A CENTRAL EXTENSION THEOREM FOR ESSENTIAL DIMENSIONS

MING-CHANG KANG

(Communicated by Martin Lorenz)

ABSTRACT. Let K be an arbitrary field and G a finite group. We will denote by $\text{ed}_K(G)$ the essential dimension of G over K . A generalization of the central extension theorem of Buhler and Reichstein (Compositio Math. **106** (1997) 159–179, Theorem 5.3) is obtained.

1. INTRODUCTION

Let G be a finite group and K any field (it is unnecessary to assume that K is algebraically closed or $\text{char } K = 0$). The notion of the essential dimension of G over K , denoted by $\text{ed}_K(G)$, was introduced by Buhler and Reichstein in [BR] when $\text{char } K = 0$. This concept was generalized for an arbitrary field K in [BF] and [JLY]. A central extension theorem was proved by Buhler and Reichstein when $\text{char } K = 0$ [BR, Theorem 5.3]. The purpose of this article is to generalize it to the case of an arbitrary field, i.e.,

Theorem 1.1. *Let p be a prime number and G a finite group. Assume that the following four properties are valid:*

- (i) *K is a field satisfying that either $\text{char } K = 0$ or $\text{char } K = l > 0$ such that G contains no non-trivial normal l -subgroup,*
- (ii) *there is an element $\sigma \in Z(G) \subset G$ with $\text{ord}(\sigma) = p$,*
- (iii) *there is a linear character $\chi : G \rightarrow K^\times$ with $\chi(\sigma) \neq 1$,*
- (iv) *for any $\tau \in Z(G)$ with $\text{ord}(\tau) = m$, it is necessary that $\zeta_m \notin K$ if $\langle \sigma \rangle$ is a proper subgroup of $\langle \tau \rangle$.*

Then $\text{ed}_K(G) = \text{ed}_K(G/\langle \sigma \rangle) + 1$.

Note that $Z(G)$ denotes the center of the group G . We will consider also a split version of the above theorem.

Theorem 1.2. *Let p be a prime number and $G = G' \times \langle \sigma \rangle$ be a finite group. Assume that the following four properties are valid:*

- (i) *K is a field satisfying that either $\text{char } K = 0$ or $\text{char } K = l > 0$ such that G contains no non-trivial normal l -subgroup,*
- (ii) *$\text{ord}(\sigma) = p$,*
- (iii) *$\zeta_p \in K$,*

Received by the editors November 28, 2006.

2000 *Mathematics Subject Classification.* Primary 12E05, 12F10, 12F20, 13F30.

Key words and phrases. Essential dimension, Galois theory, group actions, valuation rings.

©2007 American Mathematical Society
 Reverts to public domain 28 years from publication

(iv) for any prime factor p' of $|Z(G')|$ such that $p' \neq p$, it is necessary that $\zeta_{p'} \notin K$.

Then $\text{ed}_K(G) = \text{ed}_K(G') + 1$.

We remark that in Theorem 1.1(ii), since $\chi(\sigma) \neq 1$ and $\text{ord}(\sigma) = p$, it follows that $\chi(\sigma)$ is a primitive p -th root of unity. In particular, $\zeta_p \in K$ and $\text{char } K \nmid p$.

By Theorems 1.1 and 1.2, it is not difficult to prove the following result: If p is a prime number and K is a field such that $\zeta_p \in K$, then $\text{ed}_K((\mathbb{Z}/p\mathbb{Z})^r) = r$. In particular, for a field K with $\text{char } K \neq 2$, $\text{ed}_K((\mathbb{Z}/2\mathbb{Z})^r) = r$. Note that this result was proved by Berhuy and Favi in [BF, Corollary 4.16] using a cohomological method.

Standing notation and terminology. . For emphasis, K is an arbitrary field. All the fields in this article are assumed to contain the ground field K . If E is a field extension of K , $\text{trdeg}_K E$ denotes the transcendence degree of E over K . The order of an element σ in a group G is denoted by $\text{ord}(\sigma)$. When we say that $G \rightarrow GL(V)$ is a representation of a finite group G , it is understood that V is a finite-dimensional vector space over K .

