ON THE ESSENTIAL DIMENSION OF CYCLIC GROUPS

WANSHUN WONG

Abstract. We find an upper bound for the essential dimension of finite cyclic groups $\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z}$ over a field F of characteristic different from p_i containing all the primitive p_i-th roots of unity, where p_i are distinct prime numbers.

1. Introduction

The essential dimension of an algebraic structure is a numerical invariant that measures the complexity of the structure. Informally, the essential dimension of an algebraic structure over a field F is the smallest number of algebraically independent parameters required to define the structure over a field extension of F (see [1] and [8]).

Let $\mathfrak{F} : Fields/F \to Sets$ be a functor (an algebraic structure) from the category $Fields/F$ of field extensions of F and field homomorphisms over F to the category of sets. Let $K \in Fields/F$ and $a \in \mathfrak{F}(K)$. The essential dimension of a, denoted $\mathrm{ed}(a)$, is the least transcendence degree $tr.deg_F(K_0)$ over all subfields K_0 of K over F such that a is in the image of the map $\mathfrak{F}(K_0) \to \mathfrak{F}(K)$. The essential dimension of the functor $\mathfrak{F}$ is

$$\mathrm{ed}(\mathfrak{F}) = \sup\{\mathrm{ed}(a)\}$$

where the supremum is taken over all $K \in Fields/F$ and all $a \in \mathfrak{F}(K)$.

If G is a finite group, we view G as a constant group scheme over a field F. The essential dimension of G is defined as

$$\mathrm{ed}(G) = \mathrm{ed}(H^1(-, G)).$$

Thus the essential dimension of G measures the complexity of the category G-torsors. If G is a finite cyclic p-group, and F is a field of characteristic different from p containing primitive p-th roots of unity, then the essential dimension of G is computed in [4] and [5]. In this paper we prove in Thm. 3.1 that if $G = \mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z}$ is a finite cyclic group, p_i are distinct prime numbers, and F is a field of characteristic different from p_i containing all the primitive p_i-th roots of unity, then

$$\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z}) \leq [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_r^{n_r}}) : F] - r + 1$$

where ξ_r denotes r-th primitive root of unity for any positive integer r.

Let A be a central division F-algebra of degree $q_1^{a_1}\cdots q_k^{a_k}$, where q_i are distinct prime numbers, a_i are non-negative integers. It is a conjecture (see [3]) that

$$\mathrm{cdim}(SB(A)) = q_1^{a_1} + \cdots + q_k^{a_k} - k$$

2000 *Mathematics Subject Classification.* 20G15; 14L30.

Key words and phrases. Essential dimension, finite cyclic groups, algebraic tori.

where $\mathrm{cdim}(SB(A))$ is the canonical dimension of the Severi-Brauer variety of A (see Section 4 for definition). If the conjecture is valid, then we show in Thm. 4.4 that

$$\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z}) = [F(\xi_{p_1^{n_1}}):F]+\cdots+[F(\xi_{p_r^{n_r}}):F]-r+1.$$

Acknowledgements: The author would like to thank his advisor Alexander Merkurjev for his help along the way.

2. Affine Group Schemes

References for affine group schemes are [6] and [10].

Let p be a prime number, F be a field such that $char(F)\neq p$ and $\xi_p\in F$. Let Γ be the absolute Galois group of F, i.e. $\Gamma = Gal(F_{sep}/F)$ where F_{sep} is a separable closure of F.

For any non-negative integer r, let $G_r=\mathbb{Z}/p^r\mathbb{Z}$ be a constant group scheme over F, $F_r=F(\xi_{p^r})$ be a field extension of F and $\Gamma_r=Gal(F_r/F)$ be the corresponding Galois group. Then let $T_r=R_{F_r/F}(\mathbb{G}_m)$ be the corestriction of the multiplicative group $\mathbb{G}_m$ from F_r to F.

For any $\gamma\in\Gamma_r$, $\gamma(\xi_{p^r})=\xi_{p^r}^{\chi_r(\gamma)}$ for some $\chi_r(\gamma)\in(\mathbb{Z}/p^r\mathbb{Z})^\times$. Then χ_r is a Γ-homomorphism $\chi_r:\Gamma_r\to(\mathbb{Z}/p^r\mathbb{Z})^\times$. It extends linearly to a surjective Γ-homomorphism $f_r:(T_{r,sep})^*=\mathbb{Z}[\Gamma_r]\to\mathbb{Z}/p^r\mathbb{Z}=(G_{r,sep})^*$,

