Finite Group Schemes of Essential Dimension One

Najmuddin Fakhruddin

Abstract. We prove that if a finite group scheme G over a field k has essential dimension one, then it embeds in $PGL_{2/k}$. We use this to give an explicit classification of all infinitesimal group schemes of essential dimension one over any field and a characterisation of all finite group schemes of essential dimension one over algebraically closed fields.

1 Introduction

Let G be a group scheme over a field k. The essential dimension of G—see e.g. [8] or [7] for the definition—is a non-negative integer defined using G-torsors over all extensions of k. For example, if $G = GL_{n/k}$ then all G torsors are trivial and the essential dimension is zero. The essential dimension of a non-trivial finite group scheme G is always positive, so those having essential dimension one are of particular interest. The main aim of this note is to prove the following:

THEOREM 1.1. *Let G be a finite group scheme over a field k.*

1. *If the essential dimension of G over k is one then G can be embeded in $PGL_{2/k}$ and $\dim_k(\mathrm{Lie}(G)) \le 1$.*

2. *If G is infinitesimal then it has essential dimension one over k iff it can be embedded in $PGL_{2/k}$, $\dim_k(\mathrm{Lie}(G)) = 1$, and G lifts to $GL_{2/k}$. Such group schemes exist over k iff $\mathrm{char}(k) = p > 0$ and a complete list of such group schemes is as follows:*

(a) α_{p^n} *for all* $n > 0$;

(b) μ_{p^n} *for all* $n > 0$;

(c) *any form of* μ_{p^n}, $n > 0$, *which becomes isomorphic to* μ_{p^n} *over a quadratic extension of* k *if* $p \neq 2$.

Ledet proved in [5] that a constant finite group G has essential dimension one iff it embeds in $PGL_{2/k}$ and lifts to $GL_{2/k}$. A complete list of such G was given by Chu, Hu, Kang and Zhang [3]. It is likely that by combining these results with Theorem 1.1 one can classify all finite group schemes of essential dimension one. Theorem 4.1 gives such a classification for group schemes over perfect fields with constant etale quotients.

Tossici has conjectured [9, Conjecture 1.4] that for a finite commutative unipotent group G, $\mathrm{ed}_k(G) \geq n_V(G)$, where $n_V(G)$ is the order of nilpotence of the Verschiebung morphism of G. Theorem 1.1, and the fact that $\mathrm{ed}_k(\mathbb{Z}/p^2\mathbb{Z}) = 2$ (over a field of characteristic p), implies that $\mathrm{ed}_k(G) \geq 2$ if $n_V(G) \geq 2$. In particular, we see that the p-torsion of a supersingular elliptic curve has essential dimension two (Example 4.2).

For a constant group scheme G with essential dimension one over k it is immediate that G embeds in $PGL_{2/k}$; this is because any rationally defined action of a finite group on a smooth projective curve extends to a regular action. However, this extension property is far from being true for infinitesimal group actions and the key to our classification is a simple criterion (Proposition 2.2) for the existence of such extensions. Aside from this, we also use some basic structure theory of finite group schemes, especially in the case $\mathrm{char}(k) = 2$.

For the basic definitions in the theory of essential dimension we refer the reader to [8] or [7]; we only need the definition of essential dimension of a group scheme over a field k, denoted by $\mathrm{ed}_k(G)$ below, the p-essential dimension for a prime p, denoted by $\mathrm{ed}_k(G;p)$ and the notion of versal torsors [7, §3d]. For the particular case of infinitesimal group schemes the reader may consult [10]. Our basic reference for the theory of (finite) group schemes is [4].

2   Preliminary results

2.1   An extension criterion

Lemma 2.1. *Let* $\iota : A \to B$ *be an inclusion of noetherian integral domains with* A *normal and with the map* $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ *being surjective (or with*

image containing all height one primes). If $b \in B$ is such that $b \in A_{(0)}$ (the quotient field of A), then $b \in A$.

