ESSENTIAL p-DIMENSION OF PGL_n

ANTHONY RUOZZI

1. Introduction

k a fixed base field of characteristic $\neq p$. All fields mentioned in this paper are assumed to contain k.

Consider any functor $\mathcal{F} : \mathbf{Fields}/k \to \mathbf{Set}$. We say that an element $a \in F(K)$ is defined over $k \subset K_0 \subset K$ if it is in the image of the map $\mathcal{F}(K_0) \to \mathcal{F}(K)$. The essential dimension, $\mathrm{ed}_k(a)$, is the least transcendence degree$/k$ of a field of definition for a. The essential dimension of F, $\mathrm{ed}_k(\mathcal{F}) = \sup\{\mathrm{ed}_k(a)\}$ where the supremum is taken over all $a \in K$ for all field extensions K/k. The basic properties of this definition are outlined in [BF].

In this paper, we will be interested in the slightly simpler computation of essential p-dimension. Here, we are allowed some extra flexibility: $\mathrm{ed}_k(a; p)$ is the minimum essential dimension of the image of a in $\mathcal{F}(L)$ over all L/K finite prime to p extensions. As above, we define $\mathrm{ed}_k(\mathcal{F}; p)$ as the supremum of the essential p-dimensions over all elements and fields, $a \in K$.

A field F/k is called p-closed if every finite extension of F has degree prime to p. For limit-preserving functors, the essential p-dimension of any element can be computed over a p-closure [LMMR Lemma 3.3], so we can always assume that our fields F are p-closed.

A natural transformation of functors $\mathcal{F} \to \mathcal{G}$ will be called p-surjective if for any K/k, there is a finite extension L/K of degree prime to p such that $\mathcal{F}(L) \twoheadrightarrow \mathcal{G}(L)$. More specifically, if F/k is p-closed and $\mathcal{F}(F) \twoheadrightarrow \mathcal{G}(F)$, then the map is p-surjective and $\mathrm{ed}_k(\mathcal{F}; p) \geq \mathrm{ed}_k(\mathcal{G}; p)$ [LMMR Prop 3.4].

Of particular interest are the functors $\mathrm{H}^1(-, G)$ for an algebraic group G/k. For ease of notation, the essential dimension of such functors will be denoted $\mathrm{ed}(G)$. We will be studying the functor $\mathrm{H}^1(F, \mathrm{PGL}_n)$ which classifies central simple algebras$/F$ of degree n. In what follows, this functor will be denoted by $\mathrm{Alg}_n(-)$. Its essential dimension gives the least number of parameters needed to define a "generic" central simple algebra of degree n.

Because we can apply prmiary decomposition to central simple algebras, the computation of $\mathrm{ed}(\mathrm{Alg}_n(-);p)$ reduces to a computation of $\mathrm{ed}(\mathrm{Alg}_{p^s}(-);p)$ where p^s is the largest power of p dividing n. It is well-known that $\mathrm{ed}(\mathrm{Alg}_p;p) = 2$; cf. [R2]. Recently, Meyer and Reichstein gave an upper bound for $s \geq 2$ [MR2 Theorem 1.1]:

$$\mathrm{ed}(\mathrm{Alg}_{p^s};p) \leq 2p^{2s-2} - p^s + 1$$

and conjectured that this bound is sharp. The goal of this paper is to further strengthen this result.

Theorem 1.1. $\mathrm{ed}(\mathrm{Alg}_{p^s}) \leq p^{2s-2} + 1$ *for* $s \geq 2$.

For $s = 2$, Merkurjev showed that this bound is sharp [M], so we can consider $s \geq 3$.

2. Essential Dimension and Tori

Throughout this section, let F/k be an arbitrary field extension. Fix a finite group G and a finite G-set, X, of n elements. Consider the augmentation exact sequence of G-modules:

$$0 \to I \to \mathbb{Z}[X] \to \mathbb{Z} \to 0.$$

Construct any resolution of I

$$0 \to M \to P \to I \to 0$$

where P is a permutation module. Fixing bases and using the usual anti-equivalence of categories, this sequence corresponds to an exact sequence of algebraic tori split over F:

$$1 \to T \to U \to S \to 1$$

where $U = \mathrm{GL}_1(E)$ is the diagonal subgroup in $\mathrm{GL}_F(E)$ for the split étale algebra E/F corresponding to P. Thus we have a faithful representation $T \hookrightarrow \mathrm{GL}_F(E)$.