We will take the convention that $\text{char } K \nmid n$ means either $\text{char } K = 0$ or $\text{char } K = p > 0$ with $p \nmid n$. Finally ζ_n denotes a primitive n -th root of unity; whenever we write $\zeta_n \in K$, it is assumed tacitly that $\text{char } K \nmid n$.

2. PRELIMINARIES

Let K be an arbitrary field.

Definition 2.1. Let L be a field containing K and G a finite group. L is called a G -field over K if there is a group homomorphism $G \rightarrow \text{Aut}_K(L)$, i.e. G acts on L by K -automorphisms; since the ground field K is understood, we simply call it a G -field. A G -field L is called a faithful G -field if the group homomorphism $G \rightarrow \text{Aut}_K(L)$ is faithful.

Definition 2.2. Let G be a finite group. Define $\text{ed}_K(G) = \min \{\text{trdeg}_K E : E \text{ is a faithful } G\text{-subfield of } K(V)\}$ where $G \rightarrow GL(V)$ is a faithful representation of G and $K(V)$ is the function field of the affine space V over K . (Explicitly, if $x_1, \dots, x_n$ is a basis of the dual space of V , then $K(V) = K(x_1, \dots, x_n)$ is the rational function field of n variables over K .) Note that $\text{ed}_K(G)$ is independent of the choice of the faithful representation $G \rightarrow GL(V)$.

Lemma 2.3. Let R be a rank-one discrete valuation ring (DVR) containing a field K , and let $\mathfrak{M}$ be the maximal ideal of R . If $\sigma \in \text{Aut}_K(R)$ satisfies that (i) $1 < \text{ord}(\sigma) < \infty$ and (ii) the induced automorphisms of σ on $R/\mathfrak{M}$ and $\mathfrak{M}/\mathfrak{M}^2$ are the identity maps, then $\text{char } K = l > 0$ and $\text{ord}(\sigma) = l^r$ for some positive integer r .

Proof. Let $n = \text{ord}(\sigma)$. If $\text{char } K = 0$, define an integer m by $m = n$. If $\text{char } K = l > 0$, define the integer m by $m = n'$ where $n = l^r \cdot n'$ with $l \nmid n'$. We will show that $m = 1$.

Suppose not. Define $\tau = \sigma^{n/m}$. Then $\tau \in \text{Aut}_K(R)$ and $\text{ord}(\tau) = m > 1$. Choose $x \in R$ such that $\tau(x) \neq x$ and define $y = \tau(x) - x \neq 0$.

Since the induced actions of σ on $R/\mathfrak{M}$ and $\mathfrak{M}/\mathfrak{M}^2$ are the identity maps, it is not difficult to show that, for any $r = 0, 1, 2, \dots$, for any $u \in \mathfrak{M}^r$, it is necessary that $\sigma(u) - u \in \mathfrak{M}^{r+1}$. The same is valid for τ , i.e. $\tau(u) - u \in \mathfrak{M}^{r+1}$.

In particular, if $y \in \mathfrak{M}^s \setminus \mathfrak{M}^{s+1}$, then $\tau(y) - y \in \mathfrak{M}^{s+1}$.

From $\tau(x) = x + y$, we find that $\tau^2(x) = \tau(x) + \tau(y) = x + y + y + v$, where $\tau(y) = y + v$ with $v \in \mathfrak{M}^{s+1}$. Hence $\tau^2(x) = x + 2y \pmod{\mathfrak{M}^{s+1}}$. Proceed by induction. We find that $\tau^i(x) = x + iy \pmod{\mathfrak{M}^{s+1}}$ for $1 \leq i \leq m$. Consequently, $\tau^m(x) = x + my \pmod{\mathfrak{M}^{s+1}}$.

