ESSENTIAL DIMENSION OF ALGEBRAIC TORI

ALEXANDER S. MERKURJEV

1. Introduction

Let T be an algebraic torus over a field F. We can view T as a functor from the category of field extensions of F to the category of groups (or sets) taking a field extension K/F to the group $T(K)$ of points of T over K. The group $T(K)$ contains the subgroup $RT(K)$ of "rationally parameterized" points that can be connected with the identity by a rational curve. The quotient group of R-equivalence classes $T(K)/R = T(K)/RT(K)$ measures complexity of the torus T. For example, if T is a rational variety, then the group $T(K)/R$ is trivial for every K.

In the present paper we study the essential dimension $\operatorname{ed}(T/R)$ of the functor T/R taking a field K to $T(K)/R$. The nonnegative integer $\operatorname{ed}(T/R)$ provides a numerical invariant of T that also measures complexity of T. In particular, $\operatorname{ed}(T/R)$ is equal to zero if and only if the torus T is R-trivial, i.e., $RT(K) = T(K)$ for all field extensions K/F. The larger the essential dimension of T/R, the more complicated the functor. For example, T/R cannot be parameterized by the points of a variety of dimension less than $\operatorname{ed}(T/R)$.

In the second part of the paper we consider several examples of the computation of $\operatorname{ed}(T/R)$ and give their interpretations.

2. Essential dimension

Let F be a base field. Let $\mathcal{F} : \mathit{Fields}_F \to \mathit{Sets}$ be a functor, K/F a field extension, $x \in \mathcal{F}(K)$ and $\alpha : K_0 \to K$ a morphism in Fields_F (i.e., K is a field extension of K_0 over F). We say that x is *defined over* K_0 (or K_0 *is a field of definition of* x) if there is an element $x_0 \in \mathcal{F}(K_0)$ such that $\mathcal{F}(\alpha)(x_0) = x$, i.e., x belongs to the image of the map $\mathcal{F}(\alpha) : \mathcal{F}(K_0) \to \mathcal{F}(K)$.

We define the *essential dimension of* x:

$$\operatorname{ed}(x) := \min \operatorname{tr.deg}_F(K_0),$$

where $\operatorname{tr.deg}_F$ is the transcendence degree over F and the minimum is taken over all fields of definition K_0 of x and the *essential dimension of the functor* $\mathcal{F}$:

$$\operatorname{ed}(\mathcal{F}) := \max \operatorname{ed}(x),$$

where the maximum runs over all field extensions K/F and all $x \in \mathcal{F}(K)$ (see [7]).

The essential dimension of a functor $\mathcal{F}$ is an integer that measures the complexity of the functor $\mathcal{F}$. Informally speaking, essential dimension $\operatorname{ed}(\mathcal{F})$ is the smallest number of algebraically independent parameters required to define the functor.

Example 2.1. [6, Corollary 1.4] Let X be a variety (a scheme of finite type) over F. We can view X as a functor from Fields_F to Sets taking a field extension K/F to the set of K-points $X(K) := \mathrm{Mor}_F(\mathrm{Spec}\, K, X)$. Then $\mathrm{ed}(X) = \dim(X)$.

If $\alpha : \mathcal{F} \to \mathcal{F}'$ a morphism of functors from Fields_F to Sets such that the map $\mathcal{F}(K) \to \mathcal{F}'(K)$ is surjective for every a field extension K/F, then $\mathrm{ed}(\mathcal{F}) \geqslant \mathrm{ed}(\mathcal{F}')$.

If $\mathcal{F}$ is a functor such that for every K/F the set $\mathcal{F}(K)$ is parameterized by the point $X(K)$ for some variety X over F, i.e., there is a surjective morphism of functors $X \to \mathcal{F}$, then by Example 2.1, we have an upper bound $\mathrm{ed}(\mathcal{F}) \leqslant \dim(X)$ for the essential dimension of $\mathcal{F}$.

Let G be an algebraic group over F. Consider the functor

$$G\text{-}\mathit{torsors} : \mathit{Fields}_F \to \mathit{Sets},$$

taking a field K/F to the set $G\text{-}\mathit{torsors}(K)$ of isomorphism classes of G-torsors over $\mathrm{Spec}(K)$. The *essential dimension* $\mathrm{ed}(G)$ *of* G is defined in [8] as the essential dimension of the functor $G\text{-}\mathit{torsors}$:

$$\mathrm{ed}(G) := \mathrm{ed}(G\text{-}\mathit{torsors}).$$

Thus, the essential dimension of G measures the complexity of the class of G-torsors over field extensions of F.

An algebraic group G over F is called *special* if all G-torsors over all field extensions of F are trivial. Clearly, if G is special, then $\mathrm{ed}(G) = 0$ The converse also holds.

Proposition 2.2. [7, Proposition 3.16] *An algebraic group G is special if and only if* $\mathrm{ed}(G) = 0$.

3. Lattices

Let R be a PID. A *lattice over* R is a free R-module of finite rank. An abelian group A is a *lattice* if A is a lattice over $\mathbb{Z}$.

Let G be a finite group. A lattice A over R is called a *G-lattice* if there is given a G-action on A by R-module automorphisms.

A G-lattice A is called a *permutation lattice* if A admits a G-invariant R-basis.

Let p be a prime integer and let G be a group of order p^r. Let

$$J = \mathrm{Ker}(\mathbb{Z}[G] \xrightarrow{\varepsilon_p} \mathbb{F}_p),$$

where ε_p is the mod p augmentation. The ideal J is generated by p and $g-1$ for all $g \in G$ and $\mathbb{Z}[G]/J \simeq \mathbb{F}_p$.