Since T acts on E via this representation, G acts on E by algebra automorphisms, and the above representation is G-equivariant, this extends to a representation $T \rtimes G \to \mathrm{GL}_F(E)$. We will construct an upper bound for the essential dimension using the following important result:

Theorem 2.1. *If G acts faithfully on M in the resolution of I constructed above, then* $\mathrm{ed}(T \rtimes G) \leq \mathrm{rank}(P) - \mathrm{rank}(I) = \mathrm{rank}(M)$.

Proof. This result is a combination of [R Theorem 3.4] and [MR1 Lemma 3.3]. □

Since we a interested in essential p-dimension, the following result will also be useful:

Proposition 2.2. *Let* $H = \mathrm{Syl}_p(G)$. *Then* $\mathrm{ed}(T \rtimes G; p) = \mathrm{ed}(T \rtimes H; p)$.

Proof. This is just a special case of [MR1 Lemma 4.1]. □

3. Division Algebras

In what follows we are interested in computing the essential p-dimension, so we can assume that $F \supset k$ is p-closed. Let D/F be a central division algebra of degree $n = p^s$ with $s \geq 2$. The following results will be useful:

Proposition 3.1. *D contains degree p cyclic extension of F.*

Proof. See [RS Prop 1.1]. □

Theorem 3.2. *Let $L_1 \subset D$ be a degree p cyclic extension$/F$. Then there is another degree p cyclic exentsion L_2/F contained in D such that $L_1L_2 \subset D$ is a bicyclic extension.*

Proof. Fix a generator $< \sigma >= \mathrm{Gal}(L_1/F)$. The Skolem-Noether theorem gives an element $y \in D^\times$ such that $yxy^{-1} = \sigma(x)$ for all $x \in L_1$. There are two possibilities:

$\mathbf{y^p \in F}$: In this case, $y^p = a$ defines a cyclic algebra$/F$ $B = (L_1, a)$. By the double centralizer theorem $C_D B$ is division algebra$/F$ of degree $\geq p$. Thus, $C_D B \subset D$ has a cyclic subfield L_2. Since $L_1 \otimes L_2 \subset B \otimes C_D B \simeq D$ is a subfield, $L_1 \otimes L_2 \simeq L_1 L_2$ is bicyclic as desired.

$\mathbf{y^p \notin F}$: Let $K = F(y^p)$. By the proposition, K contains a cyclic subfield L_2. Any element of L_2 commutes with $F(y)$. Then $x \in L_1 \cap L_2$ commuting with y implies that σ acts trivially, so L_1 and L_2 are disjoint and give $L_1 L_2$ bicyclic. □

Corollary 3.3. *For A any central simple algebra$/F$ of degree $p^s \geq p^2$ and $L_1 \subset A$ an étale sub-algebra of degree p, there is a maximal étale sub-algebra $K \subset A$ that can be written as $K = L_1 \otimes_F L_2$ for L_2/F an étale algebra of dimension p^{s-1}.*

Proof. First, consider the case where A is a division algebra. By the theorem, A contains two distinct degree p cyclic extensions L_1 and L over F. Proceed by induction on s.

If $s = 2$, then taking $L_2 = L$ we are done. Otherwise, assume we have the result for any division algebra of degree p^{s-1} and any degree p subfield L'. The centralizer $C_A L$ is a division algebra over L_1 of degree p^{s-1}. By definition it contains the degree p subfield $L_1 L/L$, so by induction hypothesis, C_AL has subfield L_2/L disjoint from L_1L of degree p^{s-2}.

Since $L_2 \cap L_1L = L$ and L is disjoint from L_1, $L_2 \cap L_1 = F$. It follows that L_2/F is a degree p^{s-1} extension disjoint from L_1 and $L_1 \otimes L_2 \subset A$.