Since $\tau^m = 1$, we find that $x = x + my \pmod{\mathfrak{M}^{s+1}}$. It follows that $my \in \mathfrak{M}^{s+1}$. Since $y \in \mathfrak{M}^s \setminus \mathfrak{M}^{s+1}$, it follows that $m \in \mathfrak{M}$. But m is invertible in K by assumption. Thus we get a contradiction. $\square$

Now let $R, \mathfrak{M}, K$ be the same as in Lemma 2.3. Suppose that $G \subset \text{Aut}_K(R)$ is a finite group. Define

$$\begin{aligned} G_0 &= \{\sigma \in G : \text{the induced automorphism of } \sigma \text{ on } R/\mathfrak{M} \text{ is the identity map}\}, \\ G_1 &= \{\sigma \in G : \text{the induced automorphisms of } \sigma \text{ on } R/\mathfrak{M} \text{ and } \mathfrak{M}/\mathfrak{M}^2 \text{ are} \\ &\quad \text{the identity maps}\}. \end{aligned}$$

Clearly, G_0 and G_1 are normal subgroups. We will prove that, under suitable conditions, $G_1 = \{1\}$ and G_0 is contained in the center of G . We will denote by $Z(G)$ the center of the group G in the rest of this paper.

Since $\mathfrak{M}$ is a principal ideal, we may write $\mathfrak{M} = \langle t \rangle$.

For any $\sigma \in G$, choose an element $\lambda_\sigma \in R$ so that $\sigma(t) = \lambda_\sigma t$ (because $\sigma(\mathfrak{M}) = \mathfrak{M}$ for any $\sigma \in G$). Denote by $\bar{\lambda}_\sigma$ the image of λ_σ in $R/\mathfrak{M}$. We record some properties of $\bar{\lambda}_\sigma$ in the following lemma.

Lemma 2.4. (1) For any $\sigma_1, \sigma_2 \in G$, $\lambda_{\sigma_1\sigma_2} = \lambda_{\sigma_1} \cdot \sigma_1(\lambda_{\sigma_2}) \pmod{\mathfrak{M}}$. In particular, $\lambda_{\tau\sigma\tau^{-1}} = \tau(\lambda_\sigma) \pmod{\mathfrak{M}}$ for any $\sigma \in G_0$, any $\tau \in G$.

(2) The map $\Phi : G_0 \rightarrow (R/\mathfrak{M})^\times$ defined by $\Phi(\sigma) = \bar{\lambda}_\sigma$ is a group homomorphism where $(R/\mathfrak{M})^\times$ is the multiplicative group of the field $R/\mathfrak{M}$.

Proof. (1) Modulo $\mathfrak{M}^2$, we have $\lambda_{\sigma_1\sigma_2}t = \sigma_1\sigma_2(t) = \sigma_1(\sigma_2(t)) = \sigma_1(\lambda_{\sigma_2}t) = \sigma_1(\lambda_{\sigma_2}) \cdot \sigma_1(t) = \sigma_1(\lambda_{\sigma_2}) \cdot \lambda_{\sigma_1}t = [\lambda_{\sigma_1} \cdot \sigma_1(\lambda_{\sigma_2})]t$. Hence the result.

Suppose that $\sigma \in G_0$ and $\tau \in G$. Modulo $\mathfrak{M}$, we have $\lambda_{\tau\sigma\tau^{-1}} = \lambda_\tau \cdot \tau(\lambda_{\sigma\tau^{-1}}) = \lambda_\tau \cdot \tau(\lambda_\sigma \cdot \sigma(\lambda_{\tau^{-1}})) = \tau(\lambda_\sigma) \cdot \lambda_\tau \cdot \tau\sigma(\lambda_{\tau^{-1}}) = \tau(\lambda_\sigma) \cdot \lambda_\tau \cdot \tau(\lambda_{\tau^{-1}})$ because σ is the identity map on $R/\mathfrak{M}$. On the other hand, note that $\lambda_1 = 1$. Thus $1 = \lambda_1 = \lambda_{\tau\tau^{-1}} = \lambda_\tau \cdot \tau(\lambda_{\tau^{-1}}) \pmod{\mathfrak{M}}$. It follows that $\lambda_{\tau\sigma\tau^{-1}} = \tau(\lambda_\sigma) \pmod{\mathfrak{M}}$.

