.

If $\lambda \in X_*(T^Q)$, then the value of $\lambda(s)$ for $s \in \mathbb{G}_{\mathbf{m}}$ lies in $(T^Q)^0$, hence the class of $\lambda(\zeta_\ell)$ in the quotient $T^Q/(T^Q)^0$ is trivial. Conversely if $t := \lambda(\zeta_\ell) \in (T^Q)^0$ for some $\lambda \in X_*(T)$ with $\lambda \otimes 1 \in (X_*(T) \otimes \mathbb{Z}/\ell\mathbb{Z})^Q$, then choose a complement T' of $(T^Q)^0$ and write $\lambda(s) = (\mu(s), \mu'(s)) \in T = (T^Q)^0 \times T'$ for $s \in \mathbb{G}_{\mathbf{m}}$. Then $\mu \in X_*((T^Q)^0)$ can be regarded as an element of $X_*(T^Q)$ and $\mu(\zeta_\ell) = \lambda(\zeta_\ell)$ implies that the image of $\mu \otimes 1$ in $(X_*(T) \otimes \mathbb{Z}/\ell\mathbb{Z})^Q$ is equal to $\lambda \otimes 1$. Hence the image of the first horizontal map is equal to the kernel of μ_ℓ.

Each class in the quotient $T^Q/(T^Q)^0$ can be represented by an element $t \in T^Q$ of order divisible by ℓ (since T^Q is isomorphic to $(T^Q)^0 \times T^Q/(T^Q)^0$ and the exponent of $T^Q/(T^Q)^0$ divides ℓ). Using an isomorphism $T \simeq \mathbb{G}_{\mathbf{m}}^n$ and representing t by $(\zeta_\ell^{a_1}, \ldots, \zeta_\ell^{a_n})$ one sees that there exists $\lambda \in X_*(T)$ such that $t = \lambda(\zeta_\ell)$. Since $t \in T^Q$ it follows that $\lambda \otimes 1 \in X_*(T) \otimes_{\mathbb{Z}} \mathbb{Z}/\ell\mathbb{Z}$ is fixed by Q. This implies surjectivity of μ_ℓ. Hence the first row is exact and similarly the second row.

It remains to show that $T^Q/(T^Q)^0$ is a p-group. Let $m = p^r q$ denote the exponent of $T^Q/(T^Q)^0$ with $r \in \mathbb{N}_0$ and $(q, p) = 1$. Then

$$X_*(T^Q) \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} = (X_*(T^Q) \otimes_{\mathbb{Z}} \mathbb{Z}/p^r\mathbb{Z}) \times (X_*(T^Q) \otimes_{\mathbb{Z}} \mathbb{Z}/q\mathbb{Z})$$

and

$$(X_*(T) \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z})^Q = (X_*(T) \otimes_{\mathbb{Z}} \mathbb{Z}/p^r\mathbb{Z})^Q \times (X_*(T) \otimes_{\mathbb{Z}} \mathbb{Z}/q\mathbb{Z})^Q.$$

Since $T^Q/(T^Q)^0$ is the quotient of these two groups and $(X_*(T) \otimes_{\mathbb{Z}} \mathbb{Z}/p^r\mathbb{Z})^Q$ is a p-group it suffices to show that

$$(X_*(T) \otimes_{\mathbb{Z}} \mathbb{Z}/q\mathbb{Z})^Q = X_*(T^Q) \otimes_{\mathbb{Z}} \mathbb{Z}/q\mathbb{Z}.$$

Let $\lambda \in X_*(T)$ such that $\lambda \otimes 1 \in (X_*(T) \otimes \mathbb{Z}/q\mathbb{Z})^Q$. Then $\lambda \otimes 1 = \sum_{g\in Q} g\lambda \otimes \frac{1}{|Q|} \in X_*(T)^Q \otimes \mathbb{Z}/q\mathbb{Z}$, using the fact that the order of Q is invertible modulo q. □

For constructing representations we need to work with characters $\chi \in X^*(T)$ rather than with co-characters $\lambda \in X_*(T)$. Choosing an isomorphism $T \simeq \mathbb{G}_{\mathbf{m}}^n$ the two groups can be both identified with $\mathbb{Z}^n$. An element $b := (b_1, \ldots, b_n) \in \mathbb{Z}^n$ corresponds to $\chi_b \in X^*(T)$ and $\lambda_b \in X_*(T)$ defined by

$$\chi_b(t_1, \ldots, t_n) = t_1^{b_1} t_2^{b_2} \cdots t_n^{b_n}, \quad \lambda_b(s) = (s^{b_1}, s^{b_2}, \ldots, s^{b_n}).$$

An automorphism $\varepsilon \in \mathrm{Aut}(T)$ corresponds to an element $M_\varepsilon = (\varepsilon_{ij})$ of $\mathrm{GL}_n(\mathbb{Z})$ by

$$\varepsilon(t_1, \ldots, t_n) = (t_1^{\varepsilon_{11}} \cdots t_n^{\varepsilon_{1n}}, \ldots, t_1^{\varepsilon_{n1}} \cdots t_n^{\varepsilon_{nn}}).$$

We let $\mathrm{Aut}(T)$ act on $X^*(T)$ by

$$(\varepsilon\chi)(t) = \chi(\varepsilon^{-1}(t))$$

and on $X_*(T)$ by

$$(\varepsilon\lambda)(t) = \varepsilon(\lambda(t)).$$

Then $\varepsilon\lambda_b = \lambda_b$ is equivalent to $M_\varepsilon b = b$ whereas $\varepsilon\chi_b = \chi_b$ is equivalent to $(M_\varepsilon^t)^{-1} b = b$, where $(M_\varepsilon)^t$ denotes the transpose of M_ε.

Let Q be a group acting on the torus T. Let $\hat{Q} \subseteq \mathrm{GL}_n(\mathbb{Z})$ denote its image in $\mathrm{GL}_n(\mathbb{Z}) \simeq \mathrm{Aut}(T)$. Then for the fixed points the identification $T = \mathbb{G}_{\mathbf{m}}^n$ induces identifications

$$T^Q = (\mathbb{G}_{\mathbf{m}}^n)^{\hat{Q}} \quad \text{and} \quad (X_*(T))^Q = (\mathbb{Z}^n)^{\hat{Q}}$$

whereas

$$(X^*(T))^Q = (\mathbb{Z}^n)^{\hat{Q}^t}$$

where $\hat{Q}^t$ denotes the subgroup of $\mathrm{GL}_n(\mathbb{Z})$ formed by the transposed matrices of elements of $\hat{Q}$. Note that $X^*(T[m]) \simeq X^*(T) \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$ for $m \in \mathbb{N}$. Now Lemma 4.5 gives:

Corollary 4.6. *Let $Q \subseteq \mathrm{GL}_n(\mathbb{Z})$ be a p-group and let $Q^t \subseteq \mathrm{GL}_n(\mathbb{Z})$ denote its transpose, which is again a p-group. Let $T := \mathbb{G}_{\boldsymbol{m}}^n$. Then $T^{Q^t}/(T^{Q^t})^0$ is a p-group. Moreover for $r, s \in \mathbb{N}$ with the relations $\exp\left(T^{Q^t}/(T^{Q^t})^0\right) \leq p^s \leq p^r$ we have a commutative diagram with exact rows:*

$$\begin{array}{ccccccccc}
1 & \longrightarrow & X^*(T)^Q \otimes_{\mathbb{Z}} \mathbb{Z}/p^s\mathbb{Z} & \longrightarrow & (X^*(T[p^s]))^Q & \xrightarrow{\mu'_s} & T^{Q^t}/(T^{Q^t})^0 & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \| & & \\
1 & \longrightarrow & X^*(T)^Q \otimes_{\mathbb{Z}} \mathbb{Z}/p^r\mathbb{Z} & \longrightarrow & (X^*(T[p^r]))^Q & \xrightarrow{\mu'_r} & T^{Q^t}/(T^{Q^t})^0 & \longrightarrow & 1
\end{array}$$

where the second vertical arrow sends $\chi \in (X^*(T[p^s]))^Q$ to the character of $T[p^r]$ defined by $t \mapsto \chi(t^{p^{r-s}}), t \in T[p^r]$, and μ'_r, μ'_s correspond to the homomorphisms μ_{p^r}, μ_{p^s}.

Lemma 4.7. *Let $G_r \subseteq G$ be a p-subgroup such as in Lemma 4.4 and $s\colon H \to G_r$ be a section of the projection $G_r \to H$. Let $\alpha := \alpha_s\colon H \times H \to T[r], (h, h') \mapsto \alpha_{h,h'} =$*

$s(hh')^{-1}s(h)s(h')$ be the corresponding 2-cocycle. Given another algebraic group Q and morphisms $\varphi_r\colon G_r \to Q$ and $\psi\colon T \to Q$ of algebraic groups the map $\varphi\colon G \to Q$ defined by

$$\varphi(s(h)t) = \varphi_r(s(h))\psi(t) \quad \text{for } h \in H, t \in T$$

defines a morphism of algebraic groups provided that the following two conditions are satisfied:

$$\psi(g^{-1}tg) = \varphi_r(g)^{-1}\psi(t)\varphi_r(g) \text{ for all } g \in G_r, t \in T. \tag{6}$$

$$\psi(\alpha_{h,h'}) = \varphi_r(\alpha_{h,h'}) \text{ for all } h, h' \in H. \tag{7}$$

Proof. Let $h, h' \in H$ and $t, t' \in T$. Then

$$\begin{aligned}
\varphi(s(h')t's(h)t) &= \varphi(s(h'h)\alpha_{h',h}s(h)^{-1}t's(h)t) \\
&= \varphi_r(s(h'h))\psi(\alpha_{h',h}s(h)^{-1}t's(h)t) \\
&= \varphi_r(s(h'h))\psi(\alpha_{h',h})\psi(s(h)^{-1}t's(h))\psi(t) \\
&= \varphi_r(s(h'h))\varphi_r(\alpha_{h',h})\varphi_r(s(h))^{-1}\psi(t')\varphi_r(s(h))\psi(t) \\
&= \varphi_r(s(h'h)\alpha_{h',h}s(h)^{-1})\psi(t')\varphi_r(s(h))\psi(t) \\
&= \varphi_r(s(h'))\psi(t')\varphi_r(s(h))\psi(t) \\
&= \varphi(s(h')t')\varphi(s(h)t),
\end{aligned}$$

which shows that φ is a group homomorphism. Since H is finite the map $s\colon H \to G_r$ is a morphism of varieties. Therefore $G \to G_r, g \mapsto s(\pi(g))$ as well as $G \to T, g \mapsto s(\pi(g))^{-1}g$ and thus φ are morphisms of varieties as well. Hence φ is a morphism of algebraic groups. □

Lemma 4.8 (cf. [**Se**, Section 8.5, Theorem 16]). *Let F be a p-group and T' a normal abelian subgroup. Let $\rho\colon F \to \mathrm{GL}(W)$ be a representation of F. Then W has a basis $w_1, \ldots, w_d$ such that ρ factors as*

$$\begin{array}{ccc} F & \xrightarrow{\quad\rho\quad} & \mathrm{GL}(W) \\ & {\scriptstyle\varphi}\searrow \quad \nearrow{\scriptstyle\iota} & \\ & \mathbb{G}_{\boldsymbol{m}}^d \rtimes S_d & \end{array}$$

with $\varphi(T') \subseteq \mathbb{G}_{\boldsymbol{m}}^d$ where $\iota\colon \mathbb{G}_{\boldsymbol{m}}^d \rtimes S_d \hookrightarrow \mathrm{GL}(W)$ is defined by $\iota(t\sigma)(w_i) = t_{\sigma(i)}w_{\sigma(i)}$ for $t = (t_1, \ldots, t_n) \in \mathbb{G}_{\boldsymbol{m}}^d$ and $\sigma \in S_d$.

Proof of Theorem 4.1. Clearly a p-faithful representation of G becomes faithful when restricted to any p-subgroup. So it remains to construct F and to show that for a (minimal) faithful representation of F there exists a p-faithful representation of G of the same dimension.

By Lemma 4.4 there exists $r_0 \in \mathbb{N}$ and a (set-theoretic) section $s\colon H \to G$ of $\pi\colon G \to H$ such that the associated cocycle $\alpha_s\colon H \times H \to T$ takes values in $T[p^{r_0}]$. Identify T with $\mathbb{G}_{\mathbf{m}}^n$ for some $n \in \mathbb{N}_0$ and let $\hat{H}$ denote the image of H in $\mathrm{Aut}(T) = \mathrm{GL}_n(\mathbb{Z})$ under the homomorphism $H \to \mathrm{Aut}(T)$ induced by the action of H on T. Now choose $r \in \mathbb{N}$ such

that $p^r \geq p^{r_0+1} \exp\left(T^{Q^t}/T^{Q^t 0}\right)$ for all subgroups $Q \subseteq \hat{H}$. We set $F := G_r$, where G_r is as in Lemma 4.4.

Let $\rho\colon G_r \hookrightarrow \mathrm{GL}(W)$ be a faithful representation and $d = \dim W$. We will show that W affords a p-faithful representation of G. By Lemma 4.8, ρ factors through an (injective) morphism

$$\varphi_r\colon G_r \hookrightarrow \mathbb{G}_{\mathbf{m}}^d \rtimes S_d$$

of algebraic groups such that $\varphi_r(T[p^r]) \subseteq \mathbb{G}_{\mathbf{m}}^d$. Let $\chi_1, \ldots, \chi_d \in X(T[p^r])$ denote the characters of $T[p^r]$ defined by $\varphi_r(t) = (\chi_1(t), \ldots, \chi_d(t))$ for $t \in T[p^r]$. The group H acts on $X(T[p^r])$ through the action on $T[p^r]$ and on $\{1, \ldots, d\}$ through $G_r \xrightarrow{\varphi_r} \mathbb{G}_{\mathbf{m}}^d \rtimes S_d \to S_d$ (which factors through H since $\varphi_r(T[p^r]) \subseteq \mathbb{G}_{\mathbf{m}}^d$). Moreover we have $h\chi_i = \chi_{hi}$ for $i \in \{1 \ldots, d\}$.

Let $\Omega \subseteq \{1, \ldots, d\}$ be a subset such that $\{1, \ldots, d\} = \bigcup_{\omega \in \Omega} H\omega$ is a decomposition into distinct H-orbits. Fix $\omega \in \Omega$. Consider the commutative diagram of Corollary 4.6 with $s := r - r_0 - 1$ and Q the image of $\mathrm{Stab}_H \omega$ in $\mathrm{Aut}(T) = \mathrm{GL}_n(\mathbb{Z})$. Note that $p^r \geq p^s \geq \exp\left(T^{Q^t}/(T^{Q^t})^0\right)$ by our choice of r and that $\chi_\omega \in (X^*(T[p^r]))^Q$. Choose $\gamma \in X^*(T[p^{r-r_0-1}])^Q$ such that $\mu'_{r-r_0-1}(\gamma) = \mu'_r(\chi_\omega)$. Then $\mu'_r(p^{r_0+1}\gamma) = \mu'_r(\chi_\omega)$. Hence by the exactness of the bottom row in Corollary 4.6 there exists $\hat{\chi}_\omega \in X^*(T)^Q$ such that

$$\hat{\chi}_\omega(t) = \chi_\omega(t)\gamma^{-1}(t^{p^{r_0+1}}) \tag{8}$$

for all $t \in T[p^r]$. For $i \in H\omega$, $i = h\omega$ define $\hat{\chi}_i \in X^*(T)$ by:

$$\hat{\chi}_i = h\hat{\chi}_\omega.$$

Note that this definition does not depend on the choice of $h \in H$, since $\hat{\chi}_\omega$ is fixed by $Q = \mathrm{Stab}_H \omega$. Doing this for all $\omega \in \Omega$ gives us characters $\hat{\chi}_1, \ldots, \hat{\chi}_d \in X(T)$ such that

$$h\hat{\chi}_i = \hat{\chi}_{hi} \tag{9}$$

for all $h \in H$ and $i \in \{1, \ldots, d\}$ and, using equation (8), elements $\gamma_1, \ldots, \gamma_d \in X^*(T[p^{r-r_0-1}])$ such that

$$\hat{\chi}_i(t) = \chi_i(t)\gamma_i^{-1}(t^{p^{r_0+1}}) \tag{10}$$

for all $t \in T[p^r]$.