Proof. Since A is normal, it suffices to show that the valuation of b at any height one prime of A is non-negative, so by localisation we may assume that A is a dvr. If $b \notin A$ then $b^{-1} \in m_A$. By surjectivity of the map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$, it follows that $b^{-1} \in P$ for some prime ideal P of B. But this implies that $1 = b \cdot b^{-1} \in P$, a contradiction. □

PROPOSITION 2.2. *Let k be a field, let G be an infinitesimal group scheme over k and let Y be a normal projective curve with a generically defined action of G. If there exists X, a normal projective variety over k with a regular action of G, and a dominant rational map $f : X \dashrightarrow Y$ compatible (generically) with the G-actions, then the rational action of G extends uniquely to a regular action on Y. If k is perfect or Y is smooth, then G can be taken to be any finite group scheme.*

It is easy to see that rational actions of infinitesimal group schemes on smooth projective curves do not always extend to regular actions, so our hypothesis on the existence of the equivariant rational map $f : X \dashrightarrow Y$ is not superfluous; see Example 2.4 below.

Proof. Assume first that k is arbitrary and G is infinitesimal. Let U be the maximal open subset of X on which the rational map f restricts to a morphism $f|_U : U \to Y$. The map $f|_U$ is surjective, because by normality $X \backslash U$ is of codimension at least two in X so a general complete intersection curve $C \subset X$ will lie in U and $f|_C : C \to Y$ is surjective since C is proper and also general. Let $y \in Y$ be any closed point and let $u \in U$ be a (closed) point such that $f(u) = y$. Let $V = \mathrm{Spec}(A)$ be any open affine subset of Y with $y \in V$ and such that the G-action on Y is defined at all points of $V \backslash \{y\}$. Let $W \subset U$ be any affine open subset such that $u \in W$ and $f(W) \subset V$. Since G is infinitesimal, W is G-invariant and G acts generically on V. Let $W = \mathrm{Spec}(B)$, so f induces an inclusion $\iota : A \to B$.
Let $G = \mathrm{Spec}(R)$. Then R is a Hopf algebra and the G-actions correspond to maps $c_1 : B \to R \otimes_k B$ and $c_2 : A_{(0)} \to R \otimes A_{(0)}$ (satisfying the usual properties). For any $a \in A$, we have that $c_1(\iota(a)) = c_2(a)$, where the equality holds in $R \otimes B_{(0)}$. Choosing a basis of R over k and then applying Lemma 2.1 coordinatewise, we see that $c_2(a) \in R \otimes A$. This proves that the action of G on $V \backslash \{y\}$ extends to all of V—the necessary identities hold because the map $A \to A_{(0)}$ is an injection—and this extension is clearly unique. Since $y \in Y$ was arbitrary, it follows that the generically defined action of G extends uniquely to all of Y.
Now suppose that k is perfect and G is any finite group scheme over k. By [4, II, §5, 2.4], G is a semidirect product of its identity component G^0 and its etale quotient G^{et}. The action of G^0 extends to all of Y and the generic action of an etale group scheme (over any field) on a normal projective curve

extends uniquely to a regular action. This is clear for a constant group scheme and the case of an etale group scheme follows from this by Galois descent. The uniqueness of the two extensions then implies that the action of G also extends. Now suppose that k is arbitrary, G is any finite group scheme, and Y is smooth. We know that an extension of the G^0 action exists over k and an extension of the G action exists after we base change to any perfect field K/k, since Y_K is also smooth. For $V = \mathrm{Spec}(A)$ any nonempty affine open subset of Y as above, consider the action map $c_2 : A_{(0)} \to R \otimes A_{(0)}$ as above. Using a basis of R over k and writing $c_2(a)$ in terms of coordinates, we see that an extension of the G action actually exists over k since any element of $A_{(0)}$ which lies in $A \otimes_k K$ must also lie in A. The extension is unique since this holds over K. $\quad\square$

REMARK 2.3. The assumption that Y is a curve was only used in the proof to deduce the surjectivity of $f|_U$. If instead of f being a rational map, we assume that it is regular and surjective (in codimension one), then the proof in the case of infinitesimal G works for any normal Y (without any projectivity/properness hypothesis on Y or X).

