行政院國家科學委員會專題研究計畫成果報告

模不變量理論

Modular Invariant Theory

計畫編號：NSC 88-2115-M-032-006-

執行期限：87 年 8 月 1 日至 87 年 7 月 31 日

主持人：胡守仁　　淡江大學數學系

一、中文摘要

對一個群表現ρ: G ----→ GL((n, F)，$F[V]^G$ 為其不變量環，此處 V 為 F^n。在此我們將考慮當 F 之特徵數為 G 之約數時，即為模不變量時，$F[V]^G$ 之結構，並計算秩為質數方次時之情形。

關鍵詞：不變量環、擬反射群、Dickson 代數、Steenrod 代數

Abstract

Let ρ: G ----→ GL((n, F) be a representation of G. We shall study the ring of invariants $F[V]^G$ in the case when the characteristic of F divides the order of G. We shall specially consider the case when order of G is a prime power.

Keywords: ring of invariants, pseudo-reflection group, Dickson algebra, Steenrod algebra

二、緣由與目的

For a representation ρ: G ----→ GL((n, F) of a finite group G over the field F, we have an induced action on the algebra F[V] of polynomial functions on $V = F^n$. $F[V]^G$ denote the ring of invariants.

In the nonmodular case, i.e. when the order of G is relatively prime to the characteristic of f, the ring $F[V]^G$ is known to be Cohen-Macaulay [HE, S1]. Chevalley-Shephard-Todd Theorem also tells us that in this case $F[V]^G$ is a polynomial ring if and only if G is generated by pseudo-reflections [Ch, ST].

Invariant theory in the modular case is not well-developed and organized. In fact apart from the basic finiteness theorem of Noether and Hilbert's syzygy theorem, all the nice features of the nonmodular case can and do fail in the modular case.

In the modular case, the Dickson algebra provides a source of universal modular invariants. Actually, the Dickson polynomials are present in any ring of invariants in characteristic p. One way to study a ring of invariants in characteristic p is to regard it as an integral extension of the Dickson algebra.

Besides Dickson algebra, one can introduce Steenrod algebra . It organizes information derived from the Frobenius homomorphism. It also provides a mean of constructing new invariants from old ones and imposes a rigid structure on modular rings of imvariants.

三、結果與討論

Let F_q denote the Galois field, $q = p^n$. $GL(n,F_q)$ is a finite group of order $(q^n-1)(q^n-q)\ldots(q^n-q^{n-1})$ acting on $V = F^n$. Dickson algebra D*(n) is the ring of invariants $F_q[V]^{GL(n,Fq)}$ [D]. For any finite group G acting on V, the ring of invariants $F_q[V]^G$ is a finite extension of $F_q[V]^{GL(n,Fq)}$. We shall first give some theorem involving the modular case and then we shall give some examples.

Theorem (Dickson). *Suppose $n \in \mathbb{N}$, p a prime, $q = p^s$ and $V = \mathbb{F}_q^n$. Then*

$$D^*(n) = \mathbb{F}_q[V]^{GL(n,\mathbb{F}_q)} \cong \mathbb{F}_q[y_1, \ldots, y_n]$$

where $deg(y_i) = q^n - q^{n-i}$ for $i = 1, \ldots, n$.

The polynomials y_i can be found explicitly.

Theorem (Stong-Tamagawa). [S-T] *Let $n \in \mathbb{N}$, p be a prime and q a power of p. Then*

$$D^*(n) = \mathbb{F}_q[d_{n,0}, \ldots, d_{n,n-1}]$$

where

$$d_{n,i} = \sum_{\substack{W \le V \\ dim(W)=i}} \prod_{v \notin W} v$$

The polynomial $d_{n,i}$ has degree $q^n - q^i$.

The classes $d_{n,i}$ are called the Dickson polynomials.

In the case of p-group P in characteristic p, the fixed point set $V^P \neq 0$. The higher the dimension of this fixed point set is, the simpler the action is. Also in the modular case, the ring of invariants $\mathbb{F}[V]^G$ need not be Cohen-Macaulay. The Cohen-Macaulay property of $\mathbb{F}[V]^G$ is in fact controlled by the p-Sylow subgroup of G.

Theorem. *Let $\mathbb{F}$ be a field of characteristic $p \neq 0$ and $\rho :\hookrightarrow GL(n, \mathbb{F})$ a representation of finite group G. If $\mathbb{F}[V]^H$ is Cohen-Macaulay, so is $\mathbb{F}[V]^G$ where H is a p- Sylow subgroup of G.*

To construct invariants, we shall introduce orbit polynomials and orbit Chern classes.

Definition. Let G be a finite group acting on a set X. A subset $Y \subset X$ is said to be invariant if $g \cdot y \in Y$ for all $y \in Y$ and $g \in G$. If $B \subset X$ is invariant and G acts transitively on B (i.e. $\forall b, b' \in B \, \exists g \in G$ such that $g \cdot b = b'$).