Define a homomorphism $\psi\colon T \to \mathbb{G}_{\mathbf{m}}^d \rtimes S_d$ by setting

$$\psi(t) = (\hat{\chi}_1(t), \ldots, \hat{\chi}_d(t)) \in \mathbb{G}_{\mathbf{m}}^d \text{ for } t \in T.$$

We want to apply Lemma 4.7 to obtain a morphism $\varphi\colon G \to \mathbb{G}_{\mathbf{m}}^d \rtimes S_d$ of algebraic groups satisfying $\varphi(s(h)t) = \varphi_r(s(h))\psi(t)$ for $h \in H, t \in T$. Condition 6 that we must check follows from equation (9) and condition 7 follows from equation (10), using the fact that α_s takes values in $T[p^{r_0}]$. Hence such a φ exists. Composing it with $\iota\colon \mathbb{G}_{\mathbf{m}}^d \rtimes S_d \hookrightarrow \mathrm{GL}(W)$ yields a representation of G of dimension d. It remains to show that this representation is p-faithful.

By Lemma 4.3 it suffices to show that $\ker\varphi \cap Z(G)[p]$ is trivial. Let $g \in \ker\varphi \cap Z(G)[p]$ and represent it by $g = s(h)t$ for some $h \in H, t \in T$. Then $h^p = 1$ and $(s(h)t)t =$

$t(s(h)t)$ implies that $s(h)$ and t commute. Hence $1 = (s(h)t)^p = (s(h))^p t^p$. But $(s(h))^p = s(h^p)\alpha_{h,h^{p-1}} \cdots \alpha_{h,h} = \alpha_{1,1}\alpha_{h,h^{p-1}} \cdots \alpha_{h,h} \in T[p^{r_0}]$. Hence

$$t \in T[p^{r_0+1}] \subseteq T[p^r].$$

We claim that $\varphi_r(s(h)t) = \varphi(s(h)t)$. It suffices to show that $\hat{\chi}_i(t) = \chi_i(t)$ for all $i \in \{1, \ldots, d\}$. This follows from equation (10). Hence $g = s(h)t \in \ker \varphi_r = \{e\}$. This shows that $\ker \varphi \cap Z(G)[p] = \{e\}$, hence finishes the proof. □

Bibliography

[BH08] B. Bekka, P. de la Harpe: *Irreducibly represented groups*, Comment. Math. Helv. **83** (2008), 847-868.

[CGR] V. Chernousov, Ph. Gille, Z. Reichstein: *Resolving G-torsors by abelian base extensions*, J. Algebra **296** (2006), 561–581.

[Ga54] W. Gaschütz: *Endliche Gruppen mit treuen absolut-irreduziblen Darstellungen*, Math. Nachr. **12** (1954) 253-255.

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

[Se] J.-P. Serre: *Linear representations of finite groups*, Grad. Texts in Math. (1977), Springer-Verlag, Berlin.

[Sh30] K. Shoda: *Über direkt zerlegbare Gruppen*, Journ. Fac. Sci. Tokyo Imp. Univ. section I, Vol. **II-3** (1930); correction, Vol. **II-7**(1931).

CHAPTER IV

Essential p-dimension of algebraic tori

ROLAND LÖTSCHER, MARK MACDONALD, AUREL MEYER
AND ZINOVY REICHSTEIN

The essential dimension is a numerical invariant of an algebraic group G which may be thought of as a measure of complexity of G-torsors over fields. A recent theorem of N. Karpenko and A. Merkurjev gives a simple formula for the essential dimension of a finite p-group. We obtain similar formulas for the essential p-dimension of a broader class of groups, which includes all algebraic tori.

1. Introduction

Throughout this paper p will denote a prime integer, k a base field of characteristic $\neq p$ and G a (not necessarily smooth) algebraic group defined over k. Unless otherwise specified, all fields are assumed to contain k and all morphisms between them are assumed to be k-homomorphisms.

We begin by recalling the notion of essential dimension of a functor from [**BF**]. Let Fields_k be the category of field extensions K/k, Sets be the category of sets, and $F\colon \mathrm{Fields}_k \to \mathrm{Sets}$ be a covariant functor. As usual, given a field extension $k \subset K_0 \subset K$, we will denote the image of $\alpha \in F(K_0)$ under the natural map $F(K_0) \to F(K)$ by α_K.

An object $\alpha \in F(K)$ is said to *descend* to an intermediate field $k \subseteq K_0 \subseteq K$ if α is in the image of the induced map $F(K_0) \to F(K)$. The *essential dimension* $\mathrm{ed}_k(\alpha)$ is defined as the minimum of the transcendence degrees $\mathrm{trdeg}_k(K)$ taken over all fields $k \subseteq K_0 \subseteq K$ such that α descends to K_0. The essential dimension $\mathrm{ed}_k(F)$ of the functor F is defined as the maximal value of $\mathrm{ed}_k(\alpha)$, where the maximum is taken over all fields K/k and all $\alpha \in F(K)$.

Of particular interest to us will be the functor of G-torsors $F_G := H^1(*, G)$, which associates to every K/k the set of isomorphism classes of G-torsors over $\mathrm{Spec}(K)$. The essential dimension of this functor is usually called the *essential dimension of* G and is denoted by the symbol $\mathrm{ed}_k(G)$. Informally speaking, this number may be thought of as a measure of complexity of G-torsors over fields. For example, if k is an algebraically closed field of characteristic 0 then groups G of essential dimension 0 are precisely the so-called *special groups*, i.e., algebraic groups G/k with the property that every G-torsor over $\mathrm{Spec}(K)$ is split, for every field K/k. These groups were classified by A. Grothendieck [**Gro**].

For many groups the essential dimension is hard to compute, even over the field $\mathbb{C}$ of complex numbers. The following related notion is often more accessible. Let $F\colon \mathrm{Fields}_k \to \mathrm{Sets}$ be a covariant functor and p be a prime integer, as above. The *essential p-dimension* of $\alpha \in F(K)$, denoted $\mathrm{ed}_k(\alpha; p)$, is defined as the minimal value of $\mathrm{ed}_k(\alpha_{K'})$, where K' ranges over all finite field extensions of K whose degree is prime to p. The essential p-dimension of F, $\mathrm{ed}_k(F; p)$ of F is once again, defined as the maximal value of $\mathrm{ed}_k(\alpha; p)$, where the maximum is taken over all fields K/k and all $\alpha \in F(K)$, and once again we will write $\mathrm{ed}_k(G; p)$ in place of $\mathrm{ed}_k(F_G; p)$, where $F_G := H^1(*, G)$ is the functor of G-torsors.

Note that $\mathrm{ed}_k(\alpha)$, $\mathrm{ed}_k(F)$, $\mathrm{ed}_k(G)$, $\mathrm{ed}_k(\alpha; p)$, etc., depend on k. We will write ed instead of ed_k if the reference to k is clear from the context. For background material on essential dimension we refer the reader to [**BR, Re, RY, BF, Me**$_1$].

We also remark that in the case of the functor F_G of G-torsors, the maximal value of $\mathrm{ed}_k(\alpha)$ and $\mathrm{ed}_k(\alpha; p)$ in the above definitions is attained in the case where α is a versal G-torsor in the sense of [**GMS**, Section I.5]. Since every generically free linear representation $\rho\colon G \to \mathrm{GL}(V)$ gives rise to a versal G-torsor (see [**GMS**, Example I.5.4]), we obtain the inequality

$$\mathrm{ed}_k(G; p) \le \mathrm{ed}_k(G) \le \dim(V) - \dim(G)\,; \tag{11}$$

see [**Re**, Therem 3.4] or [**BF**, Lemma 4.11]. (Recall that ρ is called *generically free* if there exists a G-invariant dense open subset $U \subset V$ such that the scheme-theoretic stabilizer of every point of U is trivial.)

N. Karpenko and A. Merkurjev [**KM**] recently showed that the inequality (11) is in fact sharp for finite constant p-groups.

THEOREM 1.1. *Let G be a finite constant p-group over a field k containing a primitive pth root of unity. Then*

$$\mathrm{ed}_k(G; p) = \mathrm{ed}_k(G) = \min \dim(V)\,,$$

where the minimum is taken over all faithful k-representations $G \hookrightarrow \mathrm{GL}(V)$.

The goal of this paper is to prove similar formulas for a broader class of groups G. To state our first result, let

$$1 \to C \to G \to Q \to 1 \tag{12}$$

be an exact sequence of algebraic groups over k such that C is central in G and isomorphic to μ_p^r for some $r \ge 0$. Given a character $\chi\colon C \to \mu_p$, we will, following [**KM**], denote by Rep^χ the set of irreducible representations $\varphi\colon G \to \mathrm{GL}(V)$, defined over k, such that $\varphi(c) = \chi(c)\,\mathrm{Id}_V$ for every $c \in C$.

THEOREM 1.2. *Assume that k is a field of characteristic $\ne p$ containing a primitive pth root of unity. Suppose a sequence of k-groups of the form* (12) *satisfies the following condition:*

$$\gcd\{\dim(\varphi) \,|\, \varphi \in \mathrm{Rep}^\chi\} = \min\{\dim(\varphi) \,|\, \varphi \in \mathrm{Rep}^\chi\}$$

for every character $\chi\colon C \to \mu_p$. *(Here, as usual,* gcd *stands for the greatest common divisor.) Then*

$$\mathrm{ed}_k(G;p) \geq \min \dim(\rho) - \dim G\,,$$

where the minimum is taken over all finite-dimensional k*-representations* ρ *of* G *such that* $\rho_{|C}$ *is faithful.*

Of particular interest to us will be extensions of finite p-groups by algebraic tori, i.e., k-groups G which fit into an exact sequence of the form

$$1 \to T \to G \to F \to 1\,, \tag{13}$$

where F is a finite p-group and T is a torus over k. (A similar class of groups, where F is assumed to be supersolvable, was studied in [$\mathbf{BS}_2$].) Note that in this paper when we will work with a finite algebraic group F we will not assume it is constant, which is to say, the absolute Galois group of k may act non-trivially on the separable points of G. For the sake of computing $\mathrm{ed}_k(G;p)$ we may assume that k is a p-closed field (as in Definition 3.1); see Lemma 3.3. In this situation we will show that

(i) there is a natural choice of a split central subgroup $C \subset G$ in the sequence (12) such that the conditions of Theorem 1.2 are always satisfied.

(ii) Moreover, if G is isomorphic to the direct product of a torus and a finite twisted p-group, then a variant of (11) yields an upper bound, matching the lower bound of Theorem 1.2.

This brings us to the main result of this paper. We will say that a representation $\rho\colon G \to \mathrm{GL}(V)$ of an algebraic group G is p-faithful if its kernel is finite and of order prime to p.

Theorem 1.3. *Let* G *be an extension of a (twisted) finite* p*-group* F *by an algebraic torus* T *defined over a field* k *(of characteristic not* p*). In other words, we have an exact sequence*

$$1 \to T \to G \to F \to 1\,.$$

Denote a p*-closure of* k *by* $k^{(p)}$ *(see Definition 3.1). Then*

(a) $\mathrm{ed}_k(G;p) \geq \min \dim(\rho) - \dim G$*, where the minimum is taken over all* p*-faithful linear representations* ρ *of* $G_{k^{(p)}}$ *over* $k^{(p)}$*.*

Now assume that G *is the direct product of* T *and* F*. Then*

(b) equality holds in (a), and

(c) over $k^{(p)}$ *the absolute essential dimension of* G *and the essential* p*-dimension coincide:*

$$\mathrm{ed}_{k^{(p)}}(G_{k^{(p)}}) = \mathrm{ed}_{k^{(p)}}(G_{k^{(p)}};p) = \mathrm{ed}_k(G;p).$$

If G is a p-group, a representation ρ is p-faithful if and only if it is faithful. However, for an algebraic torus, "p-faithful" cannot be replaced by "faithful"; see Remark 10.3.

Theorem 1.3 appears to be new even in the case where G is a twisted cyclic p-group, where it extends earlier work of Rost [**Ro**], Bayarmagnai [**Ba**] and Florence [**Fl**]; see Corollary 9.3 and Remark 9.4.

If G is a direct product of a torus and an abelian p-group, the value of $\mathrm{ed}_k(G;p)$ given by Theorem 1.3 can be rewritten in terms of the character module $X(G)$; see Corollary 9.2. In particular, we obtain the following formula for the essential dimension of a torus.

THEOREM 1.4. *Let T be an algebraic torus defined over a p-closed field $k = k^{(p)}$ of characteristic $\neq p$. Suppose $\Gamma = \mathrm{Gal}(k_{\mathrm{sep}}/k)$ acts on the character lattice $X(T)$ via a finite quotient $\overline{\Gamma}$. Then*

$$\mathrm{ed}_k(T) = \mathrm{ed}_k(T;p) = \min \mathrm{rank}(L)\,,$$

where the minimum is taken over all exact sequences of $\mathbb{Z}_{(p)}\overline{\Gamma}$-lattices of the form

$$(0) \to L \to P \to X(T)_{(p)} \to (0)\,,$$

where P is permutation and $X(T)_{(p)}$ stands for $X(T) \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$.

In many cases Theorem 1.4 renders the value of $\mathrm{ed}_k(T)$ computable by known representation-theoretic methods, e.g., from [**CR**]. We will give several examples of such computations in Sections 11 and 12. Another application was recently given by Merkurjev [$\mathbf{Me}_3$], who used Theorem 1.4, in combination with techniques from [$\mathbf{Me}_2$], to show that

$$\mathrm{ed}_k(\mathrm{PGL}_{p^r};p) \geq (r-1)p^r + 1$$

for any $r \geq 1$. (For $r = 2$ the above inequality is the main result of [$\mathbf{Me}_2$].) This represents dramatic improvement over the best previously known lower bounds on $\mathrm{ed}_k(\mathrm{PGL}_{p^r})$. The question of computing $\mathrm{ed}_k(\mathrm{PGL}_{p^r})$ is a long-standing open problem; for an overview, see [$\mathbf{MR}_1$, $\mathbf{MR}_2$].

It is natural to try to extend the formula of Theorem 1.3(b) to all k-groups G, whose connected component G^0 is a torus. For example, the normalizer of a maximal torus in any reductive k-group is of this form. For the purpose of computing $\mathrm{ed}_k(G;p)$ we may assume that k is p-closed and G/G^0 is a p-group; in other words, G is as in Theorem 1.3(a). Then

$$\min \dim \mu - \dim(G) \leq \mathrm{ed}(G;p) \leq \min \dim \rho - \dim G\,, \tag{14}$$

where the two minima are taken over all p-faithful representations μ, and p-generically free representations ρ, respectively. Here we say that a representation ρ of G is *p-generically free* if the $\ker(\rho)$ is finite of order prime to p, and ρ descends to a generically free representation of $G/\ker(\rho)$. The upper bound in (14) follows from (11), in combination with Theorem 6.1; the lower bound is Theorem 1.3(a). If G is a direct product of a torus and a p-group, then every p-generically free representation is p-faithful (see Lemma 7.1). In this case the lower and upper bounds of (14) coincide, yielding the exact value of $\mathrm{ed}_k(G;p)$ of Theorem 1.3(b). However, if we only assume G is a p-group extended by a torus, then faithful G-representations no longer need to be generically free. We do not know how to bridge the gap between the upper and the lower bound in (14) in this generality; however, in all of the specific examples we have considered, the upper bound turned out to be sharp. We thus put forward the following conjecture.