EXAMPLE 2.4. Let Z be a smooth projective ordinary curve of genus $g \geq 2$ over an algebraically closed field k of charactersitic $p > 0$. Let T be a non-trivial μ_p-torsor over Z corresponding to non-zero element of $\mathrm{Pic}(Z)[p]$. Such a torsor is non-trivial over the generic point of Z, so T must be integral at its generic point. However, there is no μ_p-equivariant completion of this torsor with total space a smooth projective curve since such a curve would map to Z, so would have genus at least 2, and a smooth projective curve of genus $g \geq 2$ has no non-zero vector fields.

We do not know the answer to the following:

QUESTION 2.5. Does the action of a finite group scheme on a function field of transcendence degree one always extend to a proper model of the function field?

LEMMA 2.6. *Let k be any field and G an affine group scheme of finite type over k. Then there exists a smooth projective (geometrically irreducible) rational variety X over k with a generically free action of G.*

Proof. Since G is of finite type it can be embedded in GL_n for some $n > 0$, so G acts linearly and generically freely on M_n, the space of $n \times n$ matrices. We may then take X to be the projective completion of M_n, i.e., $\mathbb{P}(M_n \oplus k)$. $\quad\square$

2.2 INFINITESIMAL GROUP SCHEMES WITH ONE DIMENSIONAL LIE ALGEBRA

In this section we assume that $\mathrm{char}(k) = p > 0$. We denote the Lie algebra of group schemes G, H, ..., by $\mathfrak{g}$, $\mathfrak{h}$, ...

LEMMA 2.7. *Let G be an infinitesimal group scheme over a field k with $\dim_k(\mathfrak{g}) = 1$. If H is any subquotient of G, then $\dim_k(\mathfrak{h}) \leq 1$.*

Proof. The statement is clear for subgroup schemes so it suffices to prove it for quotients. Let $K \subset G$ be a normal subgroup scheme and let $H = G/K$. Clearly $\mathcal{O}(G) \cong B = k[x]/(x^{p^n})$ for some $n \geq 0$, and $\mathcal{O}(H) \cong A$, where A is a k-subalgebra of B such that B is flat over A. If $A = k$ the lemma is clear, so we may assume that the maximal ideal m_A of A is nonzero.

Let r be the smallest integer such that m_A contains an element $a \in m_B^r \setminus m_B^{r+1}$. Then the elements $1, x, \ldots, x^{r-1}$ of B are linearly independent in $B/m_A B$, so they must be part of a basis of B over A. In particular, we get that $p^n = \dim_k(B) \leq r \dim_k(A)$. On the other hand, the structure of the ring B implies that $1, a, \ldots, a^{\lceil \frac{p^n}{r} \rceil}$ are k-independent elements of A. This implies that $r | p^n$ and a generates m_A, so $\mathfrak{h}$ is one dimensional. $\qquad\square$

REMARK 2.8. The lemma holds with 1 replaced by n for arbitrary finite type group schemes G over a field k, but we do not give the details here since we do not need this.

PROPOSITION 2.9. *Let G be an infinitesimal group scheme over a field k with $\dim_k(\mathfrak{g}) = 1$. Then either G is multiplicative or it is unipotent.*

Proof. Since Lie algebras are compatible with field extensions and so are the notions of multiplicative and unipotent groups, we may assume that k is algebraically closed.

Let G_1 be the height one subgroup scheme of G corresponding to $\mathfrak{g}$ (viewed as p-Lie algebra); see for example [4, II, §7, 4.3]. This is a characteristic subgroup scheme of G of order p, so we may form the quotient G/G_1. By Lemma 2.7 and induction on the order of G, we get a filtration

$$\{1\} = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_n = G$$

where each G_i is a characteristic subgroup of G and G_i/G_{i-1} is of order p for $1 \leq i \leq n$, so isomorphic to α_p or μ_p. To prove the lemma it suffices by [4, IV, §1, 4.5] to show that all these quotients are of the same type.

If G is neither unipotent nor multiplicative, it follows from the above that G has a subquotient of order p^2 which is an extension of μ_p by α_p or an extension of α_p by μ_p.