Let V be a finite dimensional G-representation, G a finite group. For an orbit $B \subset V^*$ set

$$\varphi_B(X) = \prod_{b \in B} (X + b)$$

which we regard as an element of the ring $\mathbb{F}[V][X]$. $\varphi_B(X)$ is called the orbitm polynomial. It is clear that $\varphi_B(X) \in \mathbb{F}[V]^G[X]$. In fact, we can define $\varphi_B(X)$ as above to get an element in $\mathbb{F}[V][X]$. If B is invariant, then $\varphi_B(X) \in \mathbb{F}[V]^G[X]$. If the subsets B and B' are disjoint, then $\varphi_B(X) \cdot \varphi_B(X) = \varphi_{B \cup B'}(X)$.

If $|B|$ denotes the cardinality of the orbit B, we may expand $\varphi_B(X)$ to a polynomial of degree $|B|$ in X obtaining

$$\varphi_B(X) = \sum_{i+j=|B|} c_i(B) \cdot X^j$$

defining classes $c_i(B) \in \mathbb{F}[V]^G$ called the orbit Chern classes of the orbit B. Note that $\mathbb{F}[V]$ is integral over $\mathbb{F}[V]^G$ of finite type and for $v \in V^*$ the orbit polynomial $\varphi_{G \cdot v}(X)$ is the minimal polynomial of the element $-v$ over $\mathbb{F}[V]^G$.

Remark. 1. The first orbit Chern class $c_1(B)$ is the sum of the orbit elements and hence $c_1(B) = Tr^{G/G_b}(b)$ where $b \in B$ is arbitrary and G_b si the isotropy group of b.

2. If $k = |B|$, then $c_k(B)$ is the product of all the elements in $B$and referred to as the top Chern class of the orbit. It is also referred to as the norm of b and is multiplicative.

3. The Chern classes of the orbit are nothing but the elementary symmetric polynomials in the elements of the orbit.

Definition. $\mathbb{F}[V]^G$ is said to satisfy the weak splitting principle if there are a finite number of orbits whose orbit Chern classes generate $\mathbb{F}[V]^G$. If a single orbit suffices then we say that $\mathbb{F}[V]^G$ satisfies the splitting principle.

Example 1. Consider the subgroup of $GL(2, \mathbb{F}_3]$ generated by the matrices

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} -1 & 1, \\ 1 & 1 \end{bmatrix}$$

Set

$$C = AB = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

One readily check that

$$A^2 = B^2 = C^2 = -I$$

where I is the identity matrix. Hence this subgroup is isomorphic to the quternion group Q_8 of order 8. One can check that Q_8 acts transitively on $\mathbb{F}_3^2$. Thus the only orbits are $\{0\}$ and $V^* - \{0\}$ and the only Chern classes are therefore

$$\frac{xy^9 - x^9y}{xy^3 - x^3y}, \quad (xy^3 - x^3y)^2$$

where $\{x, y\}$ is the dual of the canonical basis of $\mathbb{F}_3^2$. These polynomials are of degree 6 and 8. However, $x^4 + y^4$ is invariant, hence the Chern classes can not generate $\mathbb{F}_3[x, y]^{Q_8}$.

Example 2. The group $G = GL(2, \mathbb{F}_2)$ is a non-abelian group of order 6, hence is isomorphic to S_3. It acts on $V = \mathbb{F}_2^2$. There are two orbits for the action namely, $\{0\}$ and $V - \{0\}$and analogously for the dual space V^*. If $\{x, y\}$ is a basis for V^* then the Chern class of $V^* - \{0\}$ are

$$c_i = \begin{cases} 0 & fori = 1 \\ x^2 + xy + y^2 & fori = 2 \\ xy^2 + x^2y & fori = 3 \end{cases}$$

as they are elementary symmetric polynomials in the elements $x.y$ and $x + y$ of $V^* - \{0\}$. The classes c_1, c_2 are algebraically independent, so $\mathbb{F}_2[V]^G \supset \mathbb{F}_2[x^2 + xy + y^2, x^2y + xy^2]$. In fact, they are equal because of the following theorem:

Theorem. *Suppose $G \hookrightarrow GL(V)$ is a finite dimensional representation of a finite group G and $\mathbb{F}[V]^G$ contains elements $f_1, \ldots f_n$, $n = dim_{\mathbb{F}}(V)$ such that deg (f_1) $\ldots$, deg(f_n)= $|G|$. If $f_1, \ldots, f_n$ are system of parameters then $\mathbb{F}[V]^G \cong \mathbb{F}[f_1, \ldots, f_n]$.*

