行政院國家科學委員會專題研究計畫 成果報告

本質維度之研究
研究成果報告(精簡版)

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 96-2115-M-032-003-
執 行 期 間 ：96 年 08 月 01 日至 97 年 10 月 31 日
執 行 單 位 ：淡江大學數學系

計 畫 主 持 人 ：胡守仁

計畫參與人員：博士班研究生-兼任助理人員：宋曉明

報 告 附 件 ：出席國際會議研究心得報告及發表論文

處 理 方 式 ：本計畫可公開查詢

中 華 民 國 97 年 11 月 13 日

行政院國家科學委員會補助專題研究計畫成果報告

本質爲度之研究

計畫類別: ☒ 個別型計畫 ☐ 整合型計畫

計畫編號:NSC 96–2115–M–032–003-

執行期間: 96 年 8 月 1 日至 97 年 10 月 31 日

計畫主持人: 胡守仁

計畫參與人員: 宋曉明

成果報告類型(依經費核定清單規定繳交): ☒ 精簡報告

本成果報告包括以下應繳交之附件:

☐ 赴國外出差或研習心得報告一份

☐ 赴大陸地區出差或研習心得報告一份

☐ 出席國際學術會議心得報告及發表之論文各一份

☐ 國際合作研究計畫國外研究報告書一份

執行單位: 淡江大學

中 華 民 國 97 年 11 月 13 日

一、中文摘要

我們研究不本質維度的一些性質, 並將本質維度爲1的群分類。令 $\mathrm{ed}_K(G)$ 爲群 G在體K上 的本質維度. 當 K 爲代數封閉的體, 其 $\mathrm{char}K = 0$, Buhler and Reichstein 決定了所有有限群其$\mathrm{ed}_K(G) = 1$ [Compositio Math. **106** (1997), Theorem 6.2]. 我們將此定理推廣到任意體上。

關鍵字**:** 本質維度, 伽羅瓦理論

二、英文摘要

Let K be a field, and G be a finite group. Inverse Galois problem looks into Galois extensions of K with Galois group G. Buhler and Reichstein [BR] defined the essential dimension of G over K when char K=0 to measure the complexity of such extensions. They determined explicitly all finite groups G with $\mathrm{ed}_K(G) = 1$ [Compositio Math. **106** (1997), Theorem 6.2]. We will prove a generalization of this theorem when K is an arbitrary field.

Key words: Essential dimension, compression of finite group actions, Galois theory, finite subgroups of $SL_2(K)$.

三、緣由與目的

Let K be a field, and G be a finite group. Inverse Galois problem looks into Galois extensions of K with Galois group G. Buhler and Reichstein [BR] defined the essential dimension of G over K when char K =0 to measure the complexity of such extensions.

Let L/L_0 be a finite separable extension and E_0 be an intermediate field, $K \subset E_0 \subset L_0$. The extension L/L_0 is said to be defined over E_0 if there exists an

extension E such that $E_0 \subset E \subset L$, $[E : E_0] = [L : L_0]$ and $L = E \cdot L_0$.

If transcendental degree of L over K, $\mathrm{trdeg}_K L$ is finite, the essential dimension of L over L_0, denoted by $\mathrm{ed}(L/L_0)$ is defined as

$$\mathrm{ed}_K(L/L_0) = \min\{\mathrm{trdeg}_K E \mid L/L_0 \text{ is defined over } E_0\}$$

If G is a finite group and $G \longrightarrow GL(V)$ is a faithful representation where $\dim_K V = n < \infty$. The essential dimension of G over K, $\mathrm{ed}_K(G)$ is defined to be $\mathrm{ed}_K(V)/K(V)^G)$ where $K(V)$ is the function field of the affine space V over K. It can be proved that this notion is independent of the representation[BR, Ka].

Buhler and Reichstein determined explicitly all finite groups G with $\mathrm{ed}_K(G) = 1$ [Compositio Math. **106** (1997), Theorem 6.2]. We will prove a generalization of this theorem when K is an arbitrary field.

四、結果與討論

It is obvious that $\mathrm{ed}_K(G) = 0$ if and only if $G = \{1\}$ the trivial group. In Theorem 6.2 [BR] the group G with $\mathrm{ed}_K(G) = 1$ was studied.

Theorem 1. (Buhler and Reichstein [BR]) *Let K be a field such that $charK = 0$ and K contains all roots of unity. If G is a nontrivial finite group, then $ed_K(G) = 1$ if and only if G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ or D_m where m is an odd integer.*

We generalized the above theorem when K is an arbitrary field. The answer is the following five theorems.

Theorem 2. *Let K be an arbitrary field. Suppose that G is a nontrivial finite group with $ed_K(G) = 1$.*

(1) *If $charK = 0$, then G is isomorphic to the cyclic group $\mathbb{Z}/n\mathbb{Z}$ or the dihedral group D_m of order $2m$.*

(2) *If* $charK = p > 0$ *and* $p \neq 2$, *then* G *is isomorphic to the cyclic group* $\mathbb{Z}/n\mathbb{Z}$, *the dihedral group* D_m, *or the group* $G(n, p^r)$.