Let A be a G-lattice (over $\mathbb{Z}$). Define the $\mathbb{F}_p$-vector space

$$\overline{A} := A/JA = A \otimes_{R[G]} \mathbb{F}_p.$$

For a subgroup $H \subset G$, consider the composition

$$\varphi_H : A^H \hookrightarrow A \to \overline{A}.$$

For every $k \geqslant -1$, let A_k denote the subspace of $\overline{A}$ spanned by the images of φ_H taken over all subgroups $H \subset G$ with $[G : H] \leqslant p^k$. We have a filtration of $\overline{A}$ by subspaces

$$0 = A_{-1} \subset A_0 \subset \cdots \subset A_r = \overline{A}.$$

Consider the following integer associated with the G-lattice A:

$$j(A) := \sum_{k=0}^{r} \dim_{\mathbb{F}_p}(A_k/A_{k-1}) \cdot p^k \geqslant 0.$$

Clearly, $j(A \oplus B) = j(A) + j(B)$ for every two G-lattices A and B.

Lemma 3.1. *If A is a permutation G-lattice, then $j(A) = \operatorname{rank}(A)$.*

Proof. We may assume that $A = \mathbb{Z}[G/H]$, where H is a subgroup of G of index p^s for some $s = 0, 1, \dots, r$. We have $\overline{A} \simeq \mathbb{F}_p$ and

$$A_k = \begin{cases} 0, & \text{if } i < s; \\ \mathbb{F}_p, & \text{if } k \geqslant s. \end{cases}$$

Therefore, $j(A) = p^s = \operatorname{rank}(A)$. □

Lemma 3.2. *If B is a quotient lattice of a G-lattice A, then $j(A) \geqslant j(B)$.*

Proof. Let $f : A \to B$ is a surjective homomorphism of G-lattices. Let $C_k = \bar{f}(A_k)$, where $\bar{f} : \overline{A} \to \overline{B}$ is the induced linear map of vector spaces over F_p. Set

$$a_k = \dim(A_k), \qquad b_k = \dim(B_k), \qquad c_k = \dim(C_k).$$

As $C_k \subset B_k$, we have $c_k \leqslant b_k$. Note also that $C_r = B_r = \overline{B}$, hence $c_r = b_r$.

Since the natural map $A_k/A_{k-1} \to C_k/C_{k-1}$ is surjective, we have

$$a_k - a_{k-1} \geqslant c_k - c_{k-1}.$$

It follows from the above inequalities that

$$\begin{aligned} j(A) &= \sum_{k=0}^{r} (a_k - a_{k-1})p^k \\ &\geqslant \sum_{k=0}^{r} (c_k - c_{k-1})p^k \\ &= c_r p^r + \sum_{k=0}^{r-1} c_k(p^k - p^{k+1}) \\ &\geqslant b_r p^r + \sum_{k=0}^{r-1} b_k(p^k - p^{k+1}) \\ &= \sum_{k=0}^{r} (b_k - b_{k-1})p^k \\ &= j(B). \end{aligned}$$

□

Proposition 3.3. *Let G be a p-group and let A be a G-lattice. Then*
1. For every surjective homomorphism of G-lattices $Q \to A$ with Q a permutation lattice, we have $\operatorname{rank}(Q) \geqslant j(A)$.
2. There is a homomorphism of G-lattices $Q \to A$ with Q a permutation lattice such that the induced linear map $\overline{Q} \to \overline{A}$ is an isomorphism and $\operatorname{rank}(Q) = j(A)$.

Proof. 1. Follows from Lemmas 3.1 and 3.2.

2. For every $k \geqslant 0$ choose a subset X_k of A in the pre-image of A_k under the canonical map $A \to \overline{A}$ with the property that for any $x \in X_k$ there is a subgroup $H_x \subset G$ with $x \in A^{H_x}$ and $[G : H_x] = p^k$ such that the composition

$$X_k \to A_k \to A_k/A_{k-1}$$

yields a bijection between X_k and a basis for A_k/A_{k-1}. In particular, $|X_k| = a_k - a_{k-1}$ and the union of the images of the compositions $X_k \to A_k \to \overline{A}$ is a basis for $\overline{A}$. Consider the G-homomorphism

$$f : Q = \coprod_{k=0}^{r} \coprod_{x \in X_k} R[G/H_x] \to A,$$

taking 1 in $R[G/H_x]$ to x in A.

By construction, the induced linear map $\overline{Q} \to \overline{A}$ is an isomorphism. The rank of the permutation G-module Q is equal to

$$\sum_{k=0}^{r} \sum_{x \in X_k} p^k = \sum_{k=0}^{r} |X_k| \cdot p^k = \sum_{k=0}^{r} (a_k - a_{k-1}) \cdot p^k = j(A). \qquad \square$$

Let $\mathbb{Z}_{(p)}$ be the localization of $\mathbb{Z}$ by the prime ideal $p\mathbb{Z}$ and set $A_{(p)} := A \otimes \mathbb{Z}_{(p)}$.

Corollary 3.4. *Let A be a G-lattice. Then*
1. $j(A) \geqslant \operatorname{rank}(A)$.
2. $j(A) = \operatorname{rank}(A)$ if and only if $A_{(p)}$ is a permutation G-lattice over $\mathbb{Z}_{(p)}$.

Proof. 1. It follows from Proposition 3.3(2) that there is a homomorphism $f : Q \to A$ with Q a permutation lattice such that $\overline{Q} \to \overline{A}$ is an isomorphism and $\operatorname{rank}(Q) = j(A)$. Note that J generates the Jacobson radical of the local ring $\mathbb{Z}_{(p)}[G]$. By the Nakayama Lemma, the homomorphism $f_{(p)} : Q_{(p)} \to A_{(p)}$ is surjective, hence $j(A) = \operatorname{rank}(Q) \geqslant \operatorname{rank}(A)$.