$$f_r(\sum a_\gamma\gamma)=\sum a_\gamma\chi_r(\gamma)\ (\mathrm{mod}\ p^r).$$

Fix a positive integer n. Let $s=\min\{n,\ \sup\{m\in\mathbb{N}|\ \xi_{p^m}\in F\}\}$. Define a surjective Γ-homomorphism $g:\mathbb{Z}[\Gamma_{n-s}]\oplus\mathbb{Z}[\Gamma_n]\to\mathbb{Z}/p^n\mathbb{Z}$ by

$$g(x,y)=p^s\cdot f_{n-s}(x)+f_n(y)$$

for every $(x,y)\in\mathbb{Z}[\Gamma_{n-s}]\oplus\mathbb{Z}[\Gamma_n]$. Let V be the factor group scheme

$$V=(T_{n-s}\times T_n)/G_n$$

with $(V_{sep})^*=\ker(g)$, so we have an exact sequence of group schemes

$$1\longrightarrow G_n\longrightarrow T_{n-s}\times T_n\longrightarrow V\longrightarrow 1.$$

For every $K\in Fields/F$, passing to cohomology and applying Hilbert's Theorem 90 give

$$V(K)\longrightarrow H^1(K,G_n)\longrightarrow H^1(K,T_{n-s}\times T_n)=1.$$

Consider the composition

$$V(K)\twoheadrightarrow H^1(K,G_n)\longrightarrow H^1(K,G_{n-s}), \tag{1}$$

where the latter homomorphism is induced by the exact sequence

$$1\longrightarrow G_s\longrightarrow G_n\longrightarrow G_{n-s}\longrightarrow 1.$$

Let $\mathfrak{F}(K)$ be the image of $V(K)$ in $H^1(K,G_{n-s})$, which is the same as the image of $H^1(K,G_n)$. Then we get a subfunctor $\mathfrak{F}$ of $H^1(-,G_{n-s})$. The main result of this section is the following

Proposition 2.1. *There exists a closed subscheme $Y\subseteq V$ of dimension $[F_n:F]-1$ such that for every infinite $K\in Fields/F$, the image of $Y(K)$ in $H^1(K,G_{n-s})$ is equal to $\mathfrak{F}(K)$.*

Proof. If $n = s$, the result follows immediately from $H^1(K, G_{n-s}) = 1$ and $[F_n : F] = 1$.

If $n > s$, first we want to show that (1) is part of a commutative diagram. Consider the following commutative diagram of Γ-modules

$$\begin{array}{ccccc} \mathbb{Z}/p^s\mathbb{Z} & \xleftarrow{\pi} & \mathbb{Z}/p^n\mathbb{Z} & \xleftarrow{p^s} & \mathbb{Z}/p^{n-s}\mathbb{Z} \\ \uparrow{\scriptstyle \pi\circ f_n} & & \uparrow{\scriptstyle g} & & \uparrow{\scriptstyle f_{n-s}} \\ \mathbb{Z}[\Gamma_n] & \xleftarrow{\varpi} & \mathbb{Z}[\Gamma_{n-s}] \oplus \mathbb{Z}[\Gamma_n] & \xleftarrow{i} & \mathbb{Z}[\Gamma_{n-s}] \\ \uparrow & & \uparrow & & \uparrow \\ \ker(\pi \circ f_n) & \xleftarrow{\varpi} & \ker(g) & \xleftarrow{i} & \ker(f_{n-s}) \end{array} \tag{2}$$

where π is the canonical projection, i is the canonical inclusion $i(x) = (x, 0)$, ϖ is the canonical projection $\varpi(x, y) = y$ for every $x \in \mathbb{Z}[\Gamma_{n-s}], y \in \mathbb{Z}[\Gamma_n]$. Note the all the rows and columns in (2) are short exact sequences. Let $U = T_n/G_s$ with $(U_{sep})^* = \ker(\pi \circ f_n)$, and $S = T_{n-s}/G_{n-s}$ with $(S_{sep})^* = \ker(f_{n-s})$. The commutative diagram of group schemes dual to (2) is

$$\begin{array}{ccccc} G_s & \longrightarrow & G_n & \longrightarrow & G_{n-s} \\ \downarrow & & \downarrow & & \downarrow \\ T_n & \longrightarrow & T_{n-s} \times T_n & \longrightarrow & T_{n-s} \\ \downarrow & & \downarrow & & \downarrow \\ U & \longrightarrow & V & \longrightarrow & S \end{array}$$

which gives the following commutative diagram

$$\begin{array}{ccc} T_{n-s}(K) \times T_n(K) & \longrightarrow & T_{n-s}(K) \\ \downarrow & & \downarrow \\ V(K) & \longrightarrow & S(K) \\ \downarrow & & \downarrow \\ H^1(K, G_n) & \longrightarrow & H^1(K, G_{n-s}) \end{array} \tag{3}$$

for every $K \in Fields/F$.