(3) *If* $charK = 2$, *then* G *is isomorphic to the cyclic group* $\mathbb{Z}/n\mathbb{Z}$, *the dihedral group* D_m, *the group* $G(n, 2^r)$ *or the group* $SL_2(\mathbb{F}_q)$ *where* q *is some power of* 2.

The group $G(n, p^r)$ or $G(n, 2^r)$ will be defined when $p \nmid n$, $s \mid r$ where $s := [\mathbb{F}_p(\zeta_n^2) : \mathbb{F}_p]$.

The group $G(n, p^r)$ first as a subgroup of $SL_2(K)$ where K is an algebraically closed field with $\mathrm{char}K = p > 0$. Another definition of $G(n, p^r)$ as an abstract group will be given in the form of generators and relations. Finally the group $G(n, p^r)$ will be characterized as a subgroup of $SL_2(K)$ (where K is an algebraically closed field with $\mathrm{char}K = p > 0$), which is a semi-direct product of an elementary abelian p-group with a cyclic group.

Now suppose that K is an algebraically closed field with $\mathrm{char}K = p > 0$. Regard K as a vector space over $\mathbb{F}_p$. Since $\zeta_n \in K$, K is also a vector space over $\mathbb{F}_p(\zeta_n)$ (and therefore over $\mathbb{F}_p(\zeta_n^2)$). Choose a vector subspace V of K over $\mathbb{F}_p(\zeta_n^2)$ so that $[V : \mathbb{F}_p] = r$. (Note that $r = [V : \mathbb{F}_p(\zeta_n^2)][\mathbb{F}_p(\zeta_n^2) : \mathbb{F}_p]$.) Choose a basis $\alpha_1, \ldots, \alpha_r$ of V over $\mathbb{F}_p$. Define $\sigma_1, \ldots, \sigma_r, \tau \in SL_2(K)$ by

$$\sigma_i = \begin{pmatrix} 1 & \alpha_i \\ 0 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} \zeta_n & a \\ 0 & \zeta_n^{-1} \end{pmatrix}$$

where a is any element in K if $n \geq 3$, while $a = 0$ if $n = 1$ or 2.

Define $G(n, p^r)$ to be the subgroup of $SL_2(K)$ generated by $\sigma_1, \ldots, \sigma_r, \tau$, i.e. $G(n, p^r) = \langle \sigma_1, \ldots, \sigma_r, \tau \rangle$. Note that $G(1, p^r)$ is an elementary abelian p-group and $G(2, p^r)$ is a direct product of an elementary abelian p-group with $\mathbb{Z}/2\mathbb{Z}$.

Define $Q = \langle \sigma_1, \ldots, \sigma_r \rangle \subset G(n, p^r)$. It is clear that Q is a normal subgroup of $G(n, p^r)$ and Q is an elementary abelian p-group. A typical element in Q is of the

form

$$\sigma = \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}$$

for some $v \in V$. It is easy to verify that

$$\tau \cdot \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} \cdot (\tau^{-1}) = \begin{pmatrix} 1 & \zeta^2 \cdot v \\ 0 & 1 \end{pmatrix}.$$

The next step is to define $G(n, p^r)$ as an abstract group. Choose a basis $\beta_1, \ldots, \beta_t$ of V over $\mathbb{F}_p(\zeta_n^2)$ (thus $r = st$ where $s = [\mathbb{F}_p(\zeta_n^2) : \mathbb{F}_p]$). Let $f(X) = X^s - a_s X^{s-1} - a_{s-1} X^{s-2} - \cdots - a_1 \in \mathbb{F}_p[T]$ be the minimum polynomial of ζ_n^2 over $\mathbb{F}_p$. (Note that $f(X)$ is an irreducible factor of the cyclotomic polynomial $\Phi_n(X)$ or $\Phi_{n/2}(X)$ over $\mathbb{F}_p$.) Define $\beta_{ij} = \zeta_n^{2(j-1)} \beta_i$ where $1 \leq j \leq s$. Then β_{ij} is a basis of V over $\mathbb{F}_p$. It is not difficult to show that $G(n, p^r)$ is generated by

$$\begin{pmatrix} 1 & \beta_{ij} \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} \zeta_n & a \\ 0 & \zeta_n^{-1} \end{pmatrix}$$

where $1 \leq i \leq t$, $1 \leq j \leq s$ and $r = st$. Moreover, the group $G(n, p^r)$ may be defined by generators σ_{ij} and τ (with $1 \leq i \leq t$, $1 \leq j \leq s$) and the relations are given by

$$\sigma_{ij}^p = \tau^n = 1, \quad \sigma_{ij}\sigma_{kl} = \sigma_{kl}\sigma_{ij},$$

$$\tau \sigma_{ij} \tau^{-1} = \sigma_{i,j+1} \quad \text{for} \ \ 1 \leq i \leq t, \ 1 \leq j \leq s-1,$$

$$\tau \sigma_{i,s} \tau^{-1} = \prod_{1 \leq j \leq s} \sigma_{i,j}^{a_j} \quad \text{for} \ \ 1 \leq i \leq t.$$

Thus, as an abstract group, $G(n, p^r)$ is independent of the choice of a.