2. $\Rightarrow$: If $j(A) = \operatorname{rank}(A)$, then $\operatorname{rank}(Q) = \operatorname{rank}(A)$, hence $f_{(p)}$ is an isomorphism.
$\Leftarrow$: If $A_{(p)}$ is a permutation G-lattice over $\mathbb{Z}_{(p)}$, then there is a permutation sublattice $B \subset A$ (over $\mathbb{Z}$) such that A/B is finite of order prime to p. Hence by Lemma 3.1, $j(A) = j(B) = \operatorname{rank}(B) = \operatorname{rank}(A)$. $\square$

Remark 3.5. It follows from Corollary 3.4 that for a p-group G a direct summand of a permutation G-lattice over $\mathbb{Z}_{(p)}$ is also permutation (see [5, Theorem 5.11.2]).

4. Algebraic tori

Let L/F be a finite Galois field extension with Galois group G. An algebraic group T is an *algebraic torus* split by L if $T \times_F \operatorname{Spec} L$ is isomorphic to the product of finitely many copies of the multiplicative group $\mathbb{G}_{m,L}$. We call G a *decomposition group* of T.

The *character group* $T^* := \operatorname{Hom}_L(T_L, \mathbb{G}_{m,L})$ is a G-lattice of rank $\dim(T)$. The cocharacter G-lattice $T_* := \operatorname{Hom}_L(\mathbb{G}_{m,L}, T_L)$ is dual to T^*. The torus T is determined by the character lattice T^* via the formula

$$T = \operatorname{Spec}(L[T^*]^G),$$

where $L[T^*]$ is the group algebra of T^* over L. A torus T is called *quasi-trivial* if its character lattice is permutation.

Example 4.1. If X be a finite G-set, then the F-algebra C of G-equivariant maps $X \to L$ is étale. The Weil transfer $R_{L/F}(\mathbb{G}_{m,C})$ (that is the group of invertible elements in C) is a quasi-trivial torus with the permutation character G-lattice $\mathbb{Z}[X]$.

A torus S is called *invertible* if there is a torus S' such that $S \times S'$ is a quasi-trivial torus.

Proposition 4.2. *Let S be an algebraic torus. The following are equivalent:*

(1) $\mathrm{ed}(S) = 0$,
(2) *S is special,*
(3) *S is invertible.*

Proof. (1) $\Leftrightarrow$ (2) by Proposition 2.2,
(2) $\Leftrightarrow$ (3) is proved in [2, Theorem 4.10]. □

Let T be an algebraic torus over F and let K/F be a field extension. Write $RT(K)$ for the subgroup of all *R-trivial* elements in $T(K)$ (see [3, §4]). This is the subgroup of the elements in $T(K)$ that can be connected by a rational curve with the identity. Equivalently, the subgroup $RT(K)$ is generated by the images of the maps $P(K) \to T(K)$ for all group homomorphisms $P \to T$, where P is a quasi-trivial torus (see [3, Theorem 2]). Informally speaking, $RT(K)$ is the subgroup of "rationally parameterized" elements in $T(K)$.

The assignment $K \mapsto T(K)/R := T(K)/RT(K)$ extends to a functor $T/R : \mathsf{Fields}_F \to \mathsf{Sets}$.

Let

$$1 \to S \to P \to T \to 1 \tag{4.3}$$

be an exact sequence of tori with decomposition group G. The torus S is called *flasque* if $H^1(H, S_*) = 0$ for all subgroups $H \subset G$ (equivalently, the map $(P_*)^H \to (T_*)^H$ is surjective).

Every torus T over F admits an exact sequence (4.3) such that S is a flasque torus and P is a quasi-trivial torus. Such a sequence is called a *flasque resolution of T*. The connecting homomorphism $T(K) \to H^1(K, S)$ yields an isomorphism

$$T(K)/R \xrightarrow{\sim} H^1(K, S).$$

In other words, the functors T/R and S-$\mathsf{torsors}$ are isomorphic. In particular,

$$\mathrm{ed}(T/R) = \mathrm{ed}(S). \tag{4.4}$$

We have proved the following proposition.

Proposition 4.5. *The torus T is R-trivial if and only if S satisfies the equivalent conditions of Proposition 4.2.*

Thus, the essential dimension of S measures the deviation of T from an R-trivial torus. Since every stably rational torus is R-trivial, the integer $\mathrm{ed}(T/R) = \mathrm{ed}(S)$ also measures the deviation of T from a stably rational variety.

Remark 4.6. The natural surjection of functors $T \to T/R$ yields the obvious upper bound $\operatorname{ed}(T/R) \leqslant \operatorname{ed}(T) = \dim(T)$ for the essential dimension of T/R. More generally, if X is an algebraic variety that admits a surjective morphism of functors $X \to T/R$, then $\operatorname{ed}(T/R) \leqslant \dim(X)$. Thus, the functor T/R cannot be parameterized by the points of a variety of dimension less than $\operatorname{ed}(T/R)$.

The following statements relates the invariant j defined in Section 3 and the essential dimension.