Suppose A is not a division algebra. If A is split, the result is immediate. Otherwise, choose a division algebra $D \sim A$. $\deg(D) = p^t \leq p^s = \deg(A)$. If $t = 1$, then any maximal subfield $K \subset D$ gives the desired étale algebra $K \otimes F^{\times p^{s-1}} \subset A$, so suppose $t \geq 2$. By the above argument, D has a subfield $K = L_1L_2 \simeq L_1 \otimes L_2$ where $[L_1 : F] = p$ and $[L_2 : F] = p^{t-1}$. Set $L = K^{\times p^{s-t}}$ an étale sub-algebra of B. Since L has dimension p^s, it is maximal. But $L \simeq L_1 \otimes L_2^{\times p^{s-t}}$, so L_1 and $L_2^{\times p^{s-t}}$ are étale algebras of the desired degree. □

Consider the functor $\mathrm{H}^1(F, S_n)$ which classifies n-dimensional étale algebras up to isomorphism [KMRT 29.9]. Let $G = S_p \times S_{p^{s-1}}$. We have the usual isomorphism

$$\mathrm{H}^1(F, S_p) \times \mathrm{H}^1(F, S_{p^{s-1}}) \to \mathrm{H}^1(F, G).$$

Converting this to the laguange of algebras, $\mathrm{H}^1(F, G)$ can be identified as pairs (L_1, L_2) of étale algebras of dimensions p and p^{s-1}, respectively. Under the natural inclusion

$$\mathrm{H}^1(F, G) \to \mathrm{H}^1(F, S_{p^s}),$$

the image of such a pair is the étale algebra $L_1 \otimes L_2$. Let $K = L_1 \otimes L_2 \subset A$ be given for a central simple algebra A as in the corollary. Using these identifications, any such $K \subset A$ can be viewed as an element of $\mathrm{H}^1(F, G)$.

Recall the notation of section 2. Consider the split torus T for G as above and X a G-set of p^s elements. For its cohomology group, we have a disjoint union of fibers

$$\mathrm{H}^1(F, T \rtimes G) = \coprod_{\gamma \in \mathrm{H}^1(F,G)} \mathrm{H}^1(F, T_\gamma)/G_\gamma^\Gamma$$

where T_γ denotes T with action twisted by the cocycle γ and $\Gamma = \mathrm{Gal}(F^{\mathrm{sep}}/F)$ [KMRT 28.C]. T_γ is also a torus with character module I. In particular, if X corresponds to a p^s-dimensional étale algebra N representated by γ then the usual anti-equivalence of categories gives an exact sequence

$$1 \to \mathbb{G}_m \to \mathrm{R}_{\mathrm{N/F}}(\mathbb{G}_{\mathrm{m,N}}) \to T_\gamma \to 1.$$

Passing to cohomology and applying Hilbert theorem 90 gives

$$1 \to \mathrm{H}^1(F, T_\gamma) \to \mathrm{H}^2(F, \mathbb{G}_m) \to \mathrm{H}^2(F, R_{N/F}(\mathbb{G}_m))$$

showing that $\mathrm{H}^1(F, T_\gamma) \simeq \mathrm{Br}(N/F)$. Now, G_γ^Γ acts on $\mathbf{G}_m$ trivially, so given $g \in G_\gamma^\Gamma$, we get a diagram:

$$\begin{array}{ccccc} 1 & \longrightarrow & \mathrm{H}^1(F, T_\gamma) & \longrightarrow & \mathrm{H}^2(F, \mathbb{G}_m) \\ & & \downarrow g & & \| \\ 1 & \longrightarrow & \mathrm{H}^1(F, T_\gamma) & \longrightarrow & \mathrm{H}^2(F, \mathbb{G}_m) \end{array}$$

and the commutativity implies that the action of g must be trivial for all $g \in G_\gamma^\Gamma$. Combining these observations with the above,

$$\mathrm{H}^1(F, T \rtimes G) = \coprod_N \mathrm{Br}(N/F),$$

and thus we can define a map $\phi_G(F) : \mathrm{H}^1(F, T \rtimes G) \to \mathrm{Alg}_{p^s}(F)$ which sends $[B] \in \mathrm{Br}(N/F)$ to the unique (up to isomorphism) $C \sim B$ with degree $C = p^s$. Since any $A \in \mathrm{Alg}_{p^s}$ is split over $K = L_1 \otimes L_2$, it is in the image of this map. We have proven:

Proposition 3.4. *ϕ_G is p-surjective.*

Let $G_s = \mathrm{Syl}_p(S_p \times S_{p^{s-1}}) = \mathrm{Syl}_p(S_p) \times \mathrm{Syl}_p(S_{p^{s-1}}) := \Sigma_1 \times \Sigma_{s-1}$. Using Proposition 2.2 and the property of p-surjective maps stated in the introduction,

$$\mathrm{ed}_k(T \rtimes G_s; p) = \mathrm{ed}_k(T \rtimes (S_p \times S_{p^{s-1}}); p) \geq \mathrm{ed}_k(\mathrm{Alg}_{p^s}(-); p).$$

We can therefore reduce to the computation of the essential dimension of $T \rtimes G_s$. The calculations for this case will be done in the next section.