(2) It suffices to show that, for any $\sigma_1, \sigma_2 \in G_0$, $\lambda_{\sigma_1\sigma_2} = \lambda_{\sigma_1} \cdot \lambda_{\sigma_2} \pmod{\mathfrak{M}}$. By (1), we have $\lambda_{\sigma_1\sigma_2} = \lambda_{\sigma_1} \cdot \sigma_1(\lambda_{\sigma_2}) = \lambda_{\sigma_1} \cdot \lambda_{\sigma_2} \pmod{\mathfrak{M}}$ since σ_1 is the identity map on $R/\mathfrak{M}$. $\square$

Lemma 2.5. Let R be a DVR containing a field K and let $\mathfrak{M}$ be its maximal ideal. Suppose that G is a finite subgroup of $\text{Aut}_K(R)$ and define G_0 and G_1 as above. Assume furthermore that K is algebraically closed in the field $R/\mathfrak{M}$. Then

- (i) $\tau\sigma\tau^{-1}\sigma^{-1} \in G_1$ for any $\tau \in G$, any $\sigma \in G_0$;
- (ii) G_0/G_1 is a cyclic group;
- (iii) if the order of G_0/G_1 is m , then $\zeta_m \in K$; in particular, $\text{char } K \nmid m$.

Corollary 2.6. Let the assumptions be the same as in Lemma 2.5. Assume that (i) $\text{char } K = 0$, or (ii) $\text{char } K = l > 0$ and G contains no non-trivial normal l -subgroup. Then $G_1 = \{1\}$, G_0 is a cyclic group and $G_0 \subset Z(G)$.

Proof of Corollary 2.6. Assume that Lemma 2.5 is valid.

Note that $G_1 = \{1\}$. Otherwise, $\text{char } K = l > 0$ by Lemma 2.3 and G_1 is an l -subgroup of G . Note that G_1 is normal in G . This leads to a contradiction to our assumption.

Now apply Lemma 2.5. Since $G_1 = \{1\}$, we find $\sigma\tau = \tau\sigma$ for any $\sigma \in G_0$, any $\tau \in G$. Thus $G_0 \subset Z(G)$. Again by Lemma 2.5 we know that $G_0 \simeq G_0/G_1$ is a cyclic group. $\square$

Proof of Lemma 2.5. Consider the group homomorphism $\Phi : G_0 \rightarrow (R/\mathfrak{M})^\times$ in Lemma 2.4. G_1 is just the kernel of Φ . The image of G_0 is a cyclic group, say, of order m . Let $\alpha \in R$ such that $\bar{\alpha}$ is a generator of the image of Φ .

Since $K \subset R/\mathfrak{M}$ and $\bar{\alpha} \in R/\mathfrak{M}$ is algebraic over K , it follows that $\alpha \in K$ because we assume that K is algebraically closed in $R/\mathfrak{M}$. Clearly, $\text{char } K \nmid m$ and G is a cyclic group.

It remains to show that $\tau\sigma\tau^{-1}\sigma^{-1} \in G_1$ for any $\tau \in G$, $\sigma \in G_0$. It suffices to show that $\lambda_{\tau\sigma\tau^{-1}\sigma^{-1}} = 1 \pmod{\mathfrak{M}}$.