In order to construct Y, we consider

$$\begin{array}{ccc} \mathbb{Z}[\Gamma_{n-s}] \oplus \mathbb{Z} & \xleftarrow{j} & \mathbb{Z}[\Gamma_{n-s}] \\ \uparrow{\scriptstyle \varphi} & & \uparrow \\ \ker(g) & \xleftarrow{i} & \ker(f_{n-s}) \end{array} \tag{4}$$

where j is the inclusion $j(x) = (x, 0)$, φ is defined by $\varphi(x, y) = (x, \epsilon(y)/p^s)$ for every $(x, y) \in \ker(g) \subseteq \mathbb{Z}[\Gamma_{n-s}] \oplus \mathbb{Z}[\Gamma_n]$, where ϵ is the augmentation map of a group ring.

Lemma 2.2. *$\varphi : \ker(g) \to \mathbb{Z}[\Gamma_{n-s}] \oplus \mathbb{Z}$ is well-defined and surjective.*

Proof. Let (x, y) be any element in $\ker(g)$.

(1) For $p \neq 2$, and for $p = 2$ and $s \geq 2$, Γ_n is a cyclic group. Let σ be the generator of Γ_n such that $\sigma(\xi_{p^n}) = \xi_{p^n}^{p^s+1}$. Then we can write $y = \sum a_m \sigma^m$, and $f_n(y) = \sum a_m (p^s+1)^m \pmod{p^n}$. Since $(x, y) \in \ker(g)$, $p^s \cdot f_{n-s}(x) + \sum a_m (p^s+1)^m = 0 \pmod{p^n}$. Therefore p^s divides $\sum a_m$.
(2) For $p = 2$ and $s = 1$, write $y = \sum a_\gamma \gamma$. Since $(x, y) \in \ker(g)$, $2f_{n-1}(x) + \sum a_\gamma \chi_n(\gamma) = 0 \pmod 2$. Note that $\chi_n(\gamma) \in (\mathbb{Z}/2^n\mathbb{Z})^\times$ for every γ, in particular $\chi_n(\gamma)$ is odd. Hence $\sum a_\gamma$ is even.

Therefore φ is well-defined.

Claim: If $\epsilon/p^s : \ker(f_n) \to \mathbb{Z}$ is surjective, then φ is surjective.

To prove the claim let (x, m) be any element in $\mathbb{Z}[\Gamma_{n-s}] \oplus \mathbb{Z}$. Recall that $f_n : \mathbb{Z}[\Gamma_n] \to \mathbb{Z}/p^n\mathbb{Z}$ is surjective. There exists $y \in \mathbb{Z}[\Gamma_n]$ such that $f_n(y) = -p^s \cdot f_{n-1}(x)$, which implies $(x, y) \in \ker(g)$. Let $m' = \epsilon(y)/p^s$. Note that for every $y' \in \ker(f_n)$, $(0, y') \in \ker(g)$. If $\epsilon/p^s : \ker(f_n) \to \mathbb{Z}$ is surjective, let $y' \in \ker(f_n)$ such that $\epsilon(y')/p^s = 1$. Then $(x, y+(m-m')y') \in \ker(g)$ and $\varphi(x, y+(m-m')y') = (x, m)$, proving the claim. It remains to show that $\epsilon/p^s : \ker(f_n) \to \mathbb{Z}$ is surjective.

(1) For $p \neq 2$, and for $p = 2$ and $s \geq 2$, simply note that $\sigma - p^s - 1 \in \ker(f_n)$.
(2) For $p = 2$ and $s = 1$, consider $Im(\chi_n) \subseteq (\mathbb{Z}/2^n\mathbb{Z})^\times$. Note that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is a direct product of two cyclic subgroups generated by 5 and -1 respectively. We claim that $-5^r \in Im(\chi_n)$ for some integer r. Suppose not, then all elements of $Im(\chi_n)$ are powers of 5, which implies Γ_n fixes $\xi_4 = \xi_{2^n}^{2^{n-2}}$ and contradicts the fact that $\xi_4 \notin F$. Let $\gamma \in \Gamma_n$ such that $\chi_n(\gamma) = -5^r$. Since $\gamma + 5^r$ and $2^n \in \ker(f_n)$, $(1+5^r)/2$ and $2^{n-1} \in Im(\epsilon/2)$. As $5^r = 1 \pmod 4$, $(1+5^r)/2$ is odd. Hence $(1+5^r)/2$ and 2^{n-1} are coprime and $Im(\epsilon/2) = \mathbb{Z}$. □