Example 3. Fix a prime p and let $m|p-1$. The dihedral group $D_{2m} := \mathbb{Z}/m \rtimes \mathbb{Z}/2$ of order $2m$ has a faithful representation of dimension 2 over $\mathbb{F}_p$ given by the matrices

$$\begin{bmatrix} \theta & 0 \\ 0 & \theta^{-1} \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in GL(2, \mathbb{F}_p)$$

where $\theta \in \mathbb{F}_p$ is a primitive $m-th$ root of unity. Let $\{u, v\}$ denote a basis for $V = \mathbb{F}_p^2$ with respect to which the generators of D_{2m} have the above form. One can see that

$$\mathbb{F}_p[V]^{D_{2m}} \simeq \mathbb{F}[\rho_1, \rho_2]$$

where

$$\rho_1 = uv, \quad \rho_2 = u^m + v^m$$

are possible choice of polynomial generators. Let B be the orbit of $u + v$. The orbit polynomial of B is

$$\varphi_B(X) = \prod_{i=1}^{m} (X + \theta^i u + \theta^{-i} v).$$

To compute this polynomial, we let

$$\alpha(u, v) := (u+v)^m - (u^m + v^m) \in \mathbb{F}_p[u, v].$$

Note that $\alpha(u, v)$ is invariant with respect to the involution that interchanges u and v. Therefore, it is possible to write $\alpha(u, v)$ as a polynomial in the elementary symmetric functions $e_1 = u + v$ and $e_2 = uv$. Taking account of homogeneity we see that

$$\alpha = \sum_{i_1 + 2i_2 = m} a_{i_1 i_2} e_1^{i_1} e_2^{i_2},$$

where $a_{i_1 i_2} \in \mathbb{F}_p$. Since $\alpha(u,v)$ does not contain the terms u^m, v^m it follows that $i_1 < m$, so we may rewrite this formula in the form

$$\alpha = \sum_{j=1}^{m/2]} b_j e_1^{m-2j} e_2^j,$$

where $b_j \in \mathbb{F}_p$ and $[m/2]$ denotes the integral part of $m/2$ After calculation, $b_1 = m \not\equiv 0 \bmod p$. Computing further we obtain

$$\begin{aligned}\alpha(u,v) &= (u+v)^m - \rho_2 \\ &= \sum_{j=1}^{m/2]} b_j e_1^{m-2j} e_2^j \\ &= \sum_{j=1}^{m/2]} b_j (u+v)^{m-2j} (uv)^j \\ &= \sum_{j=1}^{m/2]} b_j \rho_1^j (u+v)^{m-2j}\end{aligned}$$

which yields the identity
(*)

$$(u+v)^m - \sum_{j=1}^{[m/2]} b_j \rho_1^j (u+v)^{m-2j} - \rho_2 = 0$$

Let

$$h(X) = X^m - (\sum_{j=1}^{[m/2]} b_j \rho_1^j X^{m-2j}) - \rho_2 \in \mathbb{F}_p[u,v]^{D_{2m}}[X]$$

The identity (*) shows that $h(u+v) = 0$. The coefficients of $h(X)$ are invariant with respect to the action of D_{2m}, so D_{2m} acts on the roots of $h(X)$ in $\mathbb{F}_p[u,v]$. Hence $h(X)$ is zero on the elements of the orbit $D_{2m} \cdot \{\theta^i u + \theta^{-i} v\}$. But the degreeof $h(X)$ is $m = |D_{2m} \cdot (u+v)|$ and $h(X)$ is monic, hence $h(X) = \varphi D_{2m \cdot (u+v)}(X)$, the orbit polynomial of $D_{2m} \cdot (u+v)$. From this we read off the Chern classes of the orbit of $u+v$, in particular, we have

$$c_{2i}(D_{2m} \cdot (u+v)) = \begin{cases} -b_i \rho_1^i & \text{for} 1 \leq i \; [\frac{m-1}{2}] \\ b_{[m/2]} \rho_1^{[m/2]} - \rho_2 & \text{for } i = [\frac{m}{2}] \text{and } m \text{ odd} \\ -\rho_2 & \text{for } i = [\frac{m}{2}] \text{and } m \text{ even} \\ 0 & \text{otherwise} \end{cases}$$

Since $b_1 = m \not\equiv 0 \bmod p$ it follows that $c_2(D_{2m} \cdot (u+v))$ and $c_m(D_{2m} \cdot (u+v))$generate the ring of invariants, so $\mathbb{F}_p[V]^{D_{2m}}$ satisfies the splitting principle.

四、參考文獻

[Ch] Chevalley, C., *Invariants of finite groups generated by reflections*, Amer. J. Math **77** (1955), 778-782.

[D] Dickson, L. E., *Binary Modular Groups and their Invariants*, Amer. J. of Math. **33** (1911), 175-192.

[HE] Hochster, M. and Eagon, J. A., *Cohen-Macaulay rings, invariant theory and the generic perfection of determinantal loci*, Amer. J. of Math. **93** (1971), 1020-1058.

[ST] Shephard, G. C. and Todd, A., *Finite unitary reflection groups*, Canad. J. Math. **6** (1954), 274-304.

[S1] Smith, L., *Polynomial Invariants of finite groups*, A. K. Peters, Ltd, Wellesley, MA, 1995.