Theorem 3. *Let K be an arbitrary field and $G = \mathbb{Z}/n\mathbb{Z}$ be the cyclic group of order n.*

(1) *If $charK \nmid n$, then $ed_K(G) = 1$ if and only if $\zeta_n + \zeta_n^{-1} \in K$ when n is an odd integer, or $\zeta_n \in K$ when n is an even integer.*

(2) *If $charK = p > 0$ and $p \mid n$, then $ed_K(G) = 1$ if and only if $n = p$.*

Theorem 4. *Let K be an arbitrary field and $G = D_n$ be the dihedral group of order $2n$.*

(1) *If $charK = 0$, then $ed_K(G) = 1$ if and only if n is an odd integer and $\zeta_n + \zeta_n^{-1} \in K$.*

(2) *If $charK = p > 0$ and $p \neq 2$, then $ed_K(G) = 1$ if and only if n is an odd integer, $\zeta_n + \zeta_n^{-1} \in K$ when $p \nmid n$, or $n = p$ when $p \mid n$.*

(3) *If $charK = 2$, then $ed_K(G) = 1$ if and only if $\zeta_n + \zeta_n^{-1} \in K$ when n is an odd integer, or $|K| \geq 4$ with $n = 2$ when n is an even integer.*

Theorem 5. *Let K be an arbitrary field with $charK = p > 0$. If G is the group $G(n, p^r)$, then $ed_K(G) = 1$ if and only if n is an odd integer, $\zeta_n \in K$ and $[K : \mathbb{F}_p] \geq r$.*

Theorem 6. *Let K be an arbitrary field with $charK = 2$. If G is the group $SL_2(\mathbb{F}_q)$ where q is some power of 2, then $ed_K(G) = 1$ if and only if $K \supset \mathbb{F}_q$.*

As an application of the above theorems, we will prove that, when K is a field with $\mathrm{char}K = 2$, if K doesn't contain $\mathbb{F}_4$, then $\mathrm{ed}_K(A_4) = \mathrm{ed}_K(A_5) = 2$, while $\mathrm{ed}_K(A_4) = \mathrm{ed}_K(A_5) = 1$ if $K \supset \mathbb{F}_4$. Similarly, since $\mathbb{Z}/4\mathbb{Z}$ is contained in the symmetric group S_4 and $\mathrm{ed}_K(S_4) = 2$, we find that $\mathrm{ed}_K(\mathbb{Z}/4\mathbb{Z}) = 2$ if $\mathrm{char}K \neq 2$ and $\sqrt{-1} \notin K$; $\mathrm{ed}_K(\mathbb{Z}/4\mathbb{Z}) = 1$ if $\mathrm{char}K \neq 2$ and $\sqrt{-1} \in K$; $\mathrm{ed}_K(\mathbb{Z}/4\mathbb{Z}) = 2$ if $\mathrm{char}K = 2$. (This result was proved in [BF] Theorem 7.6 in the case $\mathrm{char}K \neq 2$ by a different method.) It is not difficult to verify that $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/5\mathbb{Z}) = \mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/6\mathbb{Z}) = 2$ by the same way.

References

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

[BR] *J. Buhler and Z. Reichstein, On the essential dimension of a finite group, Compositio Math.* **106** *(1997), 159–179.*

[Ka] *M. Kang, itA central extension theorem for essential dimensions, to appear in "Proc. Amer. Math. Soc.".*

[Re] *Z. Reichstein, On the notion of essential dimension for algebraic groups, Transformation Groups* **5** *(2000), 265–304.*

出國開會報告

會議名稱：Interactions between representation theory and commutative algebra

會議地點：Barcelona, Spain

會議時間：97 年 9 月 25 日至 27 日

報 告 人：淡江大學數學系 胡守仁

我於九月二十五日至二十七日參加於西班牙巴塞隆納舉行之 Interactions between representation theory and commutative algebra 會議。這並不是一個大型的會議，參加人數約莫八十人，但都是這方面之專家，討論相當深入。本次會議共有 60 分中演講 11 場，40 分鐘演講 5 場。

首場演講為日本的 Iyama 教授，講題為 *Cluster tilting for one-dimensional hypersurface singularities*，對於 maximal Cohen-Macaulay modules over one-dimensional hypersurface singularities 的範疇中的 cluster tilting object 進行分類。來自 Nebraska 的 Avramov 教授對於複形定義了新的剛性，比原有的來得廣，但仍保持唯一性與自然性。來自德國的 Dufrensne 考慮的則是較不變量環稍為廣泛的分離代數，得到反只有反射群才會存在多項式的分離代數。這是我最感興趣的結果。我以壁報形式呈現關於秩為 32 的群的有理性結果，有不少討論。三天會議收穫良多。

攜回資料：會議議程及摘要。