Theorem 4.7. *Let T be a torus over a field F and p a prime integer different from* $\operatorname{char}(F)$. *Let (4.3) be a flasque resolution of T. If the decomposition group of T is a p-group, then*

$$\operatorname{ed}(T/R) = \operatorname{ed}(S) = j(S^*) - \dim(S).$$

Proof. The first equality is (4.4). The second one was proved in [1, Theorem 3.1]. □

5. Decomposable algebras

Let r be a positive integer and p a prime integer, F a field containing a primitive root of unity ξ of degree p. Let $a_1, a_2, \dots, a_r \in F^\times$ and let

$$L = F(a_1^{1/p}, a_2^{1/p}, \dots, a_r^{1/p})$$

be a multi-cyclic Galois field extension of F with Galois group G an elementary p-group of order p^r. Choose the generators $\sigma_1, \sigma_2, \dots, \sigma_r$ of G such that $\sigma_i(a_j^{1/p}) = \xi^{\delta_{ij}} a_j^{1/p}$.

For a field extension K/F, let $\operatorname{Br}(KL/K)[p]$ denote the subgroup of elements of exponent p in the *relative Brauer group* $\operatorname{Ker}(\operatorname{Br}(K) \to \operatorname{Br}(K \otimes_F L))$.

The group $\operatorname{Br}(KL/K)[p]$ contains the subgroup of *decomposable* elements of the form $\sum_{i=1}^r (a_i, b_i)$ for all $b_i \in K^\times$, where (a_i, b_i) is the class of cyclic algebra of degree p (see [4, §2.5]). We write $\operatorname{Br}(KL/K)[p]_{\mathrm{ind}}$ for the quotient group of $\operatorname{Br}(KL/K)[p]$ by the subgroup of decomposable elements.

Consider the functor

$$\mathcal{B}r(L/F)[p]_{\mathrm{ind}} : \mathit{Fields}_F \to \mathit{Sets}$$

taking a field K to $\operatorname{Br}(KL/K)[p]_{\mathrm{ind}}$.

Following [1, §2], we will find a torus T such that $T/R \simeq \mathcal{B}r(L/F)[p]_{\mathrm{ind}}$ and compute $\operatorname{ed}(T/R)$.

Proposition 5.1. *If $r \geqslant 2$,*

$$\operatorname{ed}(\mathcal{B}r(L/F)[p]_{\mathrm{ind}}) = \begin{cases} (r-1)2^{r-1} - r & \text{if } p = 2, \\ (r-1)p^r + p^{r-1} - r & \text{if } p > 2. \end{cases}$$

Proof. Consider the G-module homomorphism $h : \mathbb{Z}[G]^{r+1} \to \mathbb{Z}[G]$ taking the ith canonical basis element e_i to $\sigma_i - 1$ for $1 \leqslant i \leqslant r$ and e_{r+1} to p. The image of h coincides with the ideal J introduced in Section 3.

Set $N := \operatorname{Ker}(h)$ and write $w_i = 1 + \sigma_i + \sigma_i^2 + \dots + \sigma_i^{p-1} \in R$ for $1 \leqslant i \leqslant r$. The following elements in N:

$$e_{ij} = (\sigma_i - 1)e_j - (\sigma_j - 1)e_i, \quad f_i = w_i e_i, \quad \text{and} \quad g_i = -pe_i + (\sigma_i - 1)e_{r+1}$$

for all $1 \leqslant i, j \leqslant r$, generate the G-module N.

Let $\varepsilon_i : R^{r+1} \to \mathbb{Z}$ be the ith projection followed by the augmentation map ε. Since $\varepsilon_i(N) = p\mathbb{Z}$ for every $i = 1, \dots, r$, we have a surjective G-homomorphism

$$q : N \to \mathbb{Z}^r, \quad x \mapsto \big(\varepsilon_1(x)/p, \dots, \varepsilon_r(x)/p\big).$$

Set $M := \mathrm{Ker}(q)$ and $Q := R^{r+1}/M$.

We have the following diagram of homomorphisms of G-modules with the exact columns and rows

(5.2)
$$\begin{array}{ccccc} M & = & M & & \\ \downarrow & & \downarrow & & \\ N & \hookrightarrow & \mathbb{Z}[G]^{r+1} & \xrightarrow{h} & J \\ \downarrow{\scriptstyle q} & & \downarrow & & \| \\ \mathbb{Z}^r & \hookrightarrow & Q & \twoheadrightarrow & J \end{array}$$

Lemma 5.3. *The G-lattice Q is flasque.*

Proof. Let $Q' \subset Q$ be the pre-image of $I := \mathrm{Ker}(\mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z})$ under $Q \to J$. Since $Q/Q' \simeq J/I \simeq \mathbb{Z}$ is flasque, it suffices to show that Q' is flasque. Consider the dual $0 \to \mathbb{Z}[G]/\mathbb{Z}N_G \to W \to \mathbb{Z}^r \to 0$ of the exact sequence $0 \to \mathbb{Z}^r \to Q' \to I \to 0$. It suffices to show that W is coflasque. Let $H \subset G$ be a subgroup. Since

$$H^1(H, \mathbb{Z}[G]/\mathbb{Z}N_G) \simeq H^2(H, \mathbb{Z}) \simeq H^\vee := \mathrm{Hom}(H, \mathbb{Q}/\mathbb{Z}),$$

we have an exact sequence

$$\mathbb{Z}^r \to H^\vee \to H^1(H, W) \to 0.$$

By functoriality in H of the first map, the composition is equal to $\mathbb{Z}^r \to G^\vee \xrightarrow{\mathrm{res}} H^\vee$. The first map takes the ith basis element to the character dual to σ_i, so the first map is surjective. The restriction map is also surjective. It follows that $H^1(H, W) = 0$, i.e., W is coflasque. □

Let P, S, T and U be the algebraic tori with character lattices $\mathbb{Z}[G]^{r+1}$, Q, M and J respectively. We have two exact sequences

$$1 \to S \to P \to T \to 1, \tag{5.4}$$

$$1 \to U \to S \to (\mathbb{G}_m)^r \to 1. \tag{5.5}$$

By Lemma 5.3, the sequence (5.4) is a flasque resolution of the torus T.