It is clear that the diagram (4) is commutative, so we have the dual commutative digram of group schemes

(5)
$$\begin{array}{ccc} T_{n-s} \times \mathbb{G}_m & \longrightarrow & T_{n-s} \\ \downarrow & & \downarrow \\ V & \longrightarrow & S \\ \downarrow \pi & & \\ V' & & \end{array}$$

where $V' = V/(T_{n-s} \times \mathbb{G}_m)$.

Let $E = F(V')$ be the function field of V'. From the exact sequence of cohomology

$$V(E) \longrightarrow V'(E) \longrightarrow H^1(E, T_{n-s} \times \mathbb{G}_m) = 1,$$

the generic point of V', Spec $(E) \to V'$ factors through V. Therefore there exists a rational map $\alpha : V' \to V$ such that the composition with the projection π is the identity map on the largest open set U which α is defined. Let $Y = \overline{Im(\alpha)}$. Clearly $\dim Y = \dim V' = \dim V - \dim(T_{n-s} \times \mathbb{G}_m) = [F_n : F] - 1$. It remains to check that the images of $Y(K)$ and $V(K)$ in $H^1(K, G_{n-s})$ are equal.

Lemma 2.3. *For every $v \in V(K)$, there exists $u \in Y(K)$ such that the images of v and u in $H^1(K, G_{n-s})$ are equal.*

Proof. Since $T_{n-s} \times T_n$ is a quasi-split torus, it is an open subset of an affine space. Therefore $T_{n-s}(K) \times T_n(K)$, viewed as the set of K-rational points, is a dense subset of $T_{n-s} \times T_n$ because K is infinite. Then the image of $T_{n-s}(K) \times T_n(K)$ in $V(K)$ is dense, and $V'(K)$ is dense in V'. As U is open in V', $U(K) = U \cap V'(K) \neq \emptyset$. We can find some v' in the image of $T_{n-s}(K) \times T_n(K)$ such that $\pi(v \cdot v') \in U(K)$. By (3) v and $v \cdot v'$ have the same image in $H^1(K, G_n)$. Therefore by replacing v by $v \cdot v'$ we may assume $\pi(v) \in U(K)$.

Let $u = \alpha \circ \pi(v) \in Y(K)$. As $\pi(u) = \pi(v)$, by (5) u and v differ by an element in $T_{n-s}(K) \times \mathbb{G}_m(K)$. Then by commutativity of (5) the images of u and v in $S(K)$ differ by the image of an element in $T_{n-s}(K)$. Hence by (3) u and v have the same image in $H^1(K, G_{n-s})$. □

This completes the proof of the proposition. □

Corollary 2.4. $\mathrm{ed}(\mathfrak{F}) \leq \mathrm{ed}(\mathbb{Z}/p^n\mathbb{Z}) - 1$.

Proof. First we show that $\mathrm{ed}(\mathfrak{F}) \leq \mathrm{ed}(Y)$. Let $K \in Fields/F$ and $a \in \mathfrak{F}(K)$. If K is a finite field, then $tr.deg_F(K) = 0$ and $\mathrm{ed}(a) = 0 \leq \mathrm{ed}(Y)$. If K is infinite, by Prop. 2.1 $Y(K) \longrightarrow \mathfrak{F}(K)$ is a surjection. Then $\mathrm{ed}(a) \leq \mathrm{ed}(Y)$ by the proof of [1] Lemma 1.9.

By [1] Prop. 1.17 and [5] Cor. 5.2, we have

$$\mathrm{ed}(\mathfrak{F}) \leq \mathrm{ed}(Y) = \dim(Y) = [F_n : F] - 1 = \mathrm{ed}(\mathbb{Z}/p^n\mathbb{Z}) - 1. \qquad \square$$

3. Main Theorem

Theorem 3.1. *Let $p_1, \ldots, p_r$ be distinct prime numbers, $n_1, \ldots, n_r$ be positive integers. Let F be a field such that $char(F) \neq p_i$ and $\xi_{p_i} \in F$ for every i. Then*

$$\begin{aligned} \mathrm{ed}(\mathbb{Z}/p_1^{n_1} \cdots p_r^{n_r}\mathbb{Z}) &\leq \mathrm{ed}(\mathbb{Z}/p_1^{n_1}\mathbb{Z}) + \cdots + \mathrm{ed}(\mathbb{Z}/p_r^{n_r}\mathbb{Z}) - r + 1 \\ &= [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_r^{n_r}}) : F] - r + 1. \end{aligned}$$

