¿Qué es... el teorema de Molien?

Verónica Calvo Cortés, Juan Sebastián Numpaque Roa
Universidad de los Andes

La teoría de invariantes es una rama del álgebra que estudia las acciones de grupos en anillos de polinomios, espacios vectoriales y variedades algebraicas más generales. Concretamente, esta teoría da una descripción explícita de qué funciones polinomiales no cambian, o quedan invariantes, bajo la acción de un grupo. Entre los resultados más relevantes en esta teoría se encuentra el bello *Teorema de Molien*. Informalmente hablando, este teorema provee una forma de calcular la dimensión del subanillo de polinomios homogéneos de grado d que quedan invariantes bajo la acción de un grupo finito G. El objetivo de este artículo es ofrecer una demostración amable de este teorema utilizando técnicas de álgebra lineal y teoría de representaciones.

Contexto

Sean G un grupo finito y (V, ρ) una representación compleja de dimensión finita de G. Recordemos que toda representación compleja admite un producto interno G-invariante $\langle \_ , \_ \rangle : V \times V \to \mathbb{C}$. Con respecto a este producto interno consideramos la base ortonormal $B = \{e_1, \ldots, e_n\}$ de V y así, para todo $g \in G$, la matriz $[\rho(g)]_B$ es una matriz unitaria.

Consideremos la base dual de B, $B^* = \{x_1, \ldots, x_n\}$. Recordemos que el anillo $R := \mathbb{C}[x_1, \ldots, x_n]$ tiene estructura natural de álgebra graduada pues lo podemos descomponer en la suma directa de sus componentes homogéneas de grado $d \in \mathbb{N}$, R_d. Más aún, cada una de estas componentes graduadas es isomorfa a la potencia simétrica de grado d de V^*. En otras palabras, tenemos el siguiente isomorfismo de álgebras:

$$R = \mathbb{C}[x_1, \ldots, x_n] \cong \bigoplus_{d\in\mathbb{N}} R_d \cong \bigoplus_{d\in\mathbb{N}} \mathrm{Sym}^d(V^*) = \mathrm{Sym}(V^*).$$

De esto se sigue que G actúa naturalmente en R. Recordemos que podemos ver a V^* como una G-representación al dotarlo de la *acción contragradiente*

$$\rho^*(g)(f)(v) = f(\rho(g^{-1})(v)) = f \circ \rho(g^{-1})(v)$$

para $g \in G$, $f \in V^*$ y $v \in V$ cualesquiera. Para todo $d \in \mathbb{N}$ podemos extender la acción contragradiente a $\mathrm{Sym}^d(V^*) \cong R_d$ mediante su propiedad universal. Denotamos por $\rho_d^* : G \to \mathrm{GL}(R_d)$ a esta representación. Del mismo modo podemos extenderla a una acción, $\rho_R^* : R \to \mathrm{GL}(R)$, en $\bigoplus \mathrm{Sym}^d(V^*) \cong R$.

El espacio vectorial de polinomios invariantes, objeto de estudio de este artículo, se denota por

$$R^G = \{f \in R \mid \rho_R^*(g)(f) = f \text{ para todo } g \in G\}.$$

No es difícil ver que R^G es una subálgebra de R y que también tiene estructura de álgebra graduada. Es decir,

$$R^G \cong \bigoplus_{d\in\mathbb{N}} R_d^G$$

donde $R_d^G := R_d \cap R^G$.

Teorema de Representación de Riesz

Podemos dotar a V^* de un producto interno hermitiano natural: $\langle \_ , \_ \rangle_* : V^* \times V^* \to \mathbb{C}$ dado por $\langle x_i, x_j \rangle_* = \delta_{ij}$. Con respecto a este producto interno los operadores $\rho^*(g)$, para todo $g \in G$, resultan ser unitarios. Es decir, $\langle \_ , \_ \rangle_*$ es G-invariante.

Sean U, W espacios vectoriales sobre $\mathbb{C}$. Una función $f : U \to W$ es *lineal conjugada* si $f(u_1 + u_2) = f(u_1) + f(u_2)$ y $f(cu_1) = \bar{c}f(u_1)$ para todos $u_1, u_2 \in U$ y $c \in \mathbb{C}$. Si, además, f es biyectiva se dice que f es un *isomorfismo conjugado*. El **Teorema de representación de Riesz** afirma que el mapa $\tau : V \to V^*$ dado por $v \mapsto \langle \_, v \rangle$ es un isomorfismo conjugado. $P := \tau^{-1}$ se define como el *mapa de Riesz*. Y, el *vector de Riesz*, $P(f)$, se escribe explicitamente como

$$P(f) = \sum_{i=1}^{n} \overline{f(e_i)} e_i$$

y esto, en particular, implica que $P(x_i) = e_i$. Note también que el vector de Riesz de $\rho^*(g)(f)$ es $\rho(g)(P(f))$ para todo $g \in G$. Es decir, el diagrama

$$\begin{tikzcd} V^* \arrow[r, "P"] \arrow[d, "\rho^*(g)"'] & V \arrow[d, "\rho(g)"] \\ V^* \arrow[r, "P"] & V \end{tikzcd}$$

conmuta para todo $g \in G$. De este modo, podemos pensar en el mapa de Riesz como un morfismo de representaciones conjugado. Otra propiedad importante del mapa de Riesz es que es equivariante. Es decir, $\langle f, h \