Since $\mathbb{Z}[G]/J = \mathbb{F}_p$, we have an exact sequence

$$1 \to \mu_p \to R_{L/F}(\mathbb{G}_m) \to U \to 1$$

that in its turn yields a canonical isomorphism

$$H^1(K, U) \simeq \mathrm{Br}(KL/K)[p].$$

The sequence (5.5) and Hilbert Theorem 90 give an exact sequence

$$(K^\times)^{\oplus r} \to H^1(K, U) \to H^1(K, S) \to 1,$$

where the image of the first map coincides with the subgroup of decomposable classes in $H^1(K,U) = \mathrm{Br}(KL/K)[p]$. It follows that

$$T(K)/R \simeq H^1(K,S) \simeq \mathrm{Br}(KL/K)[p]_{\mathrm{ind}}.$$

Set $A = S^*$. The following was computed in [1, §3]. If $p = 2$,

$$\dim A_k = \begin{cases} r+1 & \text{if } k = r \text{ or } k = r-1, \\ 0 & \text{if } 0 \leqslant k < r-1. \end{cases}$$

It follows that $j(S^*) = (r+1)2^{r-1}$ and by Theorem 4.7,

$$\mathrm{ed}(\mathcal{B}r(L/F)[2]_{\mathrm{ind}}) = j(S^*) - \dim(S) = (r+1)2^{r-1} - (2^r - r) = (r-1)2^{r-1} - r.$$

If $p > 2$,

$$\dim A_k = \begin{cases} r+1 & \text{if } k = r, \\ 1 & \text{if } k = r-1, \\ 0 & \text{if } 0 \leqslant k < r-1. \end{cases}$$

It follows that $j(S^*) = rp^r + p^{r-1}$ and by Theorem 4.7,

$$\mathrm{ed}(\mathcal{B}r(L/F)[p]_{\mathrm{ind}}) = j(S^*) - \dim(S) = (rp^r + p^{r-1}) - (p^r - r) = (r-1)p^r + p^{r-1} - r. \ \square$$

Remark 5.6. It follows from Proposition 5.1 that the essential dimension of $\mathrm{Br}[p]_{\mathrm{ind}}$ is zero only in the case $r = p = 2$. Indeed, every exponent 2 central simple algebra that is split over a biquadratic extension is decomposable. For all other values of r and p, the essential dimension of the functor $\mathcal{B}r(L/F)[p]_{\mathrm{ind}}$ is nonzero (and quite large). It follows that for every field F there are examples of indecomposable algebras of exponent p over an extension of F (cf. [9]).

6. Bicyclic extensions

Let p be a prime integer and F a field containing a primitive pth root of unity ξ. Let $a, b \in F^\times$ and let $L = F(a^{1/p}, b^{1/p})$ be a bicyclic extension of F of degree p^2 with Galois group $G = \langle \sigma_a, \sigma_b \rangle$, where $\sigma_a(a^{1/p}) = \xi \cdot a^{1/p}$, $\sigma_a(b^{1/p}) = b^{1/p}$, $\sigma_b(a^{1/p}) = a^{1/p}$, $\sigma_b(b^{1/p}) = \xi \cdot b^{1/p}$.

Denote by T the kernel of the homomorphism $R_a(\mathbb{G}_m) \times R_b(\mathbb{G}_m) \to \mathbb{G}_m$ taking (u,v) to $N_a(u) \cdot N_b(v)^{-1}$. Here $R_a = R_{F(a^{1/p})/F}$ is the Weil transfer and N_a is the norm map $F(a^{1/p})^\times \to F^\times$. In other words,

$$T(K) = \{(u,v) \in K(a^{1/p})^\times \times K(a^{1/p})^\times \mid N_a(u) = N_b(v)\} \tag{6.1}$$

for a field extension K/F. We determine the functor T/R and compute $\mathrm{ed}(T/R)$.

There is an exact sequence of tori

$$1 \to T \to R_a(\mathbb{G}_m) \times R_b(\mathbb{G}_m) \to \mathbb{G}_m \to 1$$

and the dual sequence of character lattices

$$0 \to \mathbb{Z} \to \Lambda_a \oplus \Lambda_b \to T^* \to 0, \tag{6.2}$$

where $\Lambda_a = \mathbb{Z}[G/\langle \sigma_b \rangle]$, $\Lambda_b = \mathbb{Z}[G/\langle \sigma_a \rangle]$.

Proposition 6.3. *Let T be the torus defined by (6.1). The subgroup of R-trivial elements $RT(K) \subset T(K)$ consists of all pairs*

$$(c \cdot (\sigma_a - 1)x \cdot N_b(z),\ c \cdot (\sigma_b - 1)y \cdot N_a(z)),$$

where $c \in K^\times$, $x \in K(a^{1/p})^\times$, $y \in K(b^{1/p})^\times$, $z \in K(a^{1/p}, b^{1/p})^\times$ and

$$\mathrm{ed}(T/R) = \begin{cases} 2p-2, & \text{if } p \text{ is odd;} \\ 0, & \text{if } p = 2. \end{cases}$$

Proof. Let S be the kernel of the homomorphism $P \to T$, where

$$P = \mathbb{G}_m \times R_a(\mathbb{G}_m) \times R_b(\mathbb{G}_m) \times R_{a,b}(\mathbb{G}_m),$$

taking (c, x, y, z) to $(c \cdot (\sigma_a - 1)x \cdot N_b(z),\ c \cdot (\sigma_b - 1)y \cdot N_a(z))$. Note that $\dim(S) = p^2 + 2$.