4. Construction

We will produce an upper bound for the essential dimension of $T \rtimes G_s$. By section 2, this requires finding a faithful G_s-module, M, in a resolution of I of smallest rank. In what follows, we denote $G_s = \Sigma_{s-1} \times \mathbb{Z}/p = \Sigma_{s-1} \times < \sigma >$, where as above $\Sigma_s = \mathrm{Syl}_p(S_{p^s})$.

First observe that $G_s \subset S_{p^s}$ acts by permutation on a set X_s of p^s elements. This action can be descrbibed as an action on p blocks of p^{s-1} elements where σ cyclically permutes the blocks and Σ_{s-1} acts as usual on a block of p^{s-1} elements. In particular, the action is transitive, so if $H_s = \mathrm{Stab}(x)$ for some $x \in X_s$, then $X_s \simeq G_s/H_s$ as G_s-sets.

Begin with the case $s = 2$.

$G_2 = \Sigma_1 \times \Sigma_1 =< \tau_1 > \times < \sigma >$. No non-trivial element of G_2 fixes

$x \in X_2$, so $H_2 = 1$. Identifying $X_2 \simeq G_2$, I is generated by $\sigma - 1$ and $\tau_1 - 1$ as a G_2-module. Since G_2 is abelian, the map

$$\mathbb{Z}[G_2] \oplus \mathbb{Z}[G_2] \to I$$

defined by sending a generator of the first term to $\sigma - 1$ and a generator of the second to $\tau_1 - 1$ is a well-defined G_2-module homomorphism. It is surjective by definition. The kernel of this map, M, has rank:

$$\text{rank}(M) = 2\,\text{rank}(\mathbb{Z}[G_2]) - \text{rank}(I) = 2p^2 - (p^2 - 1) = p^2 + 1.$$

For the general case,
$\Sigma_{s-1} = (\Sigma_{s-2})^p \rtimes \mathbb{Z}/p = (\Sigma_{s-2})^p \rtimes < \tau_{s-1} >$. We will show inductively that $H_s = H_{s-1} \times (\Sigma_{s-2})^{p-1}$ and $G_s =< \sigma, \tau_{s-1}, H_s >$.

The case $s = 2$ was verified above. Suppose the formula holds for $s-1 \geq 2$. Σ_s acts on a set X_s of p^s elements, and $H_s = \text{Stab}(x)$. As above, this action can be thought of as an action on p blocks of p^{s-1} elements. On any of these blocks, $\Sigma_{s-1} \subset G_s$ acts as usual by considering it as a collection of p blocks of p^{s-2} elements. Therefore, we see that to be the stabilizer of x is to stabilize the block containing x and allow the others to be permuted freely. That is, $H_s = H_{s-1} \times (\Sigma_{s-2})^{p-1}$.

Now, $\tau_{s-2} \in< \tau_{s-1}, (\Sigma_{s-2})^{p-1} >$ and since $< \tau_{s-2}, H_{s-1} >= \Sigma_{s-2}$ by assumption, we can conclude that $G_s =< \sigma, \tau_{s-1}, H_s >$. By an easy argument, I is then generated by $\sigma x - x$ and $\tau_{s-1}x - x$; cf. [MR2 proof of Theorem 4.1]. Setting $H'_s = \tau_{s-1} H \tau_{s-1}^{-1} \cap H \simeq H_{s-1} \times H_{s-1} \times (\Sigma_{s-2})^{p-2}$, we can define a map as above

$$\mathbb{Z}[G_s/H_s] \oplus \mathbb{Z}[G_s/H'_s] \to I$$

by sending a generator of the first to $\sigma x - x$ and a generator of the second to $\tau_{s-1}x - x$. This is well-defined since H'_s is exactly the subset of G_s that fixes $\tau_{s-1}x - x$. We then have constructed a surjective G_s-module map with rank(M) =

$$\text{rank}(\mathbb{Z}[G_s/H_s]) + \text{rank}(\mathbb{Z}[G_s/H'_s]) - \text{rank}(I) = p^s + p^{s+(s-2)} - (p^s - 1) = p^{2s-2} + 1.$$

5. Conclusions

We now complete the proof of the theorem stated in the introduction. Recall that we are assuming that the base field k has characteristic $\neq p$.