In the first case, [4, IV, §2, 3.3] implies that the extension is a trigonalisable group scheme. Then by [4, IV, §2, 3.5] the extension splits, i.e., it is a semidirect product. In the second case, since k is algebraically closed, so perfect, it follows from [1, Théorème 6.1.1 (B)] that the extension is trivial.

Lemma 2.7 leads to a contradiction in both cases, so the proposition is proved. $\qquad\square$

REMARK 2.10. Multiplicative group schemes G with $\dim_k(\mathfrak{g}) = 1$ are just forms of μ_{p^n} for some $n > 0$. Can one classify all unipotent group schemes with one dimensional Lie algebras? (It seems likely that they are all commutative.)

3 Proof of the main theorem

Proof of Theorem 1.1. For any non-trivial finite group scheme G, $\mathrm{ed}_k(G) \geq 1$ since there exist G-torsors over any extension of k whose underlying scheme is integral.

Now suppose G is an arbitrary finite group scheme with $\mathrm{ed}_k(G) = 1$. By Lemma 2.6, there exists a smooth projective rational variety X with a generically free action of G. Let $\emptyset \neq U \subset X$ be an open subset on which G acts freely and let $V = X/G$, so U is the total space of a G-torsor over V. The induced torsor over $\mathrm{Spec}(k(V))$ does not have essential dimension 0, since any G-torsor over $\mathrm{Spec}(k)$ becomes trivial over an algebraic closure $\bar{k}$ of k but the torsor over $\mathrm{Spec}(\bar{k}(V_{\bar{k}}))$ is non-trivial. Thus, since $\mathrm{ed}_k(G) = 1$, there is a normal integral curve Z over k, a G-torsor T over Z, and a dominant rational map $V \dashrightarrow Z$ such that X is generically equal to $V \times_Z T$ (which makes sense over the generic point of V) as a G-torsor.

Since X is integral, the fibre of T over the generic point of Z must also be integral. Let Y be the unique normal projective curve with function field equal to $k(T)$ (the residue field at the generic point of T), so Y has a generically defined, generically free, action of G and we have a G-equivariant dominant rational map from X to Y. Since X is rational, Luroth's theorem implies that $Y \cong \mathbb{P}^1_k$; in particular, Y is smooth. By Proposition 2.2, the generic G-action extends to a regular action of G on Y. The generic freeness of the G-action on Y then gives an embedding $G \hookrightarrow \mathrm{Aut}(Y) \cong PGL_{2/k}$. Finally, since the G-action on Y is generically free and Y is a smooth curve, it follows that $\dim_k(\mathfrak{g}) \leq 1$.

Now let $G \subset PGL_{2/k}$ be an infinitesimal subgroup scheme with $\dim_k(\mathfrak{g}) = 1$. If G lifts to a subgroup scheme of $GL_{2/k}$, then G acts generically freely on $\mathbb{A}^2_k$ and the map $\mathbb{A}^2_k \to \mathbb{A}^2_k/G$ gives rise to a versal G-torsor over a non-empty open subset of $\mathbb{A}^2_k/G$. We also have a G-torsor corresponding to the quotient map $\mathbb{P}^1_k \to \mathbb{P}^1_k/G$, and this torsor gives a one dimensional compression of the versal G-torsor. Thus $\mathrm{ed}_k(G) \leq 1$ and if G is non-trivial then we must have $\mathrm{ed}_k(G) = 1$.

To prove that G lifts to $GL_{2/k}$ if $\mathrm{ed}_k(G) = 1$, we first consider the case that $\mathrm{char}(k) \neq 2$. Then we have an etale isogeny $SL_{2/k} \to PGL_{2/k}$, so if G is infinitesimal it lifts (uniquely) to $SL_{2/k}$, therefore to $GL_{2/k}$.