CONJECTURE 1.5. *Let G be an extension of a p-group by a torus, defined over a field k of characteristic $\neq p$. Then*

$$\operatorname{ed}(G;p) = \min \dim \rho - \dim G,$$

where the minimum is taken over all p-generically free representations ρ of $G_{k^{(p)}}$ over $k^{(p)}$.

The rest of the paper is structured as follows. Theorem 1.2 is proved in Section 2. Section 3 is devoted to preliminary material on the p-closure of a field. Theorem 1.3(a) is proved in Sections 4 and 5. In Section 6 we will show that if $G \to Q$ is a p-isogeny then $\operatorname{ed}_k(G;p) = \operatorname{ed}_k(Q;p)$. This result playes a key role in the proof of Theorem 1.3(b) in Section 7. At the end of Section 7 we prove a formula for the essential p-dimension of any finite group G by passing to a Sylow p-subgroup defined over k; see Corollory 7.2. In Section 8 we prove the following Additivity Theorem 8.1: If G_1 and G_2 are direct products of tori and p-groups, then

$$\operatorname{ed}_k(G_1 \times G_2;p) = \operatorname{ed}_k(G_1;p) + \operatorname{ed}_k(G_2;p)\,.$$

In Section 9 we restate and amplify Theorem 1.3(b) (with G abelian) in terms of $\operatorname{Gal}(k_{\mathrm{sep}}/k)$-modules; in particular, Theorem 1.4 stated above is a special case of Corollary 9.2 which is proved there. In Section 10 we prove Theorem 1.3(c) by using Theorem 1.3(b), additivity, and the lattice perspective from Section 9. The last two sections are intended to illustrate our results by computing essential dimensions of specific algebraic tori. In Section 11 we classify algebraic tori T of essential p-dimension 0 and 1; see Theorems 11.1 and 11.5. In Section 12 we compute the essential p-dimension of all tori T over a p-closed field k, which are split by a cyclic extension l/k of degree dividing p^2.

2. Proof of Theorem 1.2

Denote by $C^* := \operatorname{Hom}(C, \mu_p)$ the character group of C. Let $E \to \operatorname{Spec} K$ be a versal Q-torsor [**GMS**, Example 5.4], where K/k is some field extension, and let $\beta\colon C^* \to \operatorname{Br}_p(K)$ denote the homomorphism that sends $\chi \in C^*$ to the image of $E \in H^1(K,Q)$ in $\operatorname{Br}_p(K)$ under the map

$$H^1(K,Q) \to H^2(K,C) \xrightarrow{\chi_*} H^2(K,\mu_p) = \operatorname{Br}_p(K)$$

given by composing the connecting map with χ_*. Then there exists a basis $\chi_1, \dots, \chi_r$ of C^* such that

$$\operatorname{ed}_k(G;p) \geq \sum_{i=1}^{r} \operatorname{ind} \beta(\chi_i) - \dim G, \tag{15}$$

see [$\mathbf{Me}_1$, Theorem 4.8, Example 3.7]. Moreover, by [**KM**, Theorem 4.4, Remark 4.5]

$$\operatorname{ind} \beta(\chi_i) = \gcd \dim(\rho)\,,$$

where the greatest common divisor is taken over all (finite-dimensional) representations ρ of G such that $\rho_{|C}$ is scalar multiplication by χ_i. By our assumption, gcd can be replaced by min. Hence, for each $i \in \{1, \dots, r\}$ we can choose a representation ρ_i of G with

$$\operatorname{ind} \beta(\chi_i) = \dim(\rho_i)$$

such that $(\rho_i)_{|C}$ is scalar multiplication by χ_i.

Set $\rho := \rho_1 \oplus \cdots \oplus \rho_r$. The inequality (15) can be written as

$$\operatorname{ed}_k(G;p) \geq \dim(\rho) - \dim G. \tag{16}$$

Since $\chi_1, \ldots, \chi_r$ forms a basis of C^* the restriction of ρ to C is faithful. This proves the theorem. □

3. The p-closure of a field

Let K be a field extension of k and K_{alg} an algebraic closure. We will construct a field $K^{(p)}/K$ in K_{alg} with all finite subextensions of $K^{(p)}/K$ of degree prime to p and all finite subextensions of $K_{\text{alg}}/K^{(p)}$ of degree a power of p.

Fix a separable closure $K_{\text{sep}} \subset K_{\text{alg}}$ of K and denote $\Gamma = \operatorname{Gal}(K_{\text{sep}}/K)$. Recall that Γ is profinite and has Sylow-p subgroups which enjoy similar properties as in the finite case, see for example [**RZ**] or [**Wi**]. Let Φ be a Sylow-p subgroup of Γ and K_{sep}^{Φ} its fixed field.

Definition 3.1. We call the field

$$K^{(p)} = \{a \in K_{\text{alg}} | a \text{ is purely inseparable over } K_{\text{sep}}^{\Phi}\}$$

a *p-closure* of K. A field K will be called *p-closed* if $K{=}K^{(p)}$.

Note that $K^{(p)}$ is unique in K_{alg} only up to the choice of a Sylow-p subgroup Φ in Γ. The notion of being p-closed does not depend on this choice.

Proposition 3.2.

(a) $K^{(p)}$ is a direct limit of finite extensions K_i/K of degree prime to p.
(b) Every finite extension of $K^{(p)}$ is separable of degree a power of p; in particular, $K^{(p)}$ is perfect.
(c) The q-cohomological dimension of $\Psi = \operatorname{Gal}(K_{\text{alg}}/K^{(p)})$ is $\operatorname{cd}_q(\Psi) = 0$ for any prime $q \neq p$.

Proof. (a) First note that K_{sep} is the limit of the directed set $\{K_{\text{sep}}^N\}$ over all normal subgroups $N \subset \Gamma$ of finite index. Let

$$\mathcal{L} = \{K_{\text{sep}}^{N\Phi} | N \text{ normal with finite index in } \Gamma\}.$$

This is a directed set, and since Φ is Sylow, the index of $N\Phi$ in Γ is prime to p. Therefore $\mathcal{L}$ consists of finite separable extensions of K of degree prime to p. Moreover, K_{sep}^{Φ} is the direct limit of fields L in $\mathcal{L}$.

If $\operatorname{char} k = 0$, $K^{(p)} = K_{\text{sep}}^{\Phi}$ and we are done. Otherwise suppose $\operatorname{char} k = q \neq p$. Let

$$\mathcal{E} = \{E \subset K_{\text{alg}} | E/L \text{ finite and purely inseparable for some } L \in \mathcal{L}\}.$$

$\mathcal{E}$ consists of finite extensions of K of degree prime to p, because a purely inseparable extension has degree a power of q. One can check that $\mathcal{E}$ forms a directed set.

Finally note that if a is purely inseparable over K_{sep}^{Φ} with minimal polynomial $x^{q^n}-l$ (so that $l \in K_{\mathrm{sep}}^{\Phi}$), then l is already in some $L \in \mathcal{L}$ since K_{sep}^{Φ} is the limit of $\mathcal{L}$. Thus $a \in E = L(a)$ which is in $\mathcal{E}$ and we conclude that $K^{(p)}$ is the direct limit of $\mathcal{E}$.

(b) $K^{(p)}$ is the purely inseparable closure of K_{sep}^{Φ} in K_{alg} and $K_{\mathrm{alg}}/K^{(p)}$ is separable, see [**Win**, 2.2.20]. Moreover, $\mathrm{Gal}(K_{\mathrm{alg}}/K^{(p)}) \simeq \mathrm{Gal}(K_{\mathrm{sep}}/K_{\mathrm{sep}}^{\Phi}) = \Phi$ is a pro-p group and so every finite extension of $K^{(p)}$ is separable of degree a power of p.

(c) See [$\mathbf{Se}_2$, Cor. 2, I. 3]. □

We call a covariant functor $\mathcal{F}\colon \mathrm{Fields}/k \to \mathrm{Sets}$ *limit-preserving* if for any directed system of fields $\{K_i\}$, $\mathcal{F}(\varinjlim K_i) = \varinjlim \mathcal{F}(K_i)$. For example if G is an algebraic group, the functor $F_G = H^1(*, G)$ is limit-preserving; see [**Ma**, 2.1].

LEMMA 3.3. *Let $\mathcal{F}$ be limit-preserving and $\alpha \in \mathcal{F}(K)$ an object. Denote the image of α in $\mathcal{F}(K^{(p)})$ by $\alpha_{K^{(p)}}$.*

(a) $\mathrm{ed}_k(\alpha; p) = \mathrm{ed}_k(\alpha_{K^{(p)}}; p) = \mathrm{ed}_k(\alpha_{K^{(p)}})$.

(b) $\mathrm{ed}_k(\mathcal{F}; p) = \mathrm{ed}_{k^{(p)}}(\mathcal{F}; p)$.

PROOF. (a) The inequalities $\mathrm{ed}(\alpha; p) \geq \mathrm{ed}(\alpha_{K^{(p)}}; p) = \mathrm{ed}(\alpha_{K^{(p)}})$ are clear from the definition and Proposition 3.2(b) since $K^{(p)}$ has no finite extensions of degree prime to p. It remains to prove $\mathrm{ed}(\alpha; p) \leq \mathrm{ed}(\alpha_{K^{(p)}})$. If L/K is finite of degree prime to p,

$$\mathrm{ed}(\alpha; p) = \mathrm{ed}(\alpha_L; p), \tag{17}$$

cf. [$\mathbf{Me}_1$, Proposition 1.5] and its proof. For the p-closure $K^{(p)}$ this is similar and uses (17) repeatedly:

Suppose there is a subfield $K_0 \subset K^{(p)}$ and $\alpha_{K^{(p)}}$ comes from an element $\beta \in \mathcal{F}(K_0)$, so that $\beta_{K^{(p)}} = \alpha_{K^{(p)}}$. Write $K^{(p)} = \lim \mathcal{L}$, where $\mathcal{L}$ is a direct system of finite prime to p extensions of K. Then $K_0 = \lim \mathcal{L}_0$ with $\mathcal{L}_0 = \{L \cap K_0 | L \in \mathcal{L}\}$ and by assumption on $\mathcal{F}$, $\mathcal{F}(K_0) = \varinjlim_{L' \in \mathcal{L}_0} \mathcal{F}(L')$. Thus there is a field $L' = L \cap K_0$ ($L \in \mathcal{L}$) and $\gamma \in \mathcal{F}(L')$ such that $\gamma_{K_0} = \beta$. Since α_L and γ_L become equal over $K^{(p)}$, after possibly passing to a finite extension, we may assume they are equal over L which is finite of degree prime to p over K. Combining these constructions with (17) we see that

$$\mathrm{ed}(\alpha; p) = \mathrm{ed}(\alpha_L; p) = \mathrm{ed}(\gamma_L; p) \leq \mathrm{ed}(\gamma_L) \leq \mathrm{ed}(\alpha_{K^{(p)}}).$$

(b) This follows immediately from (a), taking α of maximal essential p-dimension. □

PROPOSITION 3.4. *Let $\mathcal{F}, \mathcal{G}\colon \mathrm{Fields}/k \to \mathrm{Sets}$ be limit-preserving functors and $\mathcal{F} \to \mathcal{G}$ a natural transformation. If the map*

$$\mathcal{F}(K) \to \mathcal{G}(K)$$

is bijective (resp. surjective) for any p-closed field extension K/k then

$$\mathrm{ed}(\mathcal{F}; p) = \mathrm{ed}(\mathcal{G}; p) \quad (\textit{resp. } \mathrm{ed}(\mathcal{F}; p) \geq \mathrm{ed}(\mathcal{G}; p)).$$

PROOF. Assume the maps are surjective. By Proposition 3.2(a), the natural transformation is p-surjective, in the terminology of [$\mathbf{Me}_1$], so we can apply [$\mathbf{Me}_1$, Prop. 1.5] to conclude $\mathrm{ed}(\mathcal{F}; p) \geq \mathrm{ed}(\mathcal{G}; p)$.

Now assume the maps are bijective. Let α be in $\mathcal{F}(K)$ for some K/k and β its image in $\mathcal{G}(K)$. We claim that $\operatorname{ed}(\alpha;p) = \operatorname{ed}(\beta;p)$. First, by Lemma 3.3 we can assume that K is p-closed and it is enough to prove that $\operatorname{ed}(\alpha) = \operatorname{ed}(\beta)$.

Assume that β comes from $\beta_0 \in \mathcal{G}(K_0)$ for some field $K_0 \subset K$. Any finite prime to p extension of K_0 is isomorphic to a subfield of K (cf. [**Me**$_1$, Lemma 6.1]) and so also any p-closure of K_0 (which has the same transcendence degree over k). We may therefore assume that K_0 is p-closed. By assumption $\mathcal{F}(K_0) \to \mathcal{G}(K_0)$ and $\mathcal{F}(K) \to \mathcal{G}(K)$ are bijective. The unique element $\alpha_0 \in \mathcal{F}(K_0)$ which maps to β_0 must therefore map to α under the natural restriction map. This shows that $\operatorname{ed}(\alpha) \leq \operatorname{ed}(\beta)$. The other inequality always holds and the claim follows.

Taking α maximal with respect to its essential dimension, we obtain $\operatorname{ed}(\mathcal{F};p) = \operatorname{ed}(\alpha;p) = \operatorname{ed}(\beta;p) \leq \operatorname{ed}(\mathcal{G};p)$. □

4. The group $C(G)$

As we indicated in the Introduction, our proof of Theorem 1.3(a) will rely on Theorem 1.2. To apply Theorem 1.2, we need to construct a split central subgroup C of G. In this section, we will explain how to construct this subgroup (we will call it $C(G)$) and discuss some of its properties.

Recall that an algebraic group G over a field k is said to be *of multiplicative type* if $G_{k_{\mathrm{sep}}}$ is diagonalizable over the separable closure k_{sep} of k; cf., e.g., [**Vo**, Section 3.4]. Here, as usual, $G_{k'} := G \times_{\operatorname{Spec} k} \operatorname{Spec}(k')$ for any field extension k'/k. Smooth connected groups of multiplicative type are precisely the algebraic tori.

We will use the following common conventions in working with an algebraic group A of multiplicative type over k.

- We will denote the character group of A by $X(A)$.
- Given a field extension l/k, A is split over l if and only if the absolute Galois group $\operatorname{Gal}(l_{\mathrm{sep}}/l)$ acts trivially on $X(A)$.
- We will write $A[p]$ for the p-torsion subgroup $\{a \in A \,|\, a^p = 1\}$ of A. Clearly $A[p]$ is defined over k.

Let T be an algebraic torus. It is well known how to construct a maximal split subtorus of T, see for example [**Bo**, 8.15] or [**Wa**, 7.4]. The following definition is a variant of this.

Definition 4.1. Let A be an algebraic group of multiplicative type over k. Let $\Delta(A)$ be the Γ-invariant subgroup of $X(A)$ generated by elements of the form $x - \gamma(x)$, as x ranges over $X(A)$ and γ ranges over Γ. Define

$$\operatorname{Split}_k(A) = \operatorname{Diag}(X(A)/\Delta(A))\,.$$

Here Diag denotes the anti-equivalence between continuous $\mathbb{Z}\Gamma$-modules and algebraic groups of multiplicative type, cf. [**Wa**, 7.3].

Definition 4.2. Let G be an extension of a finite p-group by a torus, defined over a field k, as in (13). Then

$$C(G) := \operatorname{Split}_k(Z(G)[p])\,,$$

where $Z(G)$ denotes the centre of G.