Theorem 5.1. $\text{ed}(\text{Alg}_{p^s}; p) \leq p^{2s-2} + 1$ *for* $s \geq 2$.

Proof. For F p-closed, the construction in the previous section produced a G_s-module M of rank $p^{2s-2} + 1$. By section 2, it remains to show that the G-action on M is faithful (cf. [MR Lemma 3.2] for a more general argument). Faithfulness can be checked over $\mathbb{Q}$, so we have the split exact sequences:

$$0 \to I \otimes \mathbb{Q} \to \mathbb{Q}[G_s/H_s] \to \mathbb{Q} \to 0$$
$$0 \to N \to \mathbb{Q}[G_s/H_s'] \to \mathbb{Q}[G_s/H_s] \to 0$$
$$0 \to M \otimes \mathbb{Q} \to \mathbb{Q}[G_s/H_s] \oplus \mathbb{Q}[G_s/H_s'] \to I \otimes \mathbb{Q} \to 0$$

Combining these together,

$$\begin{aligned}(M \otimes \mathbb{Q}) \oplus (I \otimes \mathbb{Q}) &\simeq \mathbb{Q}[G_s/H_s] \oplus \mathbb{Q}[G_s/H_s'] \\ &\simeq \mathbb{Q}[G_s/H_s] \oplus N \oplus \mathbb{Q}[G_s/H_s] \\ &\simeq \mathbb{Q}[G_s/H_s] \oplus N \oplus \mathbb{Q} \oplus (I \otimes \mathbb{Q}).\end{aligned}$$

Therefore, $\mathbb{Q}[G_s/H_s]$ is a direct summand of $M \otimes \mathbb{Q}$, so it suffices to check that the G_s action on $\mathbb{Q}[G_s/H_s]$ is faithful. However, if the coset gH_s is fixed by every element in G_s, then $g \in \bigcap_{g_s \in G_s} g_s H_s g_s^{-1}$. A quick induction argument shows that for all $s \geq 2$ this group is trivial.

Since then the action is faithful, we have the bound:

$$p^{2s-2} + 1 \geq \mathrm{ed}(T \rtimes G_s; p) \geq \mathrm{ed}(\mathrm{Alg}_{p^s}; p). \qquad \square$$

References

[A] A. Albert, *Structure of algebras*, Colluquim Publications, Vol. 24, Amer. Math. Soc., Providence, 1961.

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

[KMRT] M. Knus, A. Merkurjev, M. Rost, J.P. Tignol, *The book of involutions*, Colluquim Publications, Vol. 44, Amer. Math. Soc., Providence, 1998.

[LRRS] M. Lorenz, Z. Reichstein, L.H. Rowen, D.J. Saltman, *Fields of definition for division algebras*, J. London Math. Soc. (2) **68** (2003), no. 3, 651-670.

[LMMR] . Lotscher, M. MacDonald, A. Meyer, Z. Riechstein, *Essential p-dimension of algebraic tori*, preprint, www.mathematik.uni-bielefeld.de/LAG/man/363.ps.gz.

[M] A. Merkurjev, *Essential p-dimension of* PGL_{p^2}, J. Amer. Math. Soc. **23** (2010), 693-712.

[MR1] A. Meyer, Z. Reichstein, *The essential dimension of the normalizer of a maximal torus in the projective linear group*, Algebra and Number Theory, **3** (2009), no.4, 467-487.

[MR2] A. Meyer, Z. Reichstein, *An upper bound on the essential dimension of a central simple algebra*, to appear in the issue of Journal of Algebra dedicated to Corrado de Concini's 60th birthday.

[R] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transform. Groups **5** (2000), no. 3, 265-304.

[R2] Z. Reichstein, *Essential dimension: a survey*, lecture notes for the workshop on essential and canonical dimension in Lens, France, http://www.math.ubc.ca/ reichst/lens-notes6-27-8.pdf.

[RS] L.H. Rowen, D.J. Saltman, *Prime to p extensions of division algebras*, Israel J. math. **78** (1992), no. 2-3, 197-207.

[S] D.J. Saltman, *Lectures on division algebras*, CMBS Regional Conference Series in Mathematics, No. 94, Amer. Math. Soc., Providence, 1999.

Department of Mathematics, University of California, Los Angeles, CA 90095-1555, USA

E-mail address: aruozzi@math.ucla.edu