Suppose that G is multiplicative (with $\mathrm{char}(k)$ arbitrary) and let $C(G)$ be the centralizer of G in $PGL_{2/k}$. By [1, XI, Corollaire 2.4], the centralizer of a group scheme of multiplicative type in any smooth affine group scheme is smooth, so $C(G)$ is smooth; let $C^0(G)$ be its identity component. Now $C(G)$ is a proper subgroup scheme of $PGL_{2/k}$ since the centre of $PGL_{2/k}$ is trivial. Also, G is contained in the centre of $C^0(G)$, which must therefore be positive dimensional. If $C^0(G)$ is not a torus then it must contain a smooth one dimensional unipotent subgroup U. However, since $G \subset G^0(G)$ and G is multiplicative, it follows that in this case $C^0(G)$ must be two dimensional. Therefore, $C^0(G)$ must be a Borel subgroup of $PGL_{2/k}$ and U must be its unipotent radical. However, the centre of a Borel subgroup of $PGL_{2/k}$ is trivial, so this contradicts the fact that

G is contained in the centre of $C^0(G)$. Thus, any infinitesimal multiplicative subgroup G of $PGL_{2/k}$ in any characteristic must be contained in a torus T.

Let T' be the inverse image of T in $GL_{2/k}$, so T' is a two dimensional torus. It is a maximal torus, of which the non-split ones are classified by separable quadratic extensions of k: the action of the Galois group on the character group $\cong \mathbb{Z}^2$ is given by switching coordinates. It follows that T' is a quadratic twist of $\mathbb{G}_m$. If $\mathrm{char}(k) > 2$ this gives the claimed classification of all multiplicative G with $\mathrm{ed}_k(G) = 1$.

If T is non-split then the above description shows that it contains a unique subgroup scheme of order 2. If $\mathrm{char}(k) = 2$, it follows from this that $G \subset T'$ lifts to a subgroup of $GL_{2/k}$ iff T (equivalently T') is split; in particular, G must be isomorphic to μ_{2^n} for some n.

By [6, Proposition 6.1], if G is a non-trivial quadratic twist of μ_{2^n} then $\mathrm{ed}_k(G; 2) = 2$. Since $\mathrm{ed}_k(G) \geq \mathrm{ed}_k(G; p)$ for any prime p, we conclude that if $\mathrm{char}(k) = 2$ the only infinitesimal multiplicative group schemes G with $\mathrm{ed}_k(G) = 1$ are the μ_{2^n} for $n > 0$.

Now suppose $G \neq \{1\}$ is unipotent and assume that the G-action on $\mathbb{P}^1_k$ gives a versal G-torsor.

CLAIM. G preserves a point in $\mathbb{P}^1_k(k)$.

Proof of claim. Consider a faithful representation of G on a finite dimensional k-vector space V. Since G is unipotent, by [4, IV, §2, 2.5] V has a complete filtration by k-subspaces

$$0 = V_0 \subset V_1 \subset \ldots \subset V_{n-1} \subset V_n = V$$

which is preserved by G. By induction on n, we may assume that the action on V_{n-1} is not faithful.

Since $\mathrm{Lie}(G)$ is one dimensional, the action of G on V (which we now think of as an affine variety) is generically free. By the assumed versality of the G-action on $\mathbb{P}^1_k$, there exists a rational G-equivariant morphism $f : V \dashrightarrow \mathbb{P}^1_k$. Since $\mathbb{P}^1_k$ is proper, f is defined at the generic point of V_{n-1}. The restriction of f to V_{n-1} cannot be dominant since the action of G on V_{n-1} is not faithful, so $f(V_{n-1})$ must be a rational point $x \in \mathbb{P}^1_k(k)$. Since V_{n-1} is G-invariant, it follows that so is x, and the claim is proved. □

The stabilizer in $PGL_{2/k}$ of any point in $\mathbb{P}^1_k(k)$ is Borel subgroup so G is contained in a Borel B. Since G is unipotent, it is in fact contained in the unipotent radical of B which lifts to $GL_{2/k}$. Thus, G also lifts to $GL_{2/k}$. [1]

Any unipotent subgroup of $GL_{2/k}$ in any characteristic preserves a line, so we see that any infinitesimal unipotent group G with $\mathrm{ed}_k(G) = 1$ must be isomorphic to a subgroup of $\mathbb{G}_a$, so must be α_{p^n} for some $n > 0$. □

---

[1] When $p = 2$ there do exist infinitesimal unipotent subgroups of $PGL_{2/k}$ which do not lift to $GL_{2/k}$; this was pointed out to us by D. Tossici.