LEMMA 4.3. *Let A be an algebraic group of multiplicative type over k.*

(a) $\mathrm{Split}_k(A)$ *is split over k,*
(b) $\mathrm{Split}_k(A) = A$ *if and only if A is split over k,*
(c) If B is a k-subgroup of A then $\mathrm{Split}_k(B) \subset \mathrm{Split}_k(A)$.
(d) For $A = A_1 \times A_2$, $\mathrm{Split}_k(A_1 \times A_2) = \mathrm{Split}_k(A_1) \times \mathrm{Split}_k(A_2)$,
(e) If $A[p] \neq \{1\}$ and A is split over a Galois extension l/k, such that $\overline{\Gamma} = \mathrm{Gal}(l/k)$ *is a p-group, then* $\mathrm{Split}_k(A) \neq \{1\}$.

PROOF. Parts (a), (b), (c) and (d) easily follow from the definition.

Proof of (e): By part (c), it suffices to show that $\mathrm{Split}_k(A[p]) \neq \{1\}$. Hence, we may assume that $A = A[p]$ or equivalently, that $X(A)$ is a finite-dimensional $\mathbb{F}_p$-vector space on which the p-group $\overline{\Gamma}$ acts. Any such action is upper-triangular, relative to some $\mathbb{F}_p$-basis $e_1, \dots, e_n$ of $X(A)$; see, e.g., [**Se**$_1$, Proposition 26, p.64]. That is,

$$\gamma(e_i) = e_i + (\mathbb{F}_p\text{-linear combination of } e_{i+1}, \dots, e_n)$$

for every $i = 1, \dots, n$ and every $\gamma \in \overline{\Gamma}$. Our goal is to show that $\Delta(A) \neq X(A)$. Indeed, every element of the form $x - \gamma(x)$ is contained in the Γ-invariant submodule $\mathrm{Span}(e_2, \dots, e_n)$. Hence, these elements cannot generate all of $X(A)$. □

PROPOSITION 4.4. *Suppose G is an extension of a p-group by a torus, defined over a p-closed field k. Suppose N is a normal subgroup of G defined over k. Then the following conditions are equivalent:*

(i) N is finite of order prime to p,
(ii) $N \cap C(G) = \{1\}$,
(iii) $N \cap Z(G)[p] = \{1\}$,

In particular, taking $N = G$, we see that $C(G) \neq \{1\}$ if $G \neq \{1\}$.

PROOF. (i) $\Longrightarrow$ (ii) is obvious, since $C(G)$ is a p-group.
(ii) $\Longrightarrow$ (iii). Assume the contrary: $A := N \cap Z(G)[p] \neq \{1\}$. By Lemma 4.3

$$\{1\} \neq C(A) \subset N \cap C(Z(G)[p]) = N \cap C(G)\,,$$

contradicting (ii).

Our proof of the implication (iii) $\Longrightarrow$ (i), will rely on the following

Claim: Let M be a non-trivial normal finite p-subgroup of G such that the commutator (G^0, M) is trivial. Then $M \cap Z(G)[p] \neq \{1\}$.

To prove the claim, note that $M(k_{\mathrm{sep}})$ is non-trivial and the conjugation action of $G(k_{\mathrm{sep}})$ on $M(k_{\mathrm{sep}})$ factors through an action of the p-group $(G/G^0)(k_{\mathrm{sep}})$. Thus each orbit has p^n elements for some $n \geq 0$; consequently, the number of fixed points is divisible by p. The intersection $(M \cap Z(G))(k_{\mathrm{sep}})$ is precisely the fixed point set for this action; hence, $M \cap Z(G)[p] \neq \{1\}$. This proves the claim.

We now continue with the proof of the implication (iii) $\Longrightarrow$ (i). For notational convenience, set $T := G^0$. Assume that $N \triangleleft G$ and $N \cap Z(G)[p] = \{1\}$. Applying the claim to

the normal subgroup $M := (N \cap T)[p]$ of G, we see that $(N \cap T)[p] = \{1\}$, i.e., $N \cap T$ is a finite group of order prime to p. The exact sequence

$$1 \to N \cap T \to N \to \overline{N} \to 1\,, \tag{18}$$

where $\overline{N}$ is the image of N in G/T, shows that N is finite. Now observe that for every $r \geq 1$, the commutator $(N, T[p^r])$ is a p-subgroup of $N \cap T$. Thus $(N, T[p^r]) = \{1\}$ for every $r \geq 1$. We claim that this implies $(N, T) = \{1\}$ by Zariski density. If N is smooth, this is straightforward; see [**Bo**, Proposition 2.4, p. 59]. If N is not smooth, note that the map $c\colon N \times T \to G$ sending (n, t) to the commutator $ntn^{-1}t^{-1}$ descends to $\overline{c}\colon \overline{N} \times T \to G$ (indeed, $N \cap T$ clearly commutes with T). Since $|\overline{N}|$ is a power of p and $\mathrm{char}(k) \neq p$, $\overline{N}$ is smooth over k, and we can pass to the separable closure k_{sep} and apply the usual Zariski density argument to show that the image of $\overline{c}$ is trivial.

We thus conclude that $N \cap T$ is central in N. Since $\gcd(|N \cap T|, \overline{N}) = 1$, by [$\mathbf{Sch}_2$, Corollary 5.4] the extension (18) splits, i.e., $N \simeq (N \cap T) \times \overline{N}$. This turns $\overline{N}$ into a subgroup of G satisfying the conditions of the claim. Therefore $\overline{N}$ is trivial and $N = N \cap T$ is a finite group of order prime to p, as claimed. □

For future reference, we record the following obvious consequence of the equivalence of conditions (i) and (ii) in Proposition 4.4.

Corollary 4.5. *Let $k = k^{(p)}$ be a p-closed field and G be an extension of a p-group by a torus, defined over k, as in* (13)*. A finite-dimensional representation ρ of G defined over k is p-faithful if and only $\rho_{|\,C(G)}$ is faithful.* □

5. Proof of Theorem 1.3(a)

The key step in our proof will be the following proposition.

Proposition 5.1. *Let k be a p-closed field, and G be an extension of a p-group by a torus, as in* (13)*. Then the dimension of every irreducible representation of G over k is a power of p.*

Assuming Proposition 5.1 we can easily complete the proof of Theorem 1.3(a). Indeed, by Proposition 3.4 we may assume that $k = k^{(p)}$ is p-closed. In particular, since we are assuming that $\mathrm{char}(k) \neq p$, this implies that k contains a primitive pth root of unity. (Indeed, if ζ is a p-th root of unity in k_{sep} then $d = [k(\zeta) : k]$ is prime to p; hence, $d = 1$.) Proposition 5.1 tells us that Theorem 1.2 can be applied to the exact sequence

$$1 \to C(G) \to G \to Q \to 1\,. \tag{19}$$

This yields

$$\mathrm{ed}(G; p) \geq \min\ \dim(\rho) - \dim(G)\,, \tag{20}$$

where the minimum is taken over all representations $\rho\colon G \to \mathrm{GL}(V)$ such that $\rho_{|C(G)}$ is faithful. By Corollary 4.5, $\rho_{|C(G)}$ is faithful if and only if ρ is p-faithful, and Theorem 1.3(a) follows. □

The rest of this section will be devoted to the proof of Proposition 5.1. We begin by settling it in the case where G is a finite p-group.

LEMMA 5.2. *Proposition 5.1 holds if G is a finite p-group.*

PROOF. Choose a finite Galois field extension l/k such that (i) G is constant over l and (ii) every irreducible linear representation of G over l is absolutely irreducible. Since k is assumed to be p-closed, $[l : k]$ is a power of p.

Let $A := k[G]^*$ be the dual Hopf algebra of the coordinate algebra of G. By [**Ja**, Section 8.6] a G-module structure on a k-vector space V is equivalent to an A-module structure on V. Now assume that V is an irreducible A-module and let $W \subseteq V \otimes_k l$ be an irreducible $A \otimes_k l$-submodule. Then by [**Ka**, Theorem 5.22] there exists a divisor e of $[l : k]$ such that

$$V \otimes l \simeq e\left(\bigoplus_{i=1}^{r} {}^{\sigma_i}W\right),$$

where $\sigma_i \in \mathrm{Gal}(l/k)$ and $\{{}^{\sigma_i}W \mid 1 \leq i \leq r\}$ are the pairwise non-isomorphic Galois conjugates of W. By our assumption on k, e and r are powers of p and by our choice of l, $\dim_l W = \dim_l({}^{\sigma_1}W) = \ldots = \dim_l({}^{\sigma_r}W)$ is also a power of p, since it divides the order of G_l. Hence, so is $\dim_k(V) = \dim_l V \otimes l = e(\dim_l {}^{\sigma_1}W + \cdots + \dim_l {}^{\sigma_r}W)$. □

Our proof of Proposition 5.1 in full generality will based on leveraging Lemma 5.2 as follows.

LEMMA 5.3. *Let G be an algebraic group defined over a field k and*

$$F_1 \subseteq F_2 \subseteq \cdots \subset G$$

be an ascending sequence of finite k-subgroups whose union $\cup_{n\geq 1}F_n$ is Zariski dense in G. If $\rho\colon G \to \mathrm{GL}(V)$ is an irreducible representation of G defined over k then $\rho_{|F_i}$ is irreducible for sufficiently large integers i.

PROOF. For each $d = 1, ..., \dim(V) - 1$ consider the G-action on the Grassmannian $\mathrm{Gr}(d, V)$ of d-dimensional subspaces of V. Let $X^{(d)} = \mathrm{Gr}(d, V)^G$ and $X_i^{(d)} = \mathrm{Gr}(d, V)^{F_i}$ be the subvariety of d-dimensional G- (resp. F_i-)invariant subspaces of V. Then $X_1^{(d)} \supseteq X_2^{(d)} \supseteq \ldots$ and since the union of the groups F_i is dense in G,

$$X^{(d)} = \cap_{i\geq 0} X_i^{(d)}.$$

By the Noetherian property of $\mathrm{Gr}(d, V)$, we have $X^{(d)} = X_{m_d}^{(d)}$ for some $m_d \geq 0$.

Since V does not have any G-invariant d-dimensional k-subspaces, we know that $X^{(d)}(k) = \emptyset$. Thus, $X_{m_d}^{(d)}(k) = \emptyset$, i.e., V does not have any F_{m_d}-invariant d-dimensional k-subspaces. Setting $m := \max\{m_1, \ldots, m_{\dim(V)-1}\}$, we see that $\rho_{|F_m}$ is irreducible. □

We now proceed with the proof of Proposition 5.1. By Lemmas 5.2 and 5.3, it suffices to construct a sequence of finite p-subgroups

$$F_1 \subseteq F_2 \subseteq \cdots \subset G$$

defined over k whose union $\cup_{n\geq 1}F_n$ is Zariski dense in G.

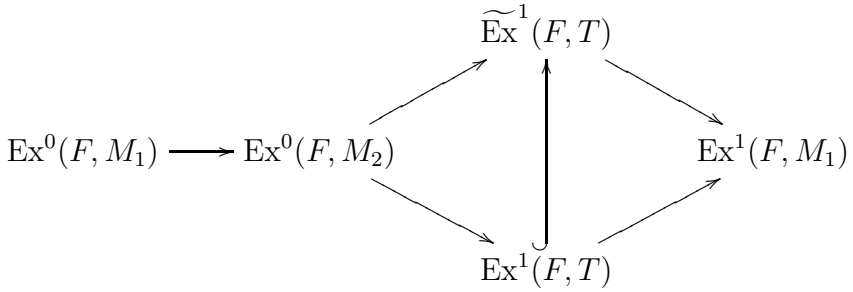
In fact, it suffices to construct one p-subgroup $F' \subset G$, defined over k such that F' surjects onto F. Indeed, once F' is constructed, we can define $F_i \subset G$ as the subgroup generated by F' and $T[p^i]$, for every $i \geq 0$. Since $\cup_{n\geq 1} F_n$ contains both F' and $T[p^i]$, for every $i \geq 0$ it is Zariski dense in G, as desired.

The following lemma, which establishes the existence of F', is thus the final step in our proof of Proposition 5.1 (and hence, of Theorem 1.3(a)).

LEMMA 5.4. *Let $1 \to T \to G \xrightarrow{\pi} F \to 1$ be an extension of a p-group F by a torus T over k. Then G has a finite p-subgroup F' with $\pi(F') = F$.*

In the case where F is split and k is algebraically closed this is proved in [**CGR**, p. 564]; cf. also the proof of [$\mathbf{BS}_1$, Lemme 5.11].

PROOF. Denote by $\widetilde{\mathrm{Ex}}^1(F,T)$ the group of equivalence classes of extensions of F by T. We claim that $\widetilde{\mathrm{Ex}}^1(F,T)$ is torsion. Let $\mathrm{Ex}^1(F,T) \subset \widetilde{\mathrm{Ex}}^1(F,T)$ be the classes of extensions which have a scheme-theoretic section (i.e. $G(K) \to F(K)$ is surjective for all K/k). There is a natural isomorphism $\mathrm{Ex}^1(F,T) \simeq H^2(F,T)$, where the latter one denotes Hochschild cohomology, see [**DG**, III. 6.2, Proposition]. By [$\mathbf{Sch}_3$] the usual restriction-corestriction arguments can be applied in Hochschild cohomology and in particular, $m \cdot H^2(F,T) = 0$ where m is the order of F. Now recall that $M \mapsto \widetilde{\mathrm{Ex}}^i(F,M)$ and $M \mapsto \mathrm{Ex}^i(F,M)$ are both derived functors of the crossed homomorphisms $M \mapsto \mathrm{Ex}^0(F,M)$, where in the first case M is in the category of F-module sheaves and in the second, F-module functors, cf. [**DG**, III. 6.2]. Since F is finite and T an affine scheme, by [$\mathbf{Sch}_1$, Satz 1.2 & Satz 3.3] there is an exact sequence of F-module schemes $1 \to T \to M_1 \to M_2 \to 1$ and an exact sequence $\mathrm{Ex}^0(F,M_1) \to \mathrm{Ex}^0(F,M_2) \to \widetilde{\mathrm{Ex}}^1(F,T) \to H^2(F,M_1) \simeq \mathrm{Ex}^1(F,M_1)$. The F-module sequence also induces a long exact sequence on $\mathrm{Ex}(F,*)$ and we have a diagram



An element in $\widetilde{\mathrm{Ex}}^1(F,T)$ can thus be killed first in $\mathrm{Ex}^1(F,M_1)$ so it comes from $\mathrm{Ex}^0(F,M_2)$. Then kill its image in $\mathrm{Ex}^1(F,T) \simeq H^2(F,T)$, so it comes from $\mathrm{Ex}^0(F,M_1)$, hence is 0 in $\widetilde{\mathrm{Ex}}^1(F,T)$. In particular we see that multiplying twice by the order m of F, $m^2 \cdot \widetilde{\mathrm{Ex}}^1(F,T) = 0$. This proves the claim.

Now let us consider the exact sequence $1 \to N \to T \xrightarrow{\times m^2} T \to 1$, where N is the kernel of multiplication by m^2. Clearly N is finite and we have an induced exact sequence

$$\widetilde{\mathrm{Ex}}^1(F,N) \to \widetilde{\mathrm{Ex}}^1(F,T) \xrightarrow{\times m^2} \widetilde{\mathrm{Ex}}^1(F,T)$$

which shows that the given extension G comes from an extension F' of F by N. Then G is the pushout of F' by $N \to T$ and we can identify F' with a subgroup of G. □

6. p-isogenies

An isogeny of algebraic groups is a surjective morphism $G \to Q$ with finite kernel. If the kernel is of order prime to p we say that the isogeny is a p-isogeny. In this section we will prove Theorem 6.1 which says that p-isogenous groups have the same essential p-dimension. This result will play a key role in the proof of Theorem 1.3(b) in Section 7.

THEOREM 6.1. *Suppose $G \to Q$ is a p-isogeny of algebraic groups over k. Then*

(a) For any p-closed field K containing k the natural map $H^1(K, G) \to H^1(K, Q)$ is bijective.

(b) $\operatorname{ed}_k(G; p) = \operatorname{ed}_k(Q; p)$.