Lemma 6.4. *The torus S is flasque.*

Proof. We need to prove that for any subgroup $H \subset G$ the co-character map $P_*^H \to T_*^H$ is surjective. The G-lattice T_* is the kernel of $\varepsilon_a - \varepsilon_b : \Lambda_a \oplus \Lambda_b \to \mathbb{Z}$.

Case 1: $H = G$. The group T_*^H is generated by (N_a, N_b) that is the image of 1 under $\mathbb{Z} = \mathbb{Z}^H \subset P_*^H \to T_*^H$.

Case 2: $H = \langle \sigma_a \rangle$. The group T_*^H is generated by (N_a, p) and $(0, \sigma_b - 1)$. The first generator is the image of $\sum_{i=0}^{p-1} \sigma_a^i$ under $\Lambda_a^H \subset P_*^H \to T_*^H$. The second generator is the image of -1 under $\Lambda_b^H = \Lambda_b^H \subset P_*^H \to T_*^H$. The case $H = \langle \sigma_b \rangle$ is similar.

Case 3: H is generated by $\sigma_a \sigma_b^i$ for some i prime to p. Then $T_*^H = T_*^G$ and we are reduced to Case1. □

We return to the proof of Proposition 6.3. It follows from Lemma 6.4 that the sequence

$$1 \to S \to P \to T \to 1$$

is a flasque resolution of T, hence $RT(K) = \mathrm{Im}(P(K) \to T(K))$. This proves the first statement.

We have an exact sequence of character lattices:

$$0 \to T^* \to \mathbb{Z} \oplus \Lambda_a \oplus \Lambda_b \oplus \Lambda \to S^* \to 0, \tag{6.5}$$

where $\Lambda = \mathbb{Z}[G]$. The composition

$$\Lambda_a \oplus \Lambda_b \to T^* \to \mathbb{Z} \oplus \Lambda_a \oplus \Lambda_b \oplus \Lambda$$

of the two homomorphisms in (6.2) and (6.5) is as follows:

$$(1, 0) \mapsto (1, \sigma_a - 1, 0, N_b),$$

$$(0, 1) \mapsto (1, 0, \sigma_b - 1, N_a).$$

In the notation of Section 3 we have $\overline{P}^* = (\mathbb{F}_p)^{\oplus 4}$. The image of $\overline{T}^* \to \overline{P}^*$ is $\mathbb{F}_p \oplus 0^{\oplus 3} \subset (\mathbb{F}_p)^{\oplus 4}$, hence for $A := S^*$ we have $\overline{A} = (\mathbb{F}_p)^{\oplus 3}$. Since $|G| = p^2$, we have a filtration

$$0 = A_{-1} \subset A_0 \subset A_1 \subset A_2 = \overline{A} = (\mathbb{F}_p)^{\oplus 3}$$

as defined in Section 3. It follows from the exact sequence (6.2) that the sequence

$$0 \to H^1(G, T^*) \to H^2(G, \mathbb{Z}) \to H^2(\langle \sigma_a \rangle, \mathbb{Z}) \oplus H^2(\langle \sigma_b \rangle, \mathbb{Z})$$

is exact. The last homomorphism in the sequence is identified with $G^\vee \to \langle\sigma_a\rangle^\vee \oplus \langle\sigma_b\rangle^\vee$ given by the restrictions, so it is an isomorphism. Therefore, $H^1(G, T^*) = 0$.

It follows from (6.5) that the map $(P^*)^G \to (S^*)^G$ is surjective. As a consequence, the space A_0 is trivial since the image of $(P^*)^G \to \overline{P}^* \to \overline{A}$ is zero. By (6.5) again, the images of $(0, 1, 0, 0)$ from $\Lambda_a^{\langle\sigma_a\rangle}$ and of $(0, 0, 1, 0)$ from $\Lambda_b^{\langle\sigma_a\rangle}$ in $\overline{A}$ yield $\dim(A_1) \geqslant 2$. Thus, the dimension of A_1 is either 2 or 3.

Now assume that p is odd. If $\dim(A_1) = 3$, then

$$j(S^*) = j(A) = 3p < p^2 + 2 = \operatorname{rank}(S^*).$$

This contradicts Proposition 3.3. Thus, $\dim(A_1) = 2$, therefore, $j(S^*) = p^2 + 2p$. By Theorem 4.7,

$$\operatorname{ed}(T/R) = \operatorname{ed}(S) = j(S^*) - \dim(S) = (p^2 + 2p) - (p^2 + 2) = 2p - 2.$$

In the case $p = 2$, consider $x = (0, 1, -1, \sigma_a) \in P^*$. The element

$$(\sigma_a\sigma_b - 1)x = (0, \sigma_a - 1, 1 - \sigma_b, \sigma_b - \sigma_a)$$

is the image of $(1, -1)$ from T^* since $\sigma_b - \sigma_a = N_b - N_a$. Hence the image of x in S^* is $\sigma_a\sigma_b$-invariant and we have $\dim(A_1) = 3$. Thus, in this case $j(S^*) = 6 = \operatorname{rank}(S^*)$ and hence $\operatorname{ed}(T/R) = \operatorname{ed}(S) = 0$. □

Remark 6.6. The value $\operatorname{ed}(T/R) = 2p - 2$ is smaller than the upper bound given by $\dim(T) = 2p - 1$. Let $\mathbb{G}_m \to T$ be the homomorphism taking a to the pair (a, a). There is an exact sequence

$$1 \to \mathbb{G}_m \to T \to T' \to 1$$

for a torus T' of dimension $2p - 2$. We have $T/R = T'/R$ and

$$\operatorname{ed}(T/R) = \operatorname{ed}(T'/R) \leqslant \operatorname{ed}_p(T') \leqslant \dim(T') = 2p - 2.$$

We have shown that the obvious upper bound $\operatorname{ed}(T'/R) \leqslant \dim(T')$ is an equality.

