行政院國家科學委員會專題研究計畫成果報告

不變量環之諾德界
Degree Bounds for Rings of Invariants

計畫編號：NSC 90-2115-M-032-001-
執行期限：90 年 8 月 1 日至 91 年 7 月 31 日
主持人：胡守仁　　淡江大學數學系
計畫參與人員：吳玲、周純玉　淡江大學數學系

一、 中文摘要

ρ:G ——>GL(V) 為一線性表現，其中 V 為域 **F** 上為數為 n 之向量空間。希伯特證明當 G 唯一有限群時，**F** 之特徵數為零時，**F**[V]^G 為有限生成。諾德並給出一個方法，造出其生成元，在某些情形下，可取生成元之次方次均不超過|G|。吾人將研究一般情形下生成元次方之上界。

關鍵詞：不變量環、生成元、諾德界

Abstract

ρ:G ——>GL(V) is a representation of G into GL(V) where V is an n-dimensional vector space over a field **F**. Hilbert proved that when characteristic of **F** is zero and G is a finite group, then the ring of invariants **F**[V]^G is finitely generated. Noether gave an algorithm to explicitly find the generators with degree ≦|G|. In this project, we shall consider Noether's bound in a more general case.

二、 緣由與目的

Given $\rho : G \to GL(n, \mathbb{F})$ a representation of a finite group G over the field $\mathbb{F}$, it induces an action on the algebra $\mathbb{F}[V]$ of polynomial functions on $V = \mathbb{F}^n$. If $\rho : G \to GL(n, \mathbb{F})$ is a faithful representation, we denote by $\mathbb{F}[V]^G = \{f \in \mathbb{F}[V] \mid \rho(g)f = f \;\forall\; f \in G\}$ the ring of invariants of G. Notice that $\mathbb{F}[V]$ can be regarded as a graded algebra over $\mathbb{F}$ with homogeneous component of degree $d, \mathbb{F}[V]_d$, the homogeneous polynomial of degree d. If G is a finite group, Hilbert proved in 1890 [H], the main theorem of invariant theory that the ring of invariants is finitely generated. Noether [N] later produced an explicit set of basic invariants. In fact, she gave an algorithm to construct a system of generators using polarizations of elementary symmetric polynomials ([W], [S1]). From this, she found generators for the ring of invariants of degree at most $|G|$. We call the maximal degree of a generator in any minimal generating set for $\mathbb{F}[V]^G$ Noether's bound and is denoted by $\beta(V)$. For example, if G is a cyclic group and ρ is a faithful representation, then $\beta(V) = |G|$. Smith and Stong [S-S] extend the results fields of characteristic $p > |G|$ (called the strong nonmodular case) and Smith also succeeded in the case that G is a solvable group when the characteristic $p \nmid |G|$ (called the nonmodular case).

In the case that G is a linearly reductive algebraic group over an algebraically closed field $\mathbb{F}$ of characteristic 0 acting rationally on an n-dimensional vector space V, Popov also got some explicit degree bound ([P1], [P2])as following

$$\beta(V) \leq nLCM(1, 2, \ldots, \sigma(V))$$

where LCM denote the least common multiple. The constant $\sigma(V)$ is the smallest integer with d with the following property: if $v \in V$ and any non-constant homogeneous invariant vanishes on v, then there is a non-constant homogeneous invariant f of degree $\leq d$ such that $f(v) \neq 0$. Derken improved the result [D] to

$$\beta(V) \leq \max(2, \frac{3}{8} s\sigma^2(V))$$

Upper bound for $\sigma(V)$ were given by Popov ([P1], [P2]). An explicit bound of $\sigma(\rho)$ can expressed in the degrees of polynomials defining the group G and the representation ρ [D]. For example, if $G = SL(W)$ where W is a q-dimensional vector space. Let $V_d = S^d(W)$ be the d-th symmetric power, then $\sigma(V_d) \leq qd^{q^2-1}$.

In special cases, sharper estimates than Popov's bound were known. Gordan already knew the finite generation of $\mathbb{C}[V]^{SL_2(\mathbb{C})}$ before Hilbert [G]. Jordan used these techniques to obtain that $\mathbb{F}[V]^G_d$ can be generated by polynomials of degree $\leq d^6$ ([J1], [J2]). Wehau gave a good degree bound for tori in [W].

We can extend the consideration to the case of a commutative ring R. In this situation, let V be a finitely generated free R-module and $G \leq GL_R(V)$ be a finite group acting naturally on the graded symmetric algebra $A = S(V)$. Fleischmann proved that for a normal subgroup H in G, $\beta(A^G) \leq \beta(A^H) \cdot |G : H|$ ([F1]). He also has some results in the special case G is the symmetric group S_n ([F2]).

三、 結果與討論

For a finitely generated algebra A over a commutative ring, $A:=R[a_1,\ldots a_r]$, with a finnite group acting as R-homomorphisms, we have that A^G can be generated as R-algebra by elements of degrees less than or equal to n if 1/n! lies in R or 1/n lies in R and there is a normal subgroup H in G, G/H is solvable, $A^{H}=R[b_1, \ldots b_m]$ and G/H sends the linear part ÓRb$_j$ into itself.

We also did some calculations on invariants of dihedral groups. We get the following results.

Theorem. Let K be any infinite field and G a finite group. Let ñ: G -→ GL(V) be a faithful representation of G where V is some finite dimensional vector space over K. If the fixed field $K(V)^G$ is stably rational over K, then there exists a generic Galois G-extension over K.

Theorem. If G is the dihedral group, then K(G) is rational over K.

Theorem. If G is the quasi-dihedral group, then K(G) is rational over K.

Theorem. If G is the modular group, then K(G) is rational over K.

四、參考資料

[D] H. Derken, *Polynomial bounds for rings of invariants*, Proc. Amer. Math. Soc. (2000), 1-9.

[F1] P. Fleischmann, *A new degree bound for vector invariants of symmetric groups*, Tranc. Amer. Math. Soc. **350** (1998), 1703-1712.

[F2] P. Fleischmann, *The Noether bound in invariant theory of finite groups*, Adv. in Math. **156** (2000), 23-32.

[G] P. Gordan, *Beweis dass jede Covariante und Invariante einer binären Form eine ganze Function mit numerischen Coefficienten solcher Formen ist*, J. Für reine u. agnew Math. **69** (1868), 323-354.

[H] D. Hilbert, *Über die Theorie der Algebraischen Formen*, Math. Ann. **36** (1890), 473-534.

[J1] C. Jordan, *Mémoire sur les covariants des formes binaires*, J. de Math. **3(2)** (1876), 177-232.

[J2] C. Jordan, *Sur les covariants des formes binaires*, J. de Math. **3(5)** (1879), 345-378.

[N] E. Noether, *Der Endlischkeitssatz der Invarianten endlicher Gruppen*, Math. ANnn. **77** (1916), 89-92.

[P1] V. Popov, *Constructive invariant theory*, Astériques **87-88** (1981), 303-334.

[P2] V. Popov, *The constructive theory of invariants*, USSR Izvest. **10** (1982), 359-376.

[S1] L. Smith, *Polynomial Invariants of Finite Groups*, A. K. Peters, Wellesley, Mass., 1995.

[S2] L. Smith, *Noether's bound in the invariant theory of finite groups*, Arch. der Math. **66** (1996), 89-92.

[S-S] L. Smith and R. E. Stong, *On the invariant theory, orbit polynomials and splitting principles*, J. of Algebra **110** (1987), 134-157.

[W] D. Wehlau, *Constructive invariant theory for tori*, Ann. Inst. Fourier **43, 4** (1993).