EXAMPLE 6.2. Let E_6^{sc}, E_7^{sc} be simply connected simple groups of type E_6, E_7 respectively. In [**GR**, 9.4, 9.6] it is shown that if k is an algebraically closed field of characteristic $\neq 2$ and 3 respectively, then

$$\operatorname{ed}_k(E_6^{sc}; 2) = 3 \text{ and } \operatorname{ed}_k(E_7^{sc}; 3) = 3.$$

For the adjoint groups $E_6^{ad} = E_6^{sc}/\mu_3$, $E_7^{ad} = E_7^{sc}/\mu_2$ we therefore have

$$\operatorname{ed}_k(E_6^{ad}; 2) = 3 \text{ and } \operatorname{ed}_k(E_7^{ad}; 3) = 3.$$

We will need two lemmas.

LEMMA 6.3. *Let N be a finite algebraic group over k ($\operatorname{char} k \neq p$). The following are equivalent:*

(a) p does not divide the order of N.

(b) p does not divide the order of $N(k_{\mathrm{alg}})$.

If N is also assumed to be abelian, denote by $N[p]$ the p-torsion subgroup of N. The following are equivalent to the above conditions.

(a′) $N[p](k_{\mathrm{alg}}) = \{1\}$.

(b′) $N[p](k^{(p)}) = \{1\}$.

PROOF. (a) $\iff$ (b): Let N° be the connected component of N and $N^{et} = N/N^\circ$ the étale quotient. Recall that the order of a finite algebraic group N over k is defined as $|N| = \dim_k k[N]$ and $|N| = |N^\circ||N^{et}|$, see for example [**Ta**]. If $\operatorname{char} k = 0$, N° is trivial, if $\operatorname{char} k = q \neq p$ is positive, $|N^\circ|$ is a power of q. Hence N is of order prime to p if and only if the étale algebraic group N^{et} is. Since N° is connected and finite, $N^\circ(k_{\mathrm{alg}}) = \{1\}$ and so $N(k_{\mathrm{alg}})$ is of order prime to p if and only if the group $N^{et}(k_{\mathrm{alg}})$ is. Then $|N^{et}| = \dim_k k[N^{et}] = |N^{et}(k_{\mathrm{alg}})|$, cf. [**Bou**, V.29 Corollary].

(b) $\iff$ (a′) $\Rightarrow$ (b′) are clear.

(a′) $\Leftarrow$ (b′): Suppose $N[p](k_{\mathrm{alg}})$ is nontrivial. The Galois group $\Gamma = \operatorname{Gal}(k_{\mathrm{alg}}/k^{(p)})$ is a pro-p group and acts on the p-group $N[p](k_{\mathrm{alg}})$. The image of Γ in $\operatorname{Aut}(N[p](k_{\mathrm{alg}}))$ is again a (finite) p-group and the size of every Γ-orbit in $N[p](k_{\mathrm{alg}})$ is a power of p. Since

Γ fixes the identity in $N[p](k_{\rm alg})$, this is only possible if it also fixes at least $p-1$ more elements. It follows that $N[p](k^{(p)})$ contains at least p elements, a contradiction. □

REMARK 6.4. Part (b′) could be replaced by the slightly stronger statement that $N[p](k^{(p)} \cap k_{\rm sep}) = \{1\}$, but we won't need this in the sequel.

LEMMA 6.5. *Let Γ be a profinite group, G an (abstract) finite Γ-group and $|\Gamma|, |G|$ coprime. Then $H^1(\Gamma, G) = \{1\}$.*

The case where Γ is finite and G abelian is classical. In the generality we stated, this lemma is also known [**Se**$_2$, I.5, ex. 2].

PROOF OF THEOREM 6.1. (a) Let N be the kernel of $G \to Q$ and $K = K^{(p)}$ be a p-closed field over k. Since $K_{\rm sep} = K_{\rm alg}$ (see Proposition 3.2(b)), the sequence of $K_{\rm sep}$-points $1 \to N(K_{\rm sep}) \to G(K_{\rm sep}) \to Q(K_{\rm sep}) \to 1$ is exact. By Lemma 6.3, the order of $N(K_{\rm sep})$ is not divisible by p and therefore coprime to the order of $\Psi = {\rm Gal}(K_{\rm sep}/K)$. Thus $H^1(K, N) = \{1\}$ (Lemma 6.5). Similarly, if ${}_cN$ is the group N twisted by a cocycle $c : \Psi \to G$, ${}_cN(K_{\rm sep}) = N(K_{\rm sep})$ is of order prime to p and $H^1(K, {}_cN) = \{1\}$. It follows that $H^1(K, G) \to H^1(K, Q)$ is injective, cf. [**Se**$_2$, I.5.5].

Surjectivity is a consequence of [**Se**$_2$, I. Proposition 46] and the fact that the q-cohomological dimension of Ψ is 0 for any divisor q of $|N(K_{\rm sep})|$ (Proposition 3.2).

This concludes the proof of part (a). Part (b) immediately follows from (a) and Proposition 3.4. □

7. Proof of Theorem 1.3(b)

Let $G = T \times F$, where T is a torus and F is a finite p-group, defined over a k. Our goal is to show that

$$\operatorname{ed}_k(G; p) \le \dim(\rho) - \dim G\,, \tag{21}$$

where ρ is a p-faithful representation of G defined over k.

LEMMA 7.1. *If a representation $\rho\colon G \to {\rm GL}(V)$ is p-faithful, then $G/\ker(\rho) \to {\rm GL}(V)$ is generically free. In other words, ρ is p-generically free.*

PROOF. Since $\ker(\rho)$ has order prime to p, its image under the projection map $G = T \times F \to F$ is trivial. Hence $\ker(\rho) \subset T$ and T/N is again a torus. So without loss of generality, we may assume ρ is faithful.

To show the claim we may assume that $k = k_{\rm alg}$. Indeed if U is a $G_{k_{\rm alg}}$-invariant dense open subset of $V_{k_{\rm alg}}$ defined over $k_{\rm alg}$ with free $G_{k_{\rm alg}}$-action then the union of all translates of U by elements of ${\rm Gal}(k_{\rm sep}/k)$ descends to a G-invariant dense open subset of V defined over k with free G-action, see [**Sp**, Prop. 11.2.8].

Now since every faithful T-variety is generically free there exists a T-invariant dense open subset U_1 of V defined over k on which T acts freely. Replacing U_1 by the intersection of all gU_1 where g runs over the elements of $F(k)$ we may assume that U_1 is G-invariant (note that F is smooth and $k = k_{\rm alg}$).

Let n be the order of F. Let U_2 be the complement of the fixed point sets of non-trivial elements of $F(k)$. Then U_2 is a dense open subset of V defined over k and it is (automatically) G-invariant. Clearly F acts freely on U_2.

Set $U := U_1 \cap U_2$, which is a G-invariant dense open subset of V defined over k. It remains to show that the G-action on U is free. First observe that $G(k)$ acts freely on $U(k)$ (where $k = k_{\mathrm{alg}}$). Indeed, assume $1 \neq g = (t, f) \in G(k)$ stabilizes some $v \in U(k)$. Since $v \in U_2(k)$, $t^n \neq 1$. Then $1 \neq g^n = (t^n, 1)$ lies in T and stabilizes v. Since $v \in U_1(k)$, this is a contradiction.

Moreover the Lie-stabilizer $\mathrm{Lie}(G_x)$ of every $x \in U(k)$ is trivial because $\mathrm{Lie}(G_x) = \mathrm{Lie}(T_x)$ and T acts freely on U. The claim follows. □

Now suppose ρ is any p-faithful representation of G. Then (11) yields

$$\mathrm{ed}_k(G/N; p) \leq \dim(\rho) - \dim(G/\ker(\rho)) = \dim(\rho) - \dim(G)\,.$$

By Theorem 6.1

$$\mathrm{ed}_k(G; p) = \mathrm{ed}(G/N; p) \leq \dim(\rho) - \dim(G)\,,$$

as desired. This completes the proof of (21) and thus of Theorem 1.3(b). □

Corollary 7.2. *Let G be a finite algebraic group over a p-closed field $k = k^{(p)}$. Then G has a Sylow-p subgroup G_p defined over k and*

$$\mathrm{ed}_k(G; p) = \mathrm{ed}_k(G_p; p) = \mathrm{ed}_k(G_p) = \min \dim(\rho)$$

where the minimum is taken over all faithful representations of G_p over k.

Proof. By assumption, $\Gamma = \mathrm{Gal}(k_{\mathrm{sep}}/k)$ is a pro-p group. It acts on the set of Sylow-p subgroups of $G(k_{\mathrm{sep}})$. Since the number of such subgroups is prime to p, Γ fixes at least one of them and by Galois descent one obtains a subgroup G_p of G. By Lemma 6.3, G_p is a Sylow-p subgroup of G. The first equality $\mathrm{ed}_k(G; p) = \mathrm{ed}_k(G_p; p)$ is shown in [**MR**$_1$, 4.1] (the reference is for smooth groups but can be generalized to the non-smooth case as well). The minimal G_p-representation ρ from Theorem 1.3(b) is faithful and thus $\mathrm{ed}_k(G_p) \leq \dim(\rho)$, see for example [**BF**, Prop. 4.11]. The Corollary follows. □

Remark 7.3. Two Sylow-p subgroups of G defined over $k = k^{(p)}$ do not need to be isomorphic over k.

8. An additivity theorem

The purpose of this section is to prove the following:

Theorem 8.1. *Let G_1 and G_2 be direct products of tori and p-groups over a field k. Then $\mathrm{ed}_k(G_1 \times G_2; p) = \mathrm{ed}_k(G_1; p) + \mathrm{ed}_k(G_2; p)$.*

Let G be an algebraic group defined over k and C be a k-subgroup of G. Denote the minimal dimension of a representation ρ of G (defined over k) such that $\rho_{|C}$ is faithful by $f(G, C)$.

LEMMA 8.2. *For $i = 1, 2$ let G_i be an algebraic group defined over k and C_i be a central k-subgroup of G_i. Assume that C_i is isomorphic to $\mu_p^{r_i}$ over k for some $r_1, r_2 \geq 0$. Then*

$$f(G_1 \times G_1; C_1 \times C_2) = f(G_1; C_1) + f(G_2; C_2)\,.$$

Our argument is a variant of the proof of [**KM**, Theorem 5.1], where G is assumed to be a (constant) finite p-group and C is the socle of G.

PROOF. For $i = 1, 2$ let $\pi_i \colon G_1 \times G_2 \to G_i$ be the natural projection and $\epsilon_i \colon G_i \to G_1 \times G_2$ be the natural inclusion.

If ρ_i is a d_i-dimensional k-representation of G_i whose restriction to C_i is faithful, then clearly $\rho_1 \circ \pi_1 \oplus \rho_2 \circ \pi_2$ is a $d_1 + d_2$-dimensional representation of $G_1 \times G_2$ whose restriction to $C_1 \times C_2$ is faithful. This shows that

$$f(G_1 \times G_1; C_1 \times C_2) \leq f(G_1; C_1) + f(G_2; C_2)\,.$$

To prove the opposite inequality, let $\rho \colon G_1 \times G_2 \to \mathrm{GL}(V)$ be a k-representation such that $\rho_{|\,C_1 \times C_2}$ is faithful, and of minimal dimension

$$d = f(G_1 \times G_1; C_1 \times C_2)$$

with this property. Let $\rho_1, \rho_2, \dots, \rho_n$ denote the irreducible decomposition factors in a decomposition series of ρ. Since $C_1 \times C_2$ is central in $G_1 \times G_2$, each ρ_i restricts to a multiplicative character of $C_1 \times C_2$ which we will denote by χ_i. Moreover since $C_1 \times C_2 \simeq \mu_p^{r_1 + r_2}$ is linearly reductive $\rho_{|\,C_1 \times C_2}$ is a direct sum $\chi_1^{\oplus d_1} \oplus \dots \oplus \chi_n^{\oplus d_n}$ where $d_i = \dim V_i$. It is easy to see that the following conditions are equivalent:

(i) $\rho_{|\,C_1 \times C_2}$ is faithful,

(ii) $\chi_1, \dots, \chi_n$ generate $(C_1 \times C_2)^*$ as an abelian group.

In particular we may assume that $\rho = \rho_1 \oplus \dots \oplus \rho_n$. Since C_i is isomorphic to $\mu_p^{r_i}$, we will think of $(C_1 \times C_2)^*$ as a $\mathbb{F}_p$-vector space of dimension $r_1 + r_2$. Since (i) $\Leftrightarrow$ (ii) above, we know that $\chi_1, \dots, \chi_n$ span $(C_1 \times C_2)^*$. In fact, they form a basis of $(C_1 \times C_2)^*$, i.e., $n = r_1 + r_2$. Indeed, if they were not linearly independent we would be able to drop some of the terms in the irreducible decomposition $\rho_1 \oplus \dots \oplus \rho_n$, so that the restriction of the resulting representation to $C_1 \times C_2$ would still be faithful, contradicting the minimality of $\dim(\rho)$.

We claim that it is always possible to replace each ρ_j by ρ'_j, where ρ'_j is either $\rho_j \circ \epsilon_1 \circ \pi_1$ or $\rho_j \circ \epsilon_2 \circ \pi_2$ such that the restriction of the resulting representation $\rho' = \rho'_1 \oplus \dots \oplus \rho'_n$ to $C_1 \times C_2$ remains faithful. Since $\dim(\rho_i) = \dim(\rho'_i)$, we see that $\dim(\rho') = \dim(\rho)$. Moreover, ρ' will then be of the form $\alpha_1 \circ \pi_1 \oplus \alpha_2 \circ \pi_2$, where α_i is a representation of G_i whose restriction to C_i is faithful. Thus, if we can prove the above claim, we will have

$$\begin{aligned} f(G_1 \times G_1; C_1 \times C_2) &= \dim(\rho) = \dim(\rho') = \dim(\alpha_1) + \dim(\alpha_2) \\ &\geq f(G_1, C_1) + f(G_2, C_2)\,, \end{aligned}$$

as desired.

To prove the claim, we will define ρ'_j recursively for $j = 1, \dots, n$. Suppose $\rho'_1, \dots, \rho'_{j-1}$ have already be defined, so that the restriction of

$$\rho'_1 \oplus \dots \oplus \rho'_{j-1} \oplus \rho_j \dots \oplus \rho_n$$

to $C_1 \times C_2$ is faithful. For notational simplicity, we will assume that $\rho_1 = \rho'_1, \dots, \rho_{j-1} = \rho'_{j-1}$. Note that

$$\chi_j = (\chi_j \circ \epsilon_1 \circ \pi_1) + (\chi_j \circ \epsilon_2 \circ \pi_2)\,.$$

Since $\chi_1, \dots, \chi_n$ form a basis $(C_1 \times C_2)^*$ as an $\mathbb{F}_p$-vector space, we see that (a) $\chi_j \circ \epsilon_1 \circ \pi_1$ or (b) $\chi_j \circ \epsilon_2 \circ \pi_2$ does not lie in $\mathrm{Span}_{\mathbb{F}_p}(\chi_1, \dots, \chi_{j-1}, \chi_{j+1}, \dots, \chi_n)$. Set

$$\rho'_j := \begin{cases} \rho_j \circ \epsilon_1 \circ \pi_1 \text{ in case (a), and} \\ \rho_j \circ \epsilon_2 \circ \pi_2, \text{ otherwise.} \end{cases}$$

Using the equivalence of (i) and (ii) above, we see that the restriction of

$$\rho_1 \oplus \dots \oplus \rho_{j-1} \oplus \rho'_j \oplus \rho_{j+1}, \dots \oplus \rho_n$$

to C is faithful. This completes the proof of the claim and thus of Lemma 8.2. □

Proof of Theorem 8.1. We can pass to a p-closure $k^{(p)}$ by Lemma 3.3. Let $C(G)$ be as in Definition 4.2. By Theorem 1.3(b)

$$\mathrm{ed}(G; p) = f(G, C(G)) - \dim G\,;$$

cf. Corollary 4.5. Furthermore, we have $C(G_1 \times G_2) = C(G_1) \times C(G_2)$; cf. Lemma 4.3(d). Applying Lemma 8.2 finishes the proof. □

9. Modules and lattices

In this section we rewrite the value of $\mathrm{ed}_k(G; p)$ in terms of the character module $X(G)$ for an *abelian* group G which is an extension of a p-group and a torus. Moreover we show that tori with locally isomorphic character lattices have the same essential dimension. We need the following preliminaries.