Proof. Let $s_i = \min\{n_i,\ \sup\{m \in \mathbb{N} |\ \xi_{p_i^m} \in F\}\}$ for every i. For each prime number p_i, let $\mathfrak{F}_i$ be the corresponding $\mathfrak{F}$ defined above. Let $C_N = \mathbb{Z}/p_1^{n_1} \cdots p_r^{n_r}\mathbb{Z}$ be a constant group scheme over F, $C_S = \mathbb{Z}/p_1^{s_1} \cdots p_r^{s_r}\mathbb{Z}$ and $C_{N-S} = \mathbb{Z}/p_1^{n_1-s_1} \cdots p_r^{n_r-s_r}\mathbb{Z}$. The exact sequence of group schemes

$$1 \longrightarrow C_S \longrightarrow C_N \longrightarrow C_{N-S} \longrightarrow 1$$

induces an exact sequence

$$\cdots \longrightarrow H^1(K, C_S) \longrightarrow H^1(K, C_N) \longrightarrow H^1(K, C_{N-S}) \longrightarrow \cdots \tag{6}$$

for every $K \in Fields/F$. Note that

$$H^1(K, C_N) = H^1(K, \mathbb{Z}/p_1^{n_1}\mathbb{Z}) \times \cdots \times H^1(K, \mathbb{Z}/p_r^{n_r}\mathbb{Z}),$$

and similarly

$$H^1(K, C_{N-S}) = H^1(K, \mathbb{Z}/p_1^{n_1-s_1}\mathbb{Z}) \times \cdots \times H^1(K, \mathbb{Z}/p_r^{n_r-s_r}\mathbb{Z}).$$

Then the exact sequence (6) implies that we have a fibration of functors ([1] Def. 1.12)

$$H^1(-, C_S) \longrightarrow H^1(-, C_N) \twoheadrightarrow \mathfrak{F}_1 \times \cdots \times \mathfrak{F}_r.$$

By Cor. 2.4, [1] Lemma 1.11 and Prop. 1.13, and [5] Cor. 5.2,

$$\begin{aligned}\mathrm{ed}(C_N) &\leq \mathrm{ed}(C_S) + \mathrm{ed}(\mathfrak{F}_1 \times \cdots \times \mathfrak{F}_r)\\ &\leq 1 + \mathrm{ed}(\mathfrak{F}_1) + \cdots + \mathrm{ed}(\mathfrak{F}_r)\\ &\leq 1 + (\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\mathbb{Z}) - 1) + \cdots + (\mathrm{ed}(\mathbb{Z}/p_r^{n_r}\mathbb{Z}) - 1)\\ &= \mathrm{ed}(\mathbb{Z}/p_1^{n_1}\mathbb{Z}) + \cdots + \mathrm{ed}(\mathbb{Z}/p_r^{n_r}\mathbb{Z}) - r + 1\\ &= [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_r^{n_r}}) : F] - r + 1,\end{aligned}$$

where $\mathrm{ed}(C_S) = 1$ as $\xi_{p_1^{s_1}\cdots p_r^{s_r}} \in F$. □

Example 3.2. If $s_i = n_i$ for $2 \leq i \leq r$, then $\xi_{p_r^{n_r}} \in F$ for $2 \leq i \leq r$. Thm. 3.1 implies

$$\begin{aligned}\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z}) &\leq [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_r^{n_r}}) : F] - r + 1\\ &= [F(\xi_{p_1^{n_1}}) : F]\\ &= \mathrm{ed}(\mathbb{Z}/p_1^{n_1}\mathbb{Z}).\end{aligned}$$

On the other hand,

$$H^1(-, \mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z}) = H^1(-, \mathbb{Z}/p_1^{n_1}\mathbb{Z}) \times \cdots \times H^1(-, \mathbb{Z}/p_r^{n_r}\mathbb{Z}).$$

By [1] Remark 1.16 $\max\{\mathrm{ed}(\mathbb{Z}/p_i^{n_i})\} \leq \mathrm{ed}(\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z})$ where the maximum is taken over $1 \leq i \leq r$. Therefore

$$\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z}) = \mathrm{ed}(\mathbb{Z}/p_1^{n_1}\mathbb{Z}).$$

Remark 3.3. Let $m = p_1^{n_1}\cdots p_r^{n_r}$, and $G = \mathbb{Z}/m\mathbb{Z}$. If V is a faithful linear representation of G over F then $\mathrm{ed}(G) \leq \dim(V)$ ([1] Prop. 4.15). We want to compare the least dimension of a faithful representation of G over F with the upper bound of $\mathrm{ed}(G)$ given by Thm. 3.1.