REMARK 3.1. If $\text{char}(k) = 2$ and μ_2 is embedded in $PGL_{2/k}$ as a subgroup of a torus (which is uniquely determined as the connected centralizer), then the μ_2 action on $\mathbb{P}^1_k$ has a fixed point iff the torus is split. It follows that the embedding gives a versal μ_2-torsor iff the torus is split.

4   APPLICATIONS OF THE MAIN THEOREM

4.1   FINITE GROUP SCHEMES OF ESSENTIAL DIMENSION ONE

Let G be any finite group scheme over k with $\text{ed}_k(G) = 1$. By Theorem 1.1, G embeds in $PGL_{2/k}$ and we also have $\dim_k(\mathfrak{g}) = 1$. If G is any finite subgroup scheme of $PGL_{2/k}$ with $\dim_k(\mathfrak{g}) = 1$, then a sufficient condition for $\text{ed}_k(G) = 1$ is that G lifts to $GL_{2/k}$. If this condition were also necessary—we know this is the case for constant as well as infinitesimal group schemes—then we would have a complete classification of all finite group schemes G with $\text{ed}_k(G) = 1$.

As a first step, one should verify this for etale group schemes. This can presumably be done using the classification of constant groups G with $\text{ed}_k(G) = 1$ in [3], but we do not do this here and proceed after making some simplifying assumptions.

Recall that for any finite group scheme G we have an exact sequence

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

where G^0 is infinitesimal and G^{et} is etale. This sequence splits when k is perfect, i.e., $G \cong G^0 \rtimes G^{et}$ [4, II, §5, 2.4].

THEOREM 4.1. *A finite group scheme over a perfect field k with G^{et} constant has $\text{ed}_k(G) \leq 1$ iff G can be embedded in $PGL_{2/k}$, $\dim_k(\mathfrak{g}) \leq 1$ and G lifts to $GL_{2/k}$.*

Note that if k is algebraically closed this gives a classification of all finite group schemes over k with $\text{ed}_k(G) = 1$. For general perfect k the method of proof, together with the classification results of [3], can be used to make a more explicit list of all such group schemes.

Proof. The conditions are clearly sufficient and we have already seen that the first two are necessary, so we need to show that if $\text{ed}_k(G) = 1$ then G has an embedding in $PGL_{2/k}$ which lifts to $GL_{2/k}$. We may assume that G^0 is non-trivial since otherwise the theorem is a consequence of [5].

If $\text{ed}_k(G) = 1$ then there is an embedding $G \hookrightarrow PGL_{2/k}$ which makes the quotient map $\mathbb{P}^1_k \to \mathbb{P}^1_k/G$ generically into a versal G-torsor. This implies (as is well known) that $\text{ed}_k(G^0) = 1$ and $\text{ed}_k(G^{et})$ and the corresponding quotient maps are also versal torsors. By Theorem 1.1 and [5, Theorem 8], both G^0 and G^{et} lift to $GL_{2/k}$; call the lifts $\widetilde{G^0}$ and $\widetilde{G^{et}}$.

If $\text{char}(k) \neq 2$, we saw in the proof of Theorem 1.1 that we can assume that $\widetilde{G^0} \subset SL_{2/k}$ and such a lift is unique. It follows that $\widetilde{G^{et}}$ normalizes $\widetilde{G^0}$ and the subgroup $\widetilde{G^0} \rtimes \widetilde{G^{et}} \subset GL_{2/k}$ is a lift of G.