Let R be a commutative ring (we use $R = \mathbb{Z}$ and $R = \mathbb{Z}_{(p)}$ mostly) and A an R-algebra. An A-module is called an *A-lattice* if it is finitely generated and projective as an R-module. For $A = \mathbb{Z}\Gamma$ (Γ a group) this is as usual a free abelian group of finite rank with an action of Γ. Particular cases of $R\Gamma$-lattices are *permutation lattices* $L = R[\Lambda]$ where Λ is a Γ-set.

For $\Gamma = \mathrm{Gal}(k_{\mathrm{sep}}/k)$ the absolute Galois group of k we tacitly assume that our $R\Gamma$-lattices are continuous, i.e. Γ acts through a finite quotient $\overline{\Gamma}$. Under the anti-equivalence Diag a $\mathbb{Z}\Gamma$-lattice corresponds to an algebraic k-torus. A torus S is called *quasi split* if it corresponds to a permutation lattice. Equivalently $S \simeq R_{E/k}(\mathbb{G}_{\mathbf{m}})$ where E/k is étale and $R_{E/k}$ denotes Weil restriction.

Recall that $\mathbb{Z}_{(p)}$ denotes the localization of the ring $\mathbb{Z}$ at the prime ideal (p). For a $\mathbb{Z}$-module M we also write $M_{(p)} := \mathbb{Z}_{(p)} \otimes M$.

When $\Gamma = \mathrm{Gal}(k_{\mathrm{sep}}/k)$ we will often pass from $\mathbb{Z}\Gamma$-lattices to $\mathbb{Z}_{(p)}\Gamma$-lattices. This corresponds to identifying p-isogeneous tori:

LEMMA 9.1. *Let $\Gamma = \mathrm{Gal}(k_{\mathrm{sep}}/k)$ and let M, L be $\mathbb{Z}\Gamma$-lattices. Then the following statements are equivalent:*

(a) $L_{(p)} \simeq M_{(p)}$.
(b) There exists an injective map $\varphi\colon L \to M$ of $\mathbb{Z}\Gamma$-modules with cokernel Q finite of order prime to p.
(c) There exists a p-isogeny $\mathrm{Diag}(M) \to \mathrm{Diag}(L)$.

PROOF. The equivalence (b) $\Leftrightarrow$ (c) is clear from the anti-equivalence of Diag.

The implication (b) $\Rightarrow$ (a) follows from $Q_{(p)} = 0$ and that tensoring with $\mathbb{Z}_{(p)}$ is exact.

For the implication (a) $\Rightarrow$ (b) we use that L and M can be considered as subsets of $L_{(p)}$ (resp. $M_{(p)}$). The image of L under a map $\alpha\colon L_{(p)} \to M_{(p)}$ of $\mathbb{Z}_{(p)}\Gamma$-modules lands in $\frac{1}{m}M$ for some $m \in \mathbb{N}$ (prime to p) and the index of $\alpha(L)$ in $\frac{1}{m}M$ is finite and prime to p if α is surjective. Since $\frac{1}{m}M \simeq M$ as $\mathbb{Z}\Gamma$-modules the claim follows. □

COROLLARY 9.2. *Let G be an abelian group which is an extension of a p-group by a torus over k and $\Gamma := \mathrm{Gal}(k_{\mathrm{sep}}/k)$ be the absolute Galois group of $k = k^{(p)}$. Let Γ act through a finite quotient $\overline{\Gamma}$ on $X(G)$. Then*

$$\mathrm{ed}_k(G; p) = \min \mathrm{rank}\, L - \dim G\,,$$

where the minimum is taken over all permutation $\mathbb{Z}\overline{\Gamma}$-lattices L which admit a map of $\mathbb{Z}\overline{\Gamma}$-modules to $X(G)$ with cokernel finite of order prime to p.

If G is a torus, then the minimum can also be taken over all $\mathbb{Z}_{(p)}\overline{\Gamma}$-lattices L which admit a surjective map of $\mathbb{Z}_{(p)}\overline{\Gamma}$-modules to $X(G)_{(p)}$.

PROOF. Let us prove the first claim. In view of Theorem 1.3(a) it suffices to show that the least dimension of a p-faithful representation of $G_{k^{(p)}}$ over $k^{(p)}$ is equal to the least rank of a permutation $\mathbb{Z}\overline{\Gamma}$-module L which admits a map to $X(G)$ with cokernel finite of order prime to p.

Assume we have such a map $L \to X(G)$. Using the anti-equivalence Diag we obtain a p-isogeny $G \to \mathrm{Diag}(L)$. We can embed the quasi-split torus $\mathrm{Diag}(L)$ in GL_n where $n = \mathrm{rank}\, L$ [**Vo**, Section 6.1]. This yields a p-faithful representation of G of dimension $\mathrm{rank}\, L$.

Conversely let $\rho\colon G \to \mathrm{GL}(V)$ be a p-faithful representation of G. Since G_{sep} is diagonalizable, there exist characters $\chi_1, \dots, \chi_n \in X(G)$ such that G acts on V_{sep} via diagonal matrices with entries $\chi_1(g), \dots, \chi_n(g)$ (for $g \in G$) with respect to a suitable basis of V_{sep}. Moreover $\overline{\Gamma}$ permutes the set $\Lambda := \{\chi_1, \dots, \chi_n\}$. Define a map $\varphi\colon \mathbb{Z}[\Lambda] \to X(G)$ of $\mathbb{Z}\overline{\Gamma}$-modules by sending the basis element $\chi_i \in \Lambda$ of $L := \mathbb{Z}[\Lambda]$ to itself. Then the p-faithfulness of ρ implies that the cokernel of φ is finite and of order prime to p. Moreover $\mathrm{rank}\, L = |\Lambda| \le n = \dim V$.

Now consider the case where G is a torus. Assume we have a surjective map $\alpha\colon L \to X(G)_{(p)}$ of $\mathbb{Z}_{(p)}\overline{\Gamma}$-modules where $L = \mathbb{Z}_{(p)}[\Lambda]$ is permutation, Λ a $\overline{\Gamma}$-set. Then $\alpha(\Lambda) \subseteq \frac{1}{m}X(G)$ for some $m \in \mathbb{N}$ prime to p (note that $\frac{1}{m}X(G)$ can be considered as a subset of $X(G)_{(p)}$ since $X(G)$ is torsion free). By construction the induced map $\mathbb{Z}[\Lambda] \to \frac{1}{m}X(G) \simeq$

$X(G)$ becomes surjective after localization at p, hence its cokernel is finite of order prime to p. □

COROLLARY 9.3. *Let A be a finite (twisted) cyclic p-group over k. Let l/k be a minimal Galois splitting field of A. Then*

$$\operatorname{ed}(A;p) = |\operatorname{Gal}(l/k)|_p = |\operatorname{Gal}(l^{(p)}/k^{(p)})|,$$

where $|\operatorname{Gal}(l/k)|_p$ denotes the p-primary part of $|\operatorname{Gal}(l/k)|$.

PROOF. The second equality follows from the properties of the p-closure. Moreover $l^{(p)}$ is a minimal Galois splitting field of $A_{k^{(p)}}$. Since the essential p-dimension of A does not change when passing to the p-closure, we can assume $k = k^{(p)}$. Set $\Gamma = \operatorname{Gal}(l/k)$ which is now automatically a p-group. By Corollary 9.2 $\operatorname{ed}(A;p)$ is equal to the least cardinality of a Γ-set Λ such that there exists a map $\varphi\colon \mathbb{Z}[\Lambda] \to X(A)$ of $\mathbb{Z}\Gamma$-modules with cokernel finite of order prime to p. The group $X(A)$ is a (cyclic) p-group, hence φ must be surjective. Moreover Γ acts faithfully on $X(A)$. Surjectivity of φ implies that some element $\lambda \in \Lambda$ maps to a generator a of $X(A)$. Hence $|\Lambda| \geq |\Gamma\lambda| \geq |\Gamma a| = |\Gamma|$. Conversely we have a surjective homomorphism $\mathbb{Z}[\Gamma a] \to X(A)$ that sends a to itself. Hence the claim follows. □

REMARK 9.4. In the case of twisted cyclic groups of order 4 Corollary 9.3 is due to Rost [**Ro**] (see also [**BF**, Theorem 7.6]), and in the case of cyclic groups of order 8 to Bayarmagnai [**Ba**]. Note that for $p = 2$ we have $|\operatorname{Gal}(l/k)|_p = |\operatorname{Gal}(l/k)|$ above since the automorphism group of $X(A) \simeq \mathbb{Z}/2^n\mathbb{Z}$ is a 2-group. The case of constant groups of arbitrary prime power order is due to Florence [**Fl**]; it is now a special case of the Karpenko-Merkurjev Theorem 1.1.

10. Proof of Theorem 1.3(c)

We will prove Theorem 1.3(c) by using the lattice point of view from Section 9 and the additivity theorem from Section 8.

Let $\overline{\Gamma}$ be a finite group. Two $\mathbb{Z}\overline{\Gamma}$-lattices M, N are said to be in the same *genus* if $M_{(p)} \simeq N_{(p)}$ for all primes p, cf. [**CR**, 31A]. It is sufficient to check this condition for divisors p of the order of $\overline{\Gamma}$. By a theorem of A.V. Roĭter [**CR**, Theorem 31.28] M and N are in the same genus if and only if there exists a $\mathbb{Z}\overline{\Gamma}$-lattice L in the genus of the free $\mathbb{Z}\overline{\Gamma}$-lattice of rank one such that $M \oplus \mathbb{Z}\overline{\Gamma} \simeq N \oplus L$. This has the following consequence for essential dimension:

PROPOSITION 10.1. *Let T, T' be k-tori. If the lattices $X(T), X(T')$ belong to the same genus then $H^1(K,T) = H^1(K,T')$ for all field extensions of K/k. In particular*

$$\operatorname{ed}_k(T) = \operatorname{ed}_k(T') \text{ and } \operatorname{ed}_k(T;\ell) = \operatorname{ed}_k(T';\ell) \text{ for all primes } \ell.$$

PROOF. Let $\operatorname{Gal}(k_{\mathrm{sep}}/k)$ act through a finite quotient $\overline{\Gamma}$ on $X(T)$ and $X(T')$. By assumption there exists a $\mathbb{Z}\overline{\Gamma}$-lattice L in the genus of $\mathbb{Z}\overline{\Gamma}$ such that $X(T) \oplus \mathbb{Z}\overline{\Gamma} \simeq X(T') \oplus L$. The torus $S = \operatorname{Diag}(\mathbb{Z}\overline{\Gamma})$ has $H^1(K,S) = \{1\}$ for all field extensions K/k. The same applies to the torus $S' := \operatorname{Diag}(L)$ since L is a direct summand of $\mathbb{Z}\overline{\Gamma} \oplus \mathbb{Z}\overline{\Gamma}$. Therefore

$H^1(K,T) = H^1(K,T\times S) = H^1(K,T'\times S') = H^1(K,T')$ for all K/k. This concludes the proof. □

COROLLARY 10.2. *Let $k = k^{(p)}$ be a p-closed field and T a k-torus. Then*

$$\operatorname{ed}_k(T) = \operatorname{ed}_k(T;p) = \min \dim(\rho) - \dim T,$$

where the minimum is taken over all p-faithful representations of T.

PROOF. The second equality follows from Theorem 1.3(a) and the inequality $\operatorname{ed}_k(T;p) \leq \operatorname{ed}_k(T)$ is clear. Hence it suffices to show $\operatorname{ed}_k(T) \leq \operatorname{ed}_k(T;p)$. Let $\rho\colon T \to \mathrm{GL}(V)$ be a p-faithful representation of minimal dimension so that $\operatorname{ed}_k(T;p) = \dim \rho - \dim T$. The representation ρ can be considered as a faithful representation of the torus $T' = T/N$ where $N := \ker \rho$ is finite of order prime to p. By construction the character lattices $X(T)$ and $X(T')$ are isomorphic after localization at p. Since $\mathrm{Gal}(k_{\mathrm{sep}}/k)$ is a (profinite) p-group it follows that $X(T)$ and $X(T')$ belong to the same genus. Hence by Proposition 10.1 we have $\operatorname{ed}_k(T') = \operatorname{ed}_k(T)$. Moreover $\operatorname{ed}_k(T') \leq \dim \rho - \dim T'$, since ρ is a generically free representation of T'. This finishes the proof. □

PROOF OF THEOREM 1.3(B). The equality $\operatorname{ed}_{k^{(p)}}(G_{k^{(p)}};p) = \operatorname{ed}_k(G;p)$ follows from Lemma 3.3. Now we are assuming $G = T\times F$ for a torus T and a p-group F over k, which is p-closed. Notice that a minimal p-faithful representation of F from Theorem 1.3(a) is also faithful, and therefore $\operatorname{ed}_k(F;p) = \operatorname{ed}_k(F)$. Combining this with Corollary 10.2 and the additivity Theorem 8.1, we see

$$\operatorname{ed}(T\times F) \leq \operatorname{ed}(T) + \operatorname{ed}(F) = \operatorname{ed}(T;p) + \operatorname{ed}(F;p) = \operatorname{ed}(T\times F;p) \leq \operatorname{ed}(T\times F).$$

This completes the proof. □

REMARK 10.3. The following example shows that "p-faithful" cannot be replaced by "faithful" in the statement of Theorem 1.3(a) (and Corollary 10.2), even in the case where G is a torus.

Let p be a prime number such that the ideal class group of $\mathbb{Q}(\zeta_p)$ is non-trivial (this applies to all but finitely many primes, e.g. to $p = 23$). This means that the subring $R = \mathbb{Z}[\zeta_p] \subseteq \mathbb{Q}(\zeta_p)$ of algebraic integers has non-principal ideals. Let k be a field which admits a Galois extension l of degree p and let $\Gamma := \mathrm{Gal}(k_{\mathrm{sep}}/k)$, $\overline{\Gamma} := \mathrm{Gal}(l/k) \simeq \Gamma/\Gamma_l \simeq C_p$ where $\Gamma_l = \mathrm{Gal}(k_{\mathrm{sep}}/l)$ and C_p denotes the cyclic group of order p.

We endow the ring R with a $\mathbb{Z}\Gamma$-module structure through the quotient map $\Gamma \to \overline{\Gamma}$ by letting a generator of $\overline{\Gamma}$ act on R via multiplication by ζ_p. The k-torus $Q := \mathrm{Diag}(R)$ is isomorphic to the Weil restriction $R_{l/k}(\mathbb{G}_{\mathbf{m}})$ and has a p-dimensional faithful representation. We will construct a k-torus G with a p-isogeny $G \to Q$, such that G does not have a p-dimensional faithful representation.

Let I be a non-principal ideal of R. We may consider I as a $\mathbb{Z}\Gamma$-module and set $G := \mathrm{Diag}(I)$. We first show that I and R become isomorphic as $\mathbb{Z}\Gamma$-modules after localization at p. For this purpose let $I^* = \{x \in \mathbb{Q}(\zeta_p) \mid xI \subseteq R\}$ denote the inverse fractional ideal. We have $I \oplus I^* \simeq R \oplus R$ by [**CR**, Theorem 34.31]. The Krull-Schmidt Theorem [**CR**, Theorem 36.1] for $\mathbb{Z}_{(p)}C_p$-lattices implies $I_{(p)} \simeq R_{(p)}$, hence the claim. Therefore

by Lemma 9.1 there exists a p-isogeny $G \to Q$, which shows in particular that G has a p-faithful representation of dimension p.