Let $n_i > s_i$ for $1 \leq i \leq a$, and $n_i = s_i$ for $a < i \leq r$ for some integer $1 \leq a \leq r$. By Maschke's Theorem ([7] Ch. XVIII Thm. 1.2), $F[G]$ is semisimple. Since $F[G]$ is a commutative ring, $F[G] \cong F[t]/\langle t^m - 1\rangle$ is isomorphic to a product of fields $E_1 \times \ldots \times E_k$. For every divisor d of m, there exists a surjection $F[t]/\langle t^m - 1\rangle \twoheadrightarrow F(\xi_d)$, $t \longmapsto \xi_d$. Therefore $F(\xi_d) \cong E_i$ for some i. On the other hand, for every E_j clearly there exists a surjection $F[t]/\langle t^m - 1\rangle \twoheadrightarrow E_j$. Let ξ be the image of t under this surjection. Then $E_j = F[\xi] = F(\xi)$, and $\xi^m = 1$. Hence $E_j \cong F(\xi_d)$ for some divisor d of m. Therefore $F[G]$ is isomorphic to a product of $F(\xi_d), d|m$. Note that there can be more than one copy of a particular $F(\xi_d)$ in the product.

For every divisor d of m, the kernel of the natural representation $G \to \mathbf{GL}(F(\xi_d))$, $1 \longmapsto \xi_d$, is the subgroup $\langle d\rangle$. Then the kernel of the natural representation $G \longrightarrow \mathbf{GL}(\coprod F(\xi_{d_j}))$ is $\bigcap\langle d_j\rangle = \langle \mathrm{lcm}\{d_j\}\rangle$, where d_j divides m for every j. By choosing d_j to be $p_1^{n_1}, \ldots, p_{a-1}^{n_{a-1}}, p_a^{n_a}\cdots p_r^{n_r}$, we can see that the natural representation of G in the F-space $V = F(\xi_{p_1^{n_1}}) \oplus \cdots \oplus F(\xi_{p_a^{n_a}})$ is a faithful representation of the least dimension, as $F(\xi_{p_a^{n_a}}) = F(\xi_{p_a^{n_a}\cdots p_r^{n_r}})$. We have

$$\begin{aligned}\dim V &= [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_a^{n_a}}) : F]\\ &\geq [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_r^{n_r}}) : F] - r + 1\end{aligned}$$

where equality holds if and only if $a = 1$ (see Example 3.2). In particular, if $a \geq 2$, then $\mathrm{ed}(G) < \dim(V)$. This is different from the case for p-groups, where the

essential dimension of a p-group G' is equal to the least dimension of a faithful representation of G' over F (see [5] Thm. 4.1).

4. A conjecture for $\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z})$

4.1. **Canonical dimension.** Let F be a field and $\mathfrak{C}$ be a class of field extensions of F. A field $E \in \mathfrak{C}$ is called generic if for any $K \in \mathfrak{C}$ there exists an F-place of E with values in K. The canonical dimension of the class $\mathfrak{C}$ is

$$\mathrm{cdim}(\mathfrak{C}) = \min\{tr.deg_F E\}$$

where the minimum is taken over all generic fields $E \in \mathfrak{C}$.

Example 4.1. If X is a separated scheme of finite type over F, let $\mathfrak{C}_X$ be the class of field extensions K of F such that $X(K) \neq \emptyset$. The canonical dimension of X is defined as $\mathrm{cdim}(X) = \mathrm{cdim}(\mathfrak{C}_X)$. It can be shown that $\mathrm{cdim}(X) \leq \dim(X)$ (see [3] and [8]).

Example 4.2. If θ is an element of $Br(F)$ the Brauer group of F, let $\mathfrak{C}_\theta$ be the class of splitting fields of θ. The canonical dimension of θ is defined as $\mathrm{cdim}(\theta) = \mathrm{cdim}(\mathfrak{C}_\theta)$.

Similarly, if D is a finite subgroup of $Br(F)$, let $\mathfrak{C}_D$ be the class of common splitting fields of all elements in D. The canonical dimension of D is defined as $\mathrm{cdim}(D) = \mathrm{cdim}(\mathfrak{C}_D)$.