Remark 6.7. If $p = 2$ the torus T is a rational variety. In fact, we have an exact sequence of tori:

$$1 \to R_{ab}(\mathbb{G}_m) \to \mathbb{G}_m \times R_{a,b}(\mathbb{G}_m) \to T \to 1,$$

where $R_{a,b}(\mathbb{G}_m) = R_{F(a^{1/p},\ b^{1/p})/F}(\mathbb{G}_m)$, the first map takes x to $(N(x), x)$ and the second map takes (y, z) to $(y^{-1} \cdot N_b(z), y^{-1} \cdot N_a(z))$. It follows that $T \simeq (\mathbb{G}_m \times R_{a,b}(\mathbb{G}_m))/R_{ab}(\mathbb{G}_m)$ is a rational (and hence R-trivial) torus.

7. Norm one tori

Let p a prime integer and let L/F be a finite Galois field extension of degree p^r with Galois group G. Let T be the norm 1 torus for the extension L/F,

$$T(K) = \{x \in (KL)^\times \mid N_{KL/K}(x) = 1\},$$

so that $T^* = \mathbb{Z}[G]/\mathbb{Z}N_G$, where $N_G = \sum_{g\in G} g \in \mathbb{Z}[G]$. We compute $\operatorname{ed}(T/R)$.

Proposition 7.1. *Let p be a prime and let T be the norm one torus for a Galois field extension L/F with Galois group G of order p^r. Then for any field extension K/F, the subgroup of R-trivial elements $RT(K) \subset T(K)$ is generated by $(g-1)y$ for all $g \in G$, $y \in (KL)^\times$ and*

$$\operatorname{ed}(T/R) = \begin{cases} p^r - 1, & \text{if } G \text{ is not cyclic;} \\ 0, & \text{if } G \text{ is cyclic.} \end{cases}$$

Proof. Let P be a permutation torus with P^* a free G-module with basis e_g, $g \in G$. Consider the G-equivariant injective homomorphism $\alpha : T^* \to P^*$ defined by

$$\alpha(u) = \sum_{g \in G} u(g-1)e_g$$

and let S be a torus with $S^* = \operatorname{Coker}(\alpha)$. By [10, §17.2, Theorem 1], S^* is a flasque G-module, hence the exact sequence

$$0 \to S \to P \to T \to 1 \tag{7.2}$$

is a flasque resolution of T and

$$RT(K) = \operatorname{Im}(P(K) \to T(K)) = \langle (g-1)y, \quad g \in G, y \in (KL)^\times \rangle$$

for all field extensions K/F. If G is cyclic, $H^1(K, S) = 0$ by Hilbert Theorem 90, so $\operatorname{ed}(S) = \operatorname{ed}(T/R) = 0$. In what follows we assume that G is not cyclic.

The first homomorphism in the exact sequence

$$\bar{T}^* \to \bar{P}^* \to \bar{S}^* \to 0$$

is trivial since $g - 1 \in J$ for all $g \in G$. It follows that $\bar{S}^* = \bar{P}^*$ is a vector space of dimension p^r over $\mathbb{F}_p$ with basis e_g, $g \in G$.

Set $A := S^*$ and compute the sequence

$$0 = A_{-1} \subset A_0 \subset \cdots \subset A_r = \bar{A}$$

defined in Section 3. We have $\dim(\bar{A}) = p^r$ and claim that $A_0 = A_1 = \ldots = A_{r-1} = 0$. It suffices to show that $A_{r-1} = 0$.

Let $H \subset G$ be a subgroup of index p^{r-1}, i.e., H is a cyclic group of order p. The exact sequence

$$0 \to \mathbb{Z} \xrightarrow{N_G} \mathbb{Z}[G] \to T^* \to 0$$

allows us to identify $H^1(H, T^*)$ with $H^2(H, \mathbb{Z}) = H^\vee$.

The sequence (7.2) yields an exact sequence

$$(P^*)^H \xrightarrow{\gamma} A^H \to H^1(H, T^*) \to H^1(H, P^*) = 0.$$

Note that $N_H \in J$, hence the composition $(P^*)^H \hookrightarrow P^* \to \bar{P}^*$ is trivial. It follows that the composition $A^H \hookrightarrow A \to \bar{A}$ factors through a map $\operatorname{Coker}\gamma \to \bar{A}$. Then the image of the composition coincides with the image of

$$H^2(H, \mathbb{Z}) \simeq H^1(H, T^*) \simeq \operatorname{Coker}\gamma \to \bar{A}. \tag{7.3}$$

We shall prove that this composition is trivial.

Choose a generator h_0 of H. For every H-module B we can then identify $H^2(H, B)$ with $B^G/N_G(B)$ and $H^1(H, B)$ with $\operatorname{Ker}(N_G)/(h_0 - 1)B$. The image in $H^1(H, T^*)$ of the

generator $1+p\mathbb{Z}$ of the cyclic group $H^2(H,\mathbb{Z})$ is the coset of $N_{G/H}:=\sum g_i$, where $\{g_i\}$ is a set of representatives of the right cosets of H in G.