Assume that G has a p-dimensional faithful representation. Similarly as in the proof of Corollary 9.2 this would imply the existence of a surjective map of $\mathbb{Z}\Gamma$-lattices $\mathbb{Z}\overline{\Gamma} \to I$. However such a map cannot exist since I is non-principal, hence non-cyclic as a $\mathbb{Z}\Gamma$-module.

11. Tori of essential dimension ≤ 1

THEOREM 11.1. *Let $k = k^{(p)}$ be a p-closed field, $\Gamma = \mathrm{Gal}(k_{\mathrm{alg}}/k)$ be the absolute Galois group of k and T be a torus over k. Then the following conditions are equivalent:*

(a) $\mathrm{ed}_k(T) = 0$.
(b) $\mathrm{ed}_k(T; p) = 0$.
(c) $H^1(K, T) = \{1\}$ *for any p-closed field K containing k.*
(d) $X(T)_{(p)}$ *is a $\mathbb{Z}_{(p)}\Gamma$-permutation module.*
(e) $X(T)$ *is an invertible $\mathbb{Z}\Gamma$-lattice (i.e. a direct summand of a permutation lattice).*
(f) There is a torus S over k and an isomorphism

$$T \times S \simeq \mathrm{R}_{E/k}(\mathbb{G}_{\boldsymbol{m}}),$$

for some étale algebra E over k.
(g) $H^1(K, T) = \{1\}$ *for any field K containing k.*

REMARK 11.2. A prime p for which any of these statements fails is called a *torsion prime* of T.

PROOF. (a) $\Leftrightarrow$ (b) by Theorem 1.3(c).

(b) $\Leftrightarrow$ (c) follows from [**Me**$_1$, Proposition 4.4].

(b) $\Rightarrow$ (d) follows from Corollary 9.2. Indeed, $\mathrm{ed}_k(T; p) = 0$ implies the existence of a $\mathbb{Z}_{(p)}\Gamma$-permutation lattice L together with a surjective homomorphism $\alpha : L \to X(T)_{(p)}$ such that $\operatorname{rank} L = \operatorname{rank} X(T)_{(p)}$. It follows that α is injective and $X(T)_{(p)} \simeq L$.

(d) $\Rightarrow$ (e): Let L be a $\mathbb{Z}\Gamma$-permutation lattice such that $L_{(p)} \simeq X(T)_{(p)}$. Then by [**CR**, Corollary 31.7] there is a $\mathbb{Z}\Gamma$-lattice L' such that $L \oplus L \simeq X(T) \oplus L'$.

(e) $\Leftrightarrow$ (f): A permutation lattice P can be written as

$$P = \bigoplus_{i+1}^{m} \mathbb{Z}[\Gamma/\Gamma_{L_i}],$$

for some (separable) extensions L_i/k and $\Gamma_{L_i} = \mathrm{Gal}(k_{\mathrm{alg}}/L_i)$. Set $E = L_1 \times \cdots \times L_m$. The torus corresponding to P is exactly $\mathrm{R}_{E/k}(\mathbb{G}_{\mathbf{m}})$, cf. [**Vo**, 3. Example 19].

(f) $\Rightarrow$ (g) because $H^1(K, \mathrm{R}_{E/k}(\mathbb{G}_{\mathbf{m}})) = \{1\}$.

(g) $\Rightarrow$ (a) is obvious from the definition of $\mathrm{ed}_k(T)$. □

EXAMPLE 11.3. Let T be a torus over k of rank $< p - 1$. Then $\mathrm{ed}_k(T; p) = 0$. This follows from the fact that there is no non-trivial integral representation of dimension $< p - 1$ of any p-group, see for example [**AP**, Satz]. Thus any finite quotient of $\Gamma = \mathrm{Gal}(k_{\mathrm{alg}}/k)$ acts trivially on $X(T)$ and so does Γ.

REMARK 11.4. The equivalence of parts (e) and (g) can also be deduced from [**CTS**, Proposition 7.4].

THEOREM 11.5. *Let p be an odd prime, T an algebraic torus over k, and $\Gamma = \mathrm{Gal}(k_{\mathrm{alg}}/k^{(p)})$.*

(a) $\mathrm{ed}(T;p) \le 1$ *iff there exists a Γ-set Λ and an $m \in \mathbb{Z}[\Lambda]$ fixed by Γ such that $X(T)_{(p)} \cong \mathbb{Z}_{(p)}[\Lambda]/\langle m\rangle$ as $\mathbb{Z}_{(p)}\Gamma$-lattices.*

(b) $\mathrm{ed}(T;p) = 1$ *iff $m = \sum a_\lambda \lambda$ from part (a) is not* 0 *and for any $\lambda \in \Lambda$ fixed by Γ, $a_\lambda = 0 \mod p$.*

(c) If $\mathrm{ed}(T;p) = 1$ *then $T_{k^{(p)}} \cong T' \times S$ where $\mathrm{ed}_{k^{(p)}}(S;p) = 0$ and $X(T')_{(p)}$ is an indecomposable $\mathbb{Z}_{(p)}\Gamma$-lattice, and $\mathrm{ed}_{k^{(p)}}(T';p) = 1$.*

PROOF. (a) If $\mathrm{ed}(T;p) = 1$, then by Corollary 9.2 there is a map of $\mathbb{Z}\Gamma$-lattices from $\mathbb{Z}[\Lambda]$ to $X(T)$ which becomes surjective after localization at p and whose kernel is generated by one element. Since the kernel is stable under Γ, any element of Γ sends a generator m to either itself or its negative. Since p is odd, m must be fixed by Γ.

The $\mathrm{ed}(T;p) = 0$ case and the converse follows from Theorem 1.4 or Corollary 9.2.

(b) Assume we are in the situation of (a), and say $\lambda_0 \in \Lambda$ is fixed by Γ and a_{λ_0} is not $0 \mod p$. Then $X(T)_{(p)} \cong \mathbb{Z}_{(p)}[\Lambda - \{\lambda_0\}]$, so by Theorem 11.1 we have $\mathrm{ed}(T;p) = 0$.

Conversely, assume $\mathrm{ed}(T;p) = 0$. Then by Theorem 11.1, we have an exact sequence $0 \to \langle m\rangle \to \mathbb{Z}_{(p)}[\Lambda] \to \mathbb{Z}_{(p)}[\Lambda'] \to 0$ for some Γ-set Λ' with one fewer element than Λ. We have

$$\mathrm{Ext}^1_\Gamma(\mathbb{Z}_{(p)}[\Lambda'], \mathbb{Z}_{(p)}) = (0)$$

by [**CTS**, Key Lemma 2.1(i)] together with the Change of Rings Theorem [**CR**, 8.16]; therefore this sequence splits. In other words, there exists a $\mathbb{Z}_{(p)}\Gamma$-module homomorphism $f\colon \mathbb{Z}_{(p)}[\Lambda] \to \mathbb{Z}_{(p)}[\Lambda]$ such that the image of f is $\langle m\rangle$ and $f(m) = m$. Then we can define $c_\lambda \in \mathbb{Z}_{(p)}$ by $f(\lambda) = c_\lambda m$. Note that $f(\gamma(\lambda)) = f(\lambda)$ and thus

$$c_{\gamma(\lambda)} = c_\lambda \tag{22}$$

for every $\lambda \in \Lambda$ and $\gamma \in \Gamma$. If $m = \sum_{\lambda\in\Lambda} a_\lambda \lambda$, as in the statement of the theorem, then $f(m) = m$ translates into

$$\sum_{\lambda\in\Lambda} c_\lambda a_\lambda = 1\,.$$

Since every Γ-orbit in Λ has a power of p elements, reducing modulo p, we obtain

$$\sum_{\lambda\in\Lambda^\Gamma} c_\lambda a_\lambda = 1 \pmod p\,.$$

This shows that $a_\lambda \ne 0$ modulo p, for some $\lambda \in \Lambda^\Gamma$, as claimed.

(c) Decompose $X(T)_{(p)}$ uniquely into a direct sum of indecomposable $\mathbb{Z}_{(p)}\Gamma$-lattices by the Krull-Schmidt theorem [**CR**, Theorem 36.1]. Since $\mathrm{ed}(T;p) = 1$, and the essential p-dimension of tori is additive (Thm. 8.1), all but one of these summands are permutation $\mathbb{Z}_{(p)}\Gamma$-lattices. Now by [**CR**, 31.12], we can lift this decomposition to $X(T) \cong X(T') \oplus X(S)$, where $\mathrm{ed}(T';p) = 1$ and $\mathrm{ed}(S;p) = 0$. □

EXAMPLE 11.6. Let E be an étale algebra over k. It can be written as $E = L_1 \times \cdots \times L_m$ with some separable field extensions L_i/k. The kernel of the norm $\mathrm{R}_{E/k}(\mathbb{G}_{\mathbf{m}}) \to \mathbb{G}_{\mathbf{m}}$ is denoted by $\mathrm{R}^{(1)}_{E/k}(\mathbb{G}_{\mathbf{m}})$. It is a torus with lattice

$$\bigoplus_{i=1}^{m} \mathbb{Z}[\Gamma/\Gamma_{L_i}] \,/\, \langle 1, \cdots, 1\rangle,$$

where $\Gamma = \mathrm{Gal}(k_{\mathrm{sep}}/k)$ and $\Gamma_{L_i} = \mathrm{Gal}(k_{\mathrm{sep}}/L_i)$. Let Λ be the disjoint union of the cosets Γ/Γ_{L_i} Passing to a p-closure $k^{(p)}$ of k, $\Gamma_{k^{(p)}}$ fixes a λ in Λ iff $[L_i : k]$ is prime to p for some i. We thus have

$$\mathrm{ed}_k(\mathrm{R}^{(1)}_{E/k}(\mathbb{G}_{\mathbf{m}}); p) = \begin{cases} 1, & [L_i : k] \text{ is divisible by } p \text{ for all } i = 1, ..., m \\ 0, & [L_i : k] \text{ is prime to } p \text{ for some } i. \end{cases}$$

12. Tori split by cyclic extensions of degree dividing p^2

In this section we assume $k = k^{(p)}$ is p-closed. Over $k = k^{(p)}$ every torus is split by a Galois extension of p-power order. We wish to compute the essential dimension of all tori split by a Galois extension with a (small) fixed Galois group G. The following theorem tells us for which G this is feasible:

THEOREM 12.1 (A. Jones [**Jo**]). *For a p-group G there are only finitely many genera of indecomposable $\mathbb{Z}G$-lattices if and only if G is cyclic of order dividing p^2.*

REMARK 12.2. For $G = C_2 \times C_2$ a classification of the (infinitely many) different genera of $\mathbb{Z}G$-lattices has been worked out by [**NA**]. In contrast for $G = C_{p^3}$ or $G = C_p \times C_p$ and p odd (in the latter case) no classification is known.

Hence in this section we consider tori T whose minimal splitting field is cyclic of degree dividing p^2. Its character lattice $X(T)$ is then a $\mathbb{Z}G$-lattice where $G = \langle g | g^{p^2} = 1\rangle$ denotes the cylic group of order p^2. Heller and Reiner [**HR**], (see also [**CR**, 34.32]) classified all indecomposable $\mathbb{Z}G$-lattices. Our goal consists in computing the essential dimension of T. By Corollary 10.2 we have $\mathrm{ed}_k(T) = \mathrm{ed}_k(T; p)$, hence by the additivity Theorem 8.1 it will be enough to find the essential p-dimension of the tori corresponding to indecomposable $\mathbb{Z}G$-lattices. Recall that two lattices are in the same genus if their p-localization (or equivalently p-adic completion) are isomorphic. By Proposition 10.1 tori with character lattices in the same genus have the same essential p-dimension, which reduces the task to calculating the essential p-dimension of tori corresponding to the $4p + 1$ cases in the list [**CR**, 34.32].

Denote by $H = \langle h | h^p = 1\rangle$ the group of order p. We can consider $\mathbb{Z}H$ as a G-lattice with the action $g \cdot h^i = h^{i+1}$. Let

$$\delta_G = 1 + g + \ldots + g^{p^2-1} \quad \delta_H = 1 + h + \ldots + h^{p-1}$$

be the "diagonals" in $\mathbb{Z}G$ and $\mathbb{Z}H$ and

$$\epsilon = 1 + g^p + \ldots + g^{p^2-p}.$$

The following $\mathbb{Z}G$-lattices represent all genera of indecomposable $\mathbb{Z}G$-lattices (by $\langle * \rangle$ we mean the $\mathbb{Z}G$-sublattice generated by $*$):

$$\begin{array}{lcll}
M_1 & = & \mathbb{Z} & \\
M_2 & = & \mathbb{Z}H & \\
M_3 & = & \mathbb{Z}H/\langle \delta_H \rangle & \\
M_4 & = & \mathbb{Z}G & \\
M_5 & = & \mathbb{Z}G/\langle \delta_G \rangle & \\
M_6 & = & \mathbb{Z}G \oplus \mathbb{Z}/\langle \delta_G - p \rangle & \\
M_7 & = & \mathbb{Z}G/\langle \epsilon \rangle & \\
M_8 & = & \mathbb{Z}G/\langle \epsilon - g\epsilon \rangle & \\
M_{9,r} & = & \mathbb{Z}G \oplus \mathbb{Z}H/\langle \epsilon - (1-h)^r \rangle & 1 \le r \le p-1 \\
M_{10,r} & = & \mathbb{Z}G \oplus \mathbb{Z}H/\langle \epsilon(1-g) - (1-h)^{r+1} \rangle & 1 \le r \le p-2 \\
M_{11,r} & = & \mathbb{Z}G \oplus \mathbb{Z}H/\langle \epsilon - (1-h)^r, \delta_H \rangle & 1 \le r \le p-2 \\
M_{12,r} & = & \mathbb{Z}G \oplus \mathbb{Z}H/\langle \epsilon(1-g) - (1-h)^{r+1}, \delta_H \rangle & 1 \le r \le p-2
\end{array}$$

In the sequel we will refer to the above list as ($\mathbb{L}$).

In ($\mathbb{L}$) we describe $\mathbb{Z}G$-lattices as quotients of permutation lattices of minimal possible rank, whereas [**CR**, 34.32] describes these lattices as certain extensions $1 \to L \to M \to N \to 1$ of $\mathbb{Z}[\zeta_{p^2}]$-lattices by $\mathbb{Z}H$-lattices. Therefore these two lists look differently. Nevertheless they represent the same $\mathbb{Z}G$-lattices. We show in the example of the lattice $M_{10,r}$ how one can translate from one list to the other.

Let $\mathbb{Z}x$ be a $\mathbb{Z}G$-module of rank 1 with trivial G-action. We have an isomorphism

$$M_{10,r} = \mathbb{Z}G \oplus \mathbb{Z}H/\langle \epsilon(1-g) - (1-h)^{r+1} \rangle \simeq \mathbb{Z}G \oplus \mathbb{Z}H \oplus \mathbb{Z}x/\langle \epsilon - (1-h)^r - x \rangle$$

induced by the inclusion $\mathbb{Z}G \oplus \mathbb{Z}H \hookrightarrow \mathbb{Z}G \oplus \mathbb{Z}H \oplus \mathbb{Z}x$.

This allows us to write $M_{10,r}$ as the pushout

$$\begin{array}{ccc}
\mathbb{Z}H & \xrightarrow{h \mapsto \epsilon} & \mathbb{Z}G \\
{\scriptstyle h \mapsto (1-h)^r + x}\downarrow & & \downarrow \\
\mathbb{Z}H \oplus \mathbb{Z}x & \longrightarrow & M_{10,r}
\end{array}$$

Completing both lines on the right we see that $M_{10,r}$ is an extension

$$0 \to \mathbb{Z}H \oplus \mathbb{Z}x \to M_{10,r} \to \mathbb{Z}G/\mathbb{Z}H \to 0$$

with extension class determined by the vertical map $h \mapsto (1-h)^r + x$ cf. [**CR**, 8.12] and we identify (the p-adic completion of) $M_{10,r}$ with one of the indecomposable lattices in the list [**CR**, 34.32].