Let $\theta \in Br(F)$ be represented by a central simple F-algebra A. Let $SB(A)$ be the Severi-Brauer variety of A. $K \in Fields/F$ splits A if and only if $SB(A)(K) \neq \emptyset$ ([6] Prop. 1.17). Therefore $\mathrm{cdim}(\theta) = \mathrm{cdim}(SB(A))$.

Conjecture 4.3. Let A be a central division F-algebra of degree $q_1^{a_1}\cdots q_k^{a_k}$, where q_i are distinct prime numbers, a_i are non-negative integers. Write A as a tensor product $A_i \otimes \cdots \otimes A_k$ where A_i is a central division F-algebra of degree $q_i^{a_i}$. Let $X = SB(A)$ be the Severi-Brauer variety of A, and let $Y = SB(A_1)\times\cdots\times SB(A_k)$. $K \in Fields/F$ splits A if and only if it splits A_i for every i, therefore $X(K) \neq \emptyset$ if and only if $Y(K) \neq \emptyset$. Hence

$$\mathrm{cdim}(SB(A)) = \mathrm{cdim}(Y) \leq \dim(Y) = q_1^{a_1} + \cdots + q_k^{a_k} - k. \tag{7}$$

It is conjectured in [3] that the inequality in (7) is actually an equality.

4.2. **Algebras and Representations.** Let G be a finite group, C be a central subgroup of G and set $H = G/C$. Then we have an exact sequence

$$1 \longrightarrow C \longrightarrow G \longrightarrow H \longrightarrow 1. \tag{8}$$

Let $E \to Spec(L)$ be a generic H-torsor, $L \in Fields/F$ (see [1] section 6, [5] section 4). Let C^* denote the character group $Hom(C, \mathbb{G}_m)$ of C. Define a homomorphism $\beta^E : C^* \to Br(L)$ by taking $\chi : C \to \mathbb{G}_m$ to the image of the class of E under the composition

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

where ∂ is the connecting homomorphism for the exact sequence (8).

Let $\chi : C \to \mathbb{G}_m$ be a character, $Rep^{(\chi)}(G)$ be the category of all finite dimensional representations ρ of G such that $\rho(c)$ is multiplication of $\chi(c)$ for any $c \in C$. It is proved in [5] Thm. 4.4 that

$$\mathrm{ind}(\beta^E(\chi)) = \gcd \dim(V)$$

over all representations $V \in Rep^{(\chi)}(G)$.

4.3. **Gerbes.** Let $\mathcal{X}$ be a gerbe over F (see [8] section 3, [9] p. 144). Define a functor $\overline{\mathcal{X}} : Fields/F \to Sets$ by mapping K to the set of isomorphism classes of objects in the category $\mathcal{X}(K)$. The essential dimension of $\mathcal{X}$ is defined as $\mathrm{ed}(\mathcal{X}) = \mathrm{ed}(\overline{\mathcal{X}})$. Let $\mathfrak{C}_{\mathcal{X}}$ be the class of field extensions K of F such that $\overline{\mathcal{X}}(K) \neq \emptyset$. Then the canonical dimension of $\mathcal{X}$ is defined as $\mathrm{cdim}(\mathcal{X}) = \mathrm{cdim}(\mathfrak{C}_{\mathcal{X}})$.

4.4. **A conjecture for** $\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z})$**.**

Theorem 4.4. *Let $p_1, \ldots, p_r$ be distinct prime numbers, $n_1, \ldots, n_r$ be positive integers. Let F be a field such that $char(F) \neq p_i$ and $\xi_{p_i} \in F$ for every i. If Conjecture 4.3 is valid, then*

$$\begin{aligned}\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z}) &= \mathrm{ed}(\mathbb{Z}/p_1^{n_1}\mathbb{Z}) + \cdots + \mathrm{ed}(\mathbb{Z}/p_r^{n_r}\mathbb{Z}) - r + 1\\ &= [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_r^{n_r}}) : F] - r + 1.\end{aligned}$$

Proof. By Thm. 3.1 we only need to prove

$$\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z}) \geq [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_r^{n_r}}) : F] - r + 1$$

when Conjecture 4.3 is valid.

Let $m = p_1^{n_1}\cdots p_r^{n_r}$, $G = \mathbb{Z}/m\mathbb{Z}$, $C = \mathbb{Z}/p_1\cdots p_r\mathbb{Z}$ be a subgroup of G, and set $H = G/C$. Let $E \to Spec(L)$ be a generic H-torsor, $L \in Fields/F$. Recall that we have a homomorphism $\beta^E : C^* \to Br(L)$.