Fix an element $g\in G$. The e_g-coefficient of the image of $N_{G/H}$ under the map $T^*\to P^*$ is equal to $N_{G/H}\cdot(g-1)$. For every i write $g_ig=(h_0)^{a_i}g_{\sigma(i)}$ for some integers $a_i=0,1,\dots,p-1$ and a permutation σ. We have

$$\begin{aligned} N_{G/H}\cdot(g-1) &= \sum_i g_i\cdot g-\sum_i g_i\\ &= \sum_i (h_0)^{a_i}\cdot g_{\sigma(i)}-\sum_i g_i\\ &= \sum_i ((h_0)^{a_i}-1)\cdot g_{\sigma(i)}\\ &= (h_0-1)\cdot\sum_i M_{a_i}\cdot g_{\sigma(i)}, \end{aligned}$$

where $M_a=1+h_0+\dots+h_0^{a-1}$. It follows that the image of $N_{G/H}$ in $\operatorname{Coker}\gamma$ in the composition (7.3) is represented by an element with the e_g-coefficient

$$\sum_i M_{a_i}\cdot g_{\sigma(i)}.$$

The e_g-coefficient of the image of this element in $\bar{A}=\coprod_{g\in G}\mathbb{F}_p e_g$ is equal to $\sum_i a_i$ modulo p. We need to show that the sum is divisible by p.

Let p^m be the order of the fixed element $g\in G$. Consider the right multiplication action of the subgroup D generated by g on the set $H\backslash G$ of right coset of H in G. For every orbit $X\subset H\backslash G$ let a_X be the sum of the a_i's such that $Hg_i\in X$. We shall prove that the sum of a_X over all orbits X is divisible by p.

Choose a D-orbit $X\subset H\backslash G$. We first determine the size of X. Let d in D stabilize a coset $Hx\in X$, i.e., $Hxd=Hx$, hence $xdx^{-1}\in H$. It follows that $d^p=1$, therefore, $d\in\langle g^{p^{m-1}}\rangle$. We proved that the orbit X has either p^m elements (when the stabilizer is trivial), or p^{m-1} elements (when the stabilizer is order p).

In the first case choose representatives $g_1,g_2,\dots,g_{p^m}$ of the cosets in X such that $g_ig=g_{i+1}$ for all $i=1,2,\dots,p^m-1$. Since $g_{p^m}g=g_1$, all the integers a_i for this orbit are zero, hence $a_X=0$.

In the second case, $Hxg^{p^{m-1}}=Hx$, hence $h:=xg^{p^{m-1}}x^{-1}\in H$. Choose representatives $g_1=x,g_2,\dots,g_{p^{m-1}}$ of the cosets in X such that $g_ig=g_{i+1}$ for all $i=1,2,\dots,p^{m-1}-1$. Since

$$g_{p^{m-1}}g=xg^{p^{m-1}}=hx=hg_1=(h_0)^bg_1$$

for some integer b, we have $a_X=b$.

We claim that for every other orbit $X'\subset H\backslash G$ of size p^{m-1} we have $a_{X'}=b$. Indeed, let $Hx'\in X'$ and set $h':=x'g^{p^{m-1}}(x')^{-1}\in H$. The element $x^{-1}x'$ normalizes the cyclic subgroup $\langle g^{p^{m-1}}\rangle$ of order p, hence it centralizes every element of this subgroup. It follows that $h'=h$ and hence $a_{X'}=a_X=b$.

Finally, it remains to show that the number v of the orbits of size p^{m-1} is divisible by p. Let u be the number of orbits of size p^m. We have $p^mu+p^{m-1}v=[G:H]=p^{s-1}$. Since G is not cyclic, we have $s>m$, therefore, v is divisible by p.

We have proved that in the case when the group G is not cyclic,

$$\mathrm{ed}(T/R) = j(S^*) - \dim(S) = (p^r \cdot p^r) - (p^{2r} - p^r + 1) = p^r - 1. \qquad \square$$

Remark 7.4. If G is not cyclic, the upper bound $\mathrm{ed}(T) \leqslant \dim(T)$ is an equality, that is the essential dimension $\mathrm{ed}(T) = \dim(T) = p^r - 1$ of T does not change when the functor $K \mapsto T(K)$ is replaced by the quotient functor $K \mapsto T(K)/R$.

References

[1] Sanghoon Baek and Alexander S. Merkurjev, *Essential dimension of central simple algebras*, Acta Math. **209** (2012), no. 1, 1–27. MR 2979508

[2] Sam Blinstein and Alexander Merkurjev, *Cohomological invariants of algebraic tori*, Algebra Number Theory **7** (2013), no. 7, 1643–1684. MR 3117503

[3] Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc, *La R-équivalence sur les tores*, Ann. Sci. École Norm. Sup. (4) **10** (1977), no. 2, 175–229. MR 56 #8576

[4] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, Cambridge, 2006. MR 2266528

[5] Markus Linckelmann, *The block theory of finite group algebras. Vol. I*, London Mathematical Society Student Texts, vol. 91, Cambridge University Press, Cambridge, 2018. MR 3821516

[6] Alexander S. Merkurjev, *Essential dimension*, Quadratic forms—algebra, arithmetic, and geometry, Contemp. Math., vol. 493, Amer. Math. Soc., Providence, RI, 2009, pp. 299–325. MR 2537108 (2010i:14014)

[7] Alexander S. Merkurjev, *Essential dimension: a survey*, Transform. Groups **18** (2013), no. 2, 415–481. MR 3055773

[8] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transform. Groups **5** (2000), no. 3, 265–304. MR 1780933 (2001j:20073)

[9] J.-P. Tignol, *Algèbres indécomposables d'exposant premier*, Adv. in Math. **65** (1987), no. 3, 205–228. MR 904723 (88h:16028)

[10] V. E. Voskresenskiĭ, *Algebraic groups and their birational invariants*, Translations of Mathematical Monographs, vol. 179, American Mathematical Society, Providence, RI, 1998, Translated from the Russian manuscript by Boris Kunyavski [Boris È. Kunyavskiĭ]. MR 99g:20090

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

Email address: merkurev@math.ucla.edu