If $\mathrm{char}(k) = 2$ and G^0 is unipotent then $\widetilde{G^0}$ is still unique, so again $\widetilde{G^0} \rtimes \widetilde{G^{et}} \subset GL_{2/k}$ is a lift of G. Finally, suppose that G^0 is multiplicative, so it is isomorphic to μ_{2^n} for some $n > 0$. We may assume that $\widetilde{G^0}$ is a subgroup of the group T' of diagonal matrices in $GL_{2/k}$ and $\widetilde{G^0} \cap Z(GL_{2/k}) = \{1\}$. If $\widetilde{G^0} \neq \{1\}$, one easily sees that the normalizer of $\widetilde{G^0}$ in $GL_{2/k}$ is T'. Thus, G has a lift to $GL_{2/k}$ iff $G \subset T$, the image of T' in $PGL_{2/k}$. If this condition is not satisfied then G contains a subgroup $G_1 \cong \mu_2 \times \mathbb{Z}/2\mathbb{Z}$. By [2, Theorem 3.1] $\mathrm{ed}_k(\mu_2 \times \mathbb{Z}/2\mathbb{Z}) = 2$—one may give an elementary proof of this particular case by using that the action of G_1 on $\mathbb{P}_k^1$ does not have any fixed points[2]— and this implies that $\mathrm{ed}_k(G) > 1$.

We conclude that if $\mathrm{ed}_k(G) = 1$ then G lifts to $GL_{2/k}$. $\qquad\square$

4.2   Some finite group schemes of essential dimension two

Using Theorem 1.1 we may compute $\mathrm{ed}_k(G)$ for various other group schemes. The point is that if one knows that $\mathrm{ed}_k(G) \leq 2$ for some group scheme G not occurring in the list of group schemes with $\mathrm{ed}_k = 1$ then we must have $\mathrm{ed}_k(G) = 2$.

EXAMPLE 4.2. Let $G = E[p]$, the p-torsion of a supersingular elliptic curve E over a field k with $\mathrm{char}(k) = p > 0$. It sits in an exact sequence

$$0 \to \alpha_p \to E[p] \to \alpha_p \to 0,$$

so by [10, Theorem 1.4] we have $\mathrm{ed}_k(E[p]) \leq 2$. However, $E[p]$ is not isomorphic to α_{p^2}, so we conclude that $\mathrm{ed}_k(E[p]) = 2$. The group scheme $E[p]$ is trigonalizable, but $2 = \mathrm{ed}_k(E[p]) > \dim_k(\mathrm{Lie}(E[p])) = 1$, so it is not *almost special* in the sense of [10, Definition 4.2]. This answers a question discussed in [10, Example 4.8].

References

[1] *Schémas en groupes. II: Groupes de type multiplicatif, et structure des schémas en groupes généraux*, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 152, Springer-Verlag, Berlin, 1962/1964.

[2] A. Babic and V. Chernousov, *Lower bounds for essential dimensions in characteristic 2 via orthogonal representations*, Pacific J. Math., 279 (2015), pp. 37–63.

[3] H. Chu, S.-J. Hu, M.-C. Kang, and J. Zhang, *Groups with essential dimension one*, Asian J. Math., 12 (2008), pp. 177–191.

---

[2] This, together with the reference in [2], was pointed out by Z. Reichstein.

[4] M. Demazure and P. Gabriel, *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*, Masson & Cie, Éditeur, Paris; North-Holland Publishing Co., Amsterdam, 1970. Avec un appendice *Corps de classes local* par Michiel Hazewinkel.

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

[6] R. Lötscher, M. MacDonald, A. Meyer, and Z. Reichstein, *Essential dimension of algebraic tori*, J. Reine Angew. Math., 677 (2013), pp. 1–13.

[7] A. S. Merkurjev, *Essential dimension: a survey*, Transform. Groups, 18 (2013), pp. 415–481.

[8] Z. Reichstein, *Essential dimension*, in Proceedings of the International Congress of Mathematicians. Volume II, Hindustan Book Agency, New Delhi, 2010, pp. 162–188.

[9] D. Tossici, *Essential dimension of inifinitesimal commutative unipotent group schemes*, Bollettino dell'Unione Matematica Italiana, 12 (2019), no. 4, pp. 575–581.

[10] D. Tossici and A. Vistoli, *On the essential dimension of infinitesimal group schemes*, Amer. J. Math., 135 (2013), pp. 103–114.

Najmuddin Fakhruddin
School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Mumbai 400005
India
naf@math.tifr.res.in