Consider the gerbe E/G banded by C. Since $\xi_{p_i} \in F$ for every i and $L \in Fields/F$, $C \cong \mu_{p_1\cdots p_r}$ and $H^2(L, C) \cong Br_{p_1\cdots p_r}(L)$. Then the element in $H^2(L, C)$ corresponding to E/G can be represented by a central division L-algebra A with $[A] \in Br_{p_1\cdots p_r}(L)$. Note that $Im(\beta^E)$ is generated by the class of A. It follows that

$$\mathrm{cdim}_L(E/G) = \mathrm{cdim}_L(Im(\beta^E)).$$

By [5] Thm. 4.2 and [2] Thm. 7.1, we have

$$\mathrm{ed}(G) \geq \mathrm{ed}_L(G) \geq \mathrm{ed}_L(E/G) = \mathrm{cdim}_L(E/G) + 1 = \mathrm{cdim}_L(Im(\beta^E)) + 1. \tag{9}$$

Let $\chi : C \to \mathbb{G}_m$ be the character such that $\beta^E(\chi) = [A]$, and

$$a = \mathrm{ind}(\beta^E(\chi)) = \gcd \dim(V)$$

over all $V \in Rep^{(\chi)}(G)$. For every $V \in Rep^{(\chi)}(G)$, by the calculation in Remark 3.3 $V = \coprod F(\xi_{d_j})$, d_j divides m for every j. For every $c \in C$, c acts on V by multiplication of $\chi(c)$. Therefore $\xi_{d_j}^{p_1^{n_1-1}\cdots p_r^{n_r-1}}$ is a primitive $p_1\cdots p_r$-root of unity. Combining with the fact that d_j divides m, we have $d_j = m$ for every j, which implies

$$a = [F(\xi_m) : F] = \prod [F(\xi_{p_i^{n_i}}) : F],$$

where the second equality follows from the fact that $\xi_{p_i} \in F$, $[F(\xi_{p_i^{n_i}}) : F]$ is a power of p_i for every i.

If Conjecture 4.3 is valid,

$$\begin{aligned}\mathrm{cdim}_L(Im(\beta^E)) = \mathrm{cdim}_L(\beta^E(\chi)) &= \mathrm{cdim}(SB(A))\\ &= [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_r^{n_r}}) : F] - r.\end{aligned}$$

By combining the above inequality with (9), we have

$$\mathrm{ed}(G) \geq \mathrm{cdim}_L(Im(\beta^E)) + 1 \geq [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_r^{n_r}}) : F] - r + 1. \quad \square$$

Example 4.5. Let $\xi_2, \xi_3 \in F$ but $\xi_4, \xi_9 \notin F$. Consider $\mathrm{ed}(\mathbb{Z}/36\mathbb{Z}) = \mathrm{ed}(\mathbb{Z}/2^2 3^2\mathbb{Z})$. In this case $\mathrm{ind}(\beta^E(\chi)) = 6$, and Conjecture 4.3 is proven when A is of degree 6 by [3] Thm. 1.3. Therefore $\mathrm{ed}(\mathbb{Z}/36\mathbb{Z}) = 4$ (see [2] Remark 14.2).

References

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

[2] P. Brosnan, Z. Reichstein, and A. Vistoli. Essential dimension and algebraic stacks. arXiv:math/0701903v1 [math.AG], 2007.

[3] J.-L. Colliot-Thélène, N. A. Karpenko, and A. S. Merkurjev. Rational surfaces and canonical dimension of pgl6. *Algebra i Analiz*, 19(5):159–178, 2007. Translation in St. Petersburg Math. J. 19 (2008), no. 5, 793-804.

[4] M. Florence. On the essential dimension of cyclic p-groups. *Inventiones Mathematicae*, 171:175–189, 2008.

[5] N. A. Karpenko and A. S. Merkurjev. Essential dimension of finite p-groups. *Inventiones Mathematicae*, 172(3):491–508, 2008.

[6] M.-A. Knus, A. S. Merkurjev, M. Rost, and J.-P. Tignol. *The Book of Involutions*, volume 44 of *Colloquium Publications*. American Mathematical Society, Providence, RI, 1998.

[7] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, revised 3rd edition, 2002.

[8] A. S. Merkurjev. Essential dimension. In *Quadratic Forms - Algebra, Arithmetic, and Geometry*, volume 493 of *Contemporary Mathematics*, pages 299–325. American Mathematical Society, Providence, RI, 2009.

[9] J. S. Milne. *Etale Cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, New Jersey, 1980.

[10] W. C. Waterhouse. *Introduction to Affine Group Schemes*, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.

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

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