Since $\text{Im}(\Phi) = \langle \alpha \rangle$, it follows that $\bar{\lambda}_\sigma = \alpha^i \in K$ for some i . Since $\tau\sigma\tau^{-1} \in G_0$, it follows that $\bar{\lambda}_{\tau\sigma\tau^{-1}} = \tau(\bar{\lambda}_\sigma)$ by Lemma 2.4. Thus $\tau(\bar{\lambda}_\sigma) = \tau(\alpha^i) = \alpha^i$ because G is a K -linear automorphism group. Thus $\bar{\lambda}_{\tau\sigma\tau^{-1}\sigma^{-1}} = \bar{\lambda}_{\tau\sigma\tau^{-1}} \cdot \bar{\lambda}_{\sigma^{-1}} = \alpha^i \cdot \alpha^{-i} = 1$. $\square$

3. PROOF OF THEOREMS 1.1 AND 1.2

In the situation of Theorem 1.1 write $G' = G/\langle \sigma \rangle$. In the situation of Theorem 1.2 define a linear character $\chi : G = G' \times \langle \sigma \rangle \rightarrow K^\times$ by $\chi(\tau\sigma^i) = \zeta_p^i$ for any $\tau \in G'$, any $0 \leq i \leq p-1$. Thus there is an embedding of G into $G' \times \chi(G)$ for both situations. Note that $\text{ed}_K(G) \leq \text{ed}_K(G' \times \chi(G)) \leq \text{ed}_K(G') + 1$ because $\text{ed}_K(\chi(G)) = 1$. It remains to show that $\text{ed}_K(G) \geq \text{ed}_K(G') + 1$.

Step 1. Let $G' \rightarrow GL(V)$ be a faithful representation of G' . Then G acts faithfully on $V \oplus K$ by $\tau \cdot (v + \lambda) = \tau \cdot v + \chi(\tau)\lambda$ for any $\tau \in G$, any $v \in V$, any $\lambda \in K$.

Write the function field $K(V \oplus K) = K(V)(x)$. Thus $\tau \cdot x = \chi(\tau)^{-1} \cdot x$. Hence $\tau \cdot (\frac{1}{x}) = \chi(\tau) \cdot (\frac{1}{x})$. By abusing the notation, we will write $K(V \oplus K) = K(V)(x)$ with $\tau \cdot x = \chi(\tau) \cdot x$.

Step 2. Let E be a faithful G -subfield of $K(V)(x)$ with $\text{ed}_K(G) = \text{trdeg}_K E$. We will prove that $\text{trdeg}_K E \geq \text{ed}_K(G') + 1$.

Let ν be a rank-one discrete valuation on $K(V)(x)$ determined by the prime ideal $\langle x \rangle$ in the polynomial ring $K(V)[x]$. Let O_ν be its valuation ring and $\mathfrak{M}_\nu$ its maximal ideal. Then the field $K(V)$ maps isomorphically onto the residue field of ν , i.e. $K(V) \simeq O_\nu/\mathfrak{M}_\nu$. In particular, K is algebraically closed in $O_\nu/\mathfrak{M}_\nu$.

Note that O_ν is invariant under the action of G . In fact, $K[V]$ is isomorphic to a polynomial ring and $K[V]$ is invariant under the action of G . Moreover, every element of O_ν can be written as

$$u = x^n(a_0 + a_1x + \cdots + a_rx^r)(b_0 + b_1x + \cdots + b_sx^s)^{-1},$$

where $n \geq 0$, $a_i, b_j \in K[V]$ with $a_0b_0 \neq 0$. Thus for any $\tau \in G$,

$$\begin{aligned} \tau \cdot u &= (\chi(\tau)x)^n(\tau(a_0) + \chi(\tau) \cdot \tau(a_1) \cdot x + \cdots + \chi(\tau)^r \cdot \tau(a_r) \cdot x^r) \\ &\quad \times (\tau(b_0) + \chi(\tau) \cdot \tau(b_1) \cdot x + \cdots + \chi(\tau)^s \cdot \tau(b_s) \cdot x^s)^{-1} \in O_\nu. \end{aligned}$$

Step 3. Consider the restriction of ν on the field E .

We claim that ν is non-trivial on E . Otherwise, $E \subset O_\nu$. Thus there is a G -embedding of E into $K(V)$, because $K(V)$ is isomorphic to the residue field of ν . However, the element $\sigma \in G$ acts trivially on $K(V)$ while G is faithful on E . This is a contradiction.