Similarly, $M_1, \ldots, M_{12,r}$ are representatives of the genera of indecomposable $\mathbb{Z}G$-lattices.

THEOREM 12.3. *Every indecomposable torus T over k split by G has character lattice isomorphic to one of the $\mathbb{Z}G$-lattices M in the list* ($\mathbb{L}$) *after p-localization and* $\operatorname{ed}(T) =$

$\operatorname{ed}(T;p) = \operatorname{ed}(\operatorname{Diag}(M);p)$. *Their essential dimensions are given in the tables below.*

M	$\operatorname{rank} M$	$\operatorname{ed}(T)$
M_1	1	0
M_2	p	0
M_3	$p-1$	1
M_4	p^2	0
M_5	p^2-1	1
M_6	p^2	1

M	$\operatorname{rank} M$	$\operatorname{ed}(T)$
M_7	p^2-p	p
M_8	p^2-p+1	$p-1$
$M_{9,r}$	p^2	p
$M_{10,r}$	p^2+1	$p-1$
$M_{11,r}$	p^2-1	$p+1$
$M_{12,r}$	p^2	p

Proof of Proposition 12.3. We will assume $p > 2$ in the sequel. For $p = 2$ the Theoerem is still true but some easy additional arguments are needed which we leave out here.

The essential p-dimension of tori corresponding to $M_1 \dots, M_6$ easily follows from the discussion in section 11. Let M be one of the lattices $M_7, \dots, M_{12,r}$ and $T = \operatorname{Diag} M$ the corresponding torus. We will determine the minimal rank of a permutation $\mathbb{Z}G$-lattice P admitting a homomorphism $P \to M$ which becomes surjective after localization at p. Then we conclude $\operatorname{ed}(T;p) = \operatorname{rank} P - \operatorname{rank} M$ with Corollary 9.2.

We have the bounds

$$\operatorname{rank} M \le \operatorname{rank} P \le p^2 \text{ (or } p^2+p), \tag{23}$$

where the upper bound holds since every M is given as a quotient of $\mathbb{Z}G$ (or $\mathbb{Z}G \oplus \mathbb{Z}H$). Let $C = \operatorname{Split}_k(T[p])$ the finite constant group used in the proof of Theorem 1.3. The rank of C determines exactly the number of direct summands into which P decomposes. Moreover each indecomposable summand has rank a power of p.

As an example, we show how to find C for $M = M_{11,r}$: The relations $g^j \cdot (\epsilon - (1-h)^r); \delta_H$ are written out as

$$\sum_{i=0}^{p-1} g^{pi+j} - \sum_{\ell=0}^{r} \binom{r}{\ell} (-1)^\ell h^{\ell+j},\ 0 \le j \le p-1; \quad \sum_{i=0}^{p-1} h^i$$

and the k_{sep}-point of the torus are

$$T(k_{\mathrm{sep}}) = \Big\{ (t_0, \dots, t_{p^2-1}, s_0, \dots, s_{p-1}) \mid \prod_{i=0}^{p-1} t_{pi+j} = \prod_{\ell=0}^{r} s_{\ell+j}^{(-1)^\ell \binom{r}{\ell}},\ 0 \le j \le p-1; \quad \prod_{i=0}^{p-1} s_i = 1 \Big\}$$

and C is the constant group of fixed points of the p-torsion $T[p]$:

$$C(k) = \left\{ \left(\zeta_p^i, \dots, \zeta_p^i, \zeta_p^j, \dots, \zeta_p^j\right) \mid\ 0 \le i, j \le p-1 \right\} \simeq \mu_p^2.$$

(Note that the primitive pth root of unity ζ_p is in k by our assumption that k is p-closed). For other lattices this is similar: C is equal to $\operatorname{Split}_k(\operatorname{Diag}(P)[p]) \simeq \mu_p^r$ where M is presented as a quotient P/N of a permutation lattice P (of minimal rank) as in ($\mathbb{L}$)

and where r denotes the number of summands in a decomposition of P.

M	rank C	rank M	possible rank P
M_7	1	p^2-p	p^2
M_8	1	p^2-p+1	p^2
$M_{9,r}$	2	p^2	p^2+1 or p^2+p
$M_{10,r}$	2	p^2+1	p^2+1 or p^2+p
$M_{11,r}$	2	p^2-1	p^2+1 or p^2+p
$M_{12,r}$	2	p^2	p^2+1 or p^2+p

We need to exclude the possibility $\operatorname{rank} P = p^2+1$ for the lattices $M = M_{9,r}, \dots, M_{12,r}$. We can only have the value p^2+1 if there exists a character in M which is fixed under the Galois group and nontrivial on C. The following Lemma 12.4 tells us, that such characters do not exist in either case. Hence the minimal dimension of a p-faithful representation of all these tori is p^2+p. □

LEMMA 12.4. *For $i = 9, \dots, 12$ and $r \geq 1$ every character $\chi \in M_{i,r}$ fixed under G has trivial restriction to C.*

PROOF. By [**Hi**] the cohomology group $H^0(G, M_{i,r}) = M_{i,r}^G$ of G-fixed points in $M_{i,r}$ is trivial for $i = 11$, has rank 1 for $i = 9, 12$ and rank 2 for $i = 10$, respectively. They are represented by $\mathbb{Z}\delta_H$ in $M_{9,r}$, by $\mathbb{Z}(\epsilon - (1-h)^r)$ in $M_{12,r}$ and by $\mathbb{Z}(\epsilon - (1-h)^r) \oplus \mathbb{Z}\delta_H$ in $M_{10,r}$, respectively. Since all these characters are trivial on

$$C = \operatorname{Split}_k(\operatorname{Diag}(\mathbb{Z}G \oplus \mathbb{Z}H)[p]),$$

the claim follows. □

Acknowledgments

The authors are grateful to A. Auel, A. Merkurjev and A. Vistoli for helpful comments and conversations.

Bibliography

[AP] H. Abold, W. Plesken, *Ein Sylowsatz für endliche p-Untergruppen von* GL(n, Z), Math. Ann. 232 (1978), no. 2, 183–186.

[Ba] G. Bayarmagnai, *Essential dimension of some twists of* μ_{p^n}, Proceedings of the Symposium on Algebraic Number Theory and Related Topics, 145–151, RIMS Kôkyûroku Bessatsu, B4, Res. Inst. Math. Sci. (RIMS), Kyoto (2007).

[BF] G. Berhuy, G. Favi, *Essential Dimension: A Functorial Point of View (after A. Merkurjev)*, Doc. Math. 8:279–330 (electronic) (2003).

[Bo] A. Borel *Linear Algebraic Groups*, Benjamin (1969).

[BS_1] A. Borel, J.-P. Serre, *Théorèmes de finitude en cohomologie galoisienne*, Comment. Math. Helv. **39** (1964), 111–164.

[BS_2] A. Borel, J.-P. Serre, Sur certains sous-groupes des groupes de Lie compacts. (French) Comment. Math. Helv. 27, (1953). 128–139.

[Bou] N. Bourbaki, *Algebra. II. Chapters 4–7.* Translated from the French by P. M. Cohn and J. Howie. Elements of Mathematics. Springer-Verlag, Berlin, (1990).

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

[CGR] V. Chernousov, Ph. Gille, Z. Reichstein, *Resolving G-torsors by abelian base extensions*, J. Algebra **296** (2006), no. 2, 561–581.

[CTS] J.-L. Colliot-Thélène, J. J. Sansuc, *Principal Homogeneous Spaces under Flasque Tori: Applications*, J. Algebra **106** (1087), 148–205.

[CR] C. W. Curtis, I. Reiner, *Methods of representation theory* ,vol. 1, Wiley (Interscience), 1981.

[DG] M. Demazure, P. Gabriel, *Groupes algébriques. Tome I*, Masson & Cie, Paris; North-Holland Publishing Co., Amsterdam, 1970.

[Fl] M. Florence, *On the essential dimension of cyclic p-groups*, Inventiones Mathematicae, **171** (2007), 175-189.

[GMS] S. R. Garibaldi, A. Merkurjev, J.-P. Serre: *Cohomological Invariants in Galois Cohomology*, University Lecture Series, Vol. 28, American Mathematical Society, Providence, RI, (2003).

[GR] Ph. Gille, Z. Reichstein, *A lower bound on the essential dimension of a connected linear group*, Comment. Math. Helv. **4**, no. 1 (2009), 189–212.

[Gro] A. Grothendieck, *La torsion homologique et les sections rationnelles*, Exposé 5, Séminaire C. Chevalley, Anneaux de Chow et applications, IHP, (1958).

[HR] A. Heller, I. Reiner: *Representations of cyclic groups in rings of integers I*, Annals of Math, **76** (1962), 73-92.

[Hi] H. Hiller, *Flat Manifolds with* $\mathbb{Z}/p^2$ *Holonomy*, L'Enseignement Mathématique, **31** (1985), 283–297.

[Ja] J. C. Jantzen, *Representations of Algebraic Groups.* Pure and Applied Mathematics, 131. Academic Press, Orlando, Florida, (1987).

[Jo] A. Jones, *Groups with a finite number of indecomposable integral representations*, Mich. Math. J, **10** (1963), 257-261.

[Ka] G. Karpilovsky, *Clifford Theory for Group Representations.* Mathematics Studies, 156. North-Holland, Netherlands, (1989).

[KM] N. Karpenko, A. Merkurjev, *Essential dimension of finite p-groups*, Inventiones Mathematicae, **172** (2008), 491–508.

[Ma] B. Margaux, *Passage to the limit in non-abelian Čech cohomology.* J. Lie Theory 17, no. 3 (2007), 591–596.

[Me$_1$] A. Merkurjev, *Essential dimension*, in Quadratic forms – algebra, arithmetic, and geometry (R. Baeza, W.K. Chan, D.W. Hoffmann, and R. Schulze-Pillot, eds.), Contemp. Math. **493** (2009), 299–326.

[Me$_2$] A. Merkurjev, *Essential dimension of PGL(p^2)*, preprint, available at `http://www.math.ucla.edu/~merkurev/publicat.htm`.

[Me$_3$] A. Merkurjev, *Essential dimension of simple algebras*, preprint, available at `http://www.math.ucla.edu/~merkurev/publicat.htm`.

[MR$_1$] A. Meyer, Z. Reichstein, *The essential dimension of the normalizer of a maximal torus in the projective linear group*, Algebra and Number Theory, **3**, no. 4 (2009), 467–487.

[MR$_2$] A. Meyer, Z. Reichstein, *An upper bound on the essential dimension of a central simple algebra*, to appear in Journal of Algebra, 10.1016/j.jalgebra.2009.09.019, preprint available at arXiv:0907.4496

[NA] L. A. Nazarova, *Unimodular representations of the four group*, Dokl. Akad. Nauk SSSR, **140** (1961), 1011–1014.

[Re] Z. Reichstein, *On the Notion of Essential Dimension for Algebraic Groups*, Transformation Groups, **5**, 3 (2000), 265-304.

[RY] Z. Reichstein, B. Youssin, *Essential Dimensions of Algebraic Groups and a Resolution Theorem for G-varieties*, with an appendix by J. Kollar and E. Szabo, Canadian Journal of Mathematics, **52**, 5 (2000), 1018–1056.

[RZ] L. Ribes, P. Zalesskii, *Profinite Groups.* Springer-Verlag, Berlin, 2000.

[Ro] M. Rost, *Essential dimension of twisted C_4*, available at `http://www.math.uni-bielefeld.de/~rost/ed.html`.

[Sch$_1$] H.-J. Schneider, *Zerlegbare Erweiterungen affiner Gruppen* J. Algebra **66**, no. 2 (1980), 569–593.

[Sch$_2$] H.-J. Schneider, *Decomposable Extensions of Affine Groups*, in Lecture Notes in Mathematics **795**, Springer Berlin/Heidelberg (1980), 98–115.

[Sch$_3$] H.-J. Schneider, *Restriktion und Corestriktion fr algebraische Gruppen* J. Algebra, **68**, no. 1 (1981), 177–189.

[Se$_1$] J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, **42**, Springer-Verlag, 1977.

[Se$_2$] J.-P. Serre, *Galois cohomology.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002.

[Sp] T. A. Springer, *Linear algebraic groups*, 2nd ed., Progress in Mathematics (Boston, MA, 1998), Birkhäuser, Boston, 1998.

[Ta] J. Tate, *Finite flat group schemes.* Modular forms and Fermat's last theorem (Boston, MA, 1995), 121–154, Springer, New York, 1997.

[Vo] V. E. Voskresenskiĭ, *Algebraic Groups and Their Birational Invariants*, American Mathematical Society, Providence, RI, 1998.

[Wa] W. C. Waterhouse, *Introduction to affine group schemes.* Springer-Verlag, New York-Berlin, 1979.

[Wi] J. S. Wilson, *Profinite Groups.* London Math. Soc. Monographs 19, Oxford University Press, New York, 1998.

[Win] D. Winter, *The structure of fields.* Graduate Texts in Mathematics, no. 16. Springer-Verlag, New York-Heidelberg, 1974.

ROLAND LÖTSCHER, INSTITUTE OF MATHEMATICS, UNIVERSITY OF BASEL, RHEINSPRUNG 21, CH-4051 BASEL, SWITZERLAND

Email adress: `roland.loetscher@unibas.ch`

MARK MACDONALD, AUREL MEYER AND ZINOVY REICHSTEIN, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, BC V6T 1Z2, CANADA

Email adresses: mlm@math.ubc.ca, aurel@math.ubc.ca, reichst@math.ubc.ca

Curriculum Vitae

Roland Oskar Lötscher, born on February 5th 1982 in Wolhusen, Luzern. I am citizen of Ruswil, Luzern. My parents are Anne and Franz Lötscher-Steiner.

Education

Aug.1989-July 1995	Primary school in Werthenstein
Aug.1995-July 1998	Kantonsschule (grammar school) in Schüpfheim
Aug.1998-Mai 2001	Gymnasium (grammar school) in Engelberg
Oct.2001-April 2006	Studies in Mathematics at the ETH Zürich
Feb.2004-June 2004	Studies of Mathematics at the State University of St. Petersburg
April 2006	Diploma in Mathematics, Diploma Thesis with title *Eine Verallgemeinerung der Komposition von quadratischen Formen* Advisor: Prof. Dr. M.-A. Knus
April-Sept. 2006	Assistant at the Department of Mathematics, ETH Zürich
Oct. 2006-April 2010	PhD at the University of Basel Advisor: Prof. Dr. H. Kraft Assistant at the Institute of Mathematics in Basel
April-May 2009	Research visit at the Department of Mathematics at the University of British Columbia, Vancouver
April 15, 2010	Doctoral Colloquium

I have visited seminars and lectures of Prof. O.E. Lanford, Prof. G. Mislin, Prof. M.-A. Knus, Prof. R. Eichler, Prof. R. Jeltsch, Prof. E. Feichtner, Prof. R. Peikert, Prof. F. Delbaen, Prof. F. Hampel, Prof. G. Wüstholz, Prof. E. Trubowitz, Prof. T. Ilmanen, Prof. G.M. Graf, Prof. T. Rivière, Prof. M. Struwe, Prof. U. Stammbach, Prof. B. Makarov, Prof. N. Netsvetaev, Prof. W. Suchanov, Prof. V. Lyakhovsky, Prof. U. Lang, Prof. E. Welzl, Dr. T. Szabo, Prof. R. Pink, Prof. G. Felder, Dr. P. Turnheer, Prof. H. Kraft, Dr. G. Favi, Prof. U. Brodmann, Dr. K. Baur, Dr. A. Moreau