Let R be the valuation ring of the restriction of ν on E and $\mathfrak{M}$ be its maximal ideal. Write $\mathbb{E} = R/\mathfrak{M}$, the residue field. Since $R = E \cap O_\nu$, it follows that R is invariant under the action of G . Hence there is a natural G -embedding of $\mathbb{E}$ into $K(V)$. Note that $\text{trdeg}_K \mathbb{E} \leq \text{trdeg}_K E - 1$ by [Bo, p. 439, Corollary 1] or by [[JLY], Lemma 8.1.2, p. 187].

The action of σ on V is trivial while $G' = G/\langle\sigma\rangle$ acts faithfully on V . We will show that G' acts faithfully also on $\mathbb{E}$. Thus $\mathbb{E}$ is a faithful G' -subfield of $K(V)$. It follows that $\text{ed}_K(G') \leq \text{trdeg}_K(\mathbb{E}) \leq \text{trdeg}_K E - 1$, which will conclude our proof of Theorem 1.1 and Theorem 1.2.

Step 4. We will prove that G' acts faithfully on $\mathbb{E}$.

Define $G_0 = \{\tau \in G : \text{the induced action of } \tau \text{ on } R/\mathfrak{M} \simeq \mathbb{E} \text{ is the identity map}\}$. Clearly, $\sigma \in G_0$. Note that G' acts faithfully on $\mathbb{E}$ if and only if $G_0 = \langle\sigma\rangle$.

Since E is a faithful G -subfield, the action of G on R is faithful. Thus $G \subset \text{Aut}_K(R)$ and K is algebraically closed in $\mathbb{E}$ because so is it in $K(V)$ which contains $\mathbb{E}$.

Define $G_1 = \{\tau \in G : \text{The induced actions of } \tau \text{ on } R/\mathfrak{M} \text{ and } \mathfrak{M}/\mathfrak{M}^2 \text{ are the identity maps}\}$. By Corollary 2.6, $G_1 = \{1\}$ and G_0 is a cyclic subgroup of $Z(G)$. Let $m = |G_0|$. Then $\zeta_m \in K$ by Lemma 2.5.

We will show that $G_0 = \langle\sigma\rangle$, which is equivalent to showing that $p = m$. Note that m is divisible by p .

In the situation of Theorem 1.1, if $p < m$, the property $\zeta_m \in K$ violates assumption (iv) in Theorem 1.1.

In the situation of Theorem 1.2, since G_0 is cyclic containing σ , it follows that $G_0 = H \times \langle\sigma\rangle$ for some subgroup $H \subset Z(G')$. Should p divide $|H|$, then G_0 would contain an elementary abelian group of order p^2 . But G_0 is a cyclic group! Thus $p \nmid |H|$. Any prime divisor of $|H|$ is a divisor of $\gcd\{m, |Z(G')|\}$. If $p < m$, the property $\zeta_m \in K$ would lead to a contradiction to assumption (iv) of Theorem 1.2.

REFERENCES

- [BF] G. Berhuy and G. Favi, *Essential dimension: a functorial point of view after A. Merkurjev*, Documenta Math. **8** (2003), 279–330. MR2029168 (2004m:11056)
- [Bo] N. Bourbaki, *Commutative algebra*, Hermann, Paris, 1972. MR0360549 (50:12997)
- [BR] J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), 159–179. MR1457337 (98e:12004)
- [JLY] C. Jensen, A. Ledet and N. Yui, *Generic polynomials: constructive aspects of the inverse Galois problem*, MSRI Publ. vol. 45, Cambridge University Press, Cambridge, 2002. MR1969648 (2004d:12007)

DEPARTMENT OF MATHEMATICS, NATIONAL TAIWAN UNIVERSITY, TAIPEI, TAIWAN
E-mail address: kang@math.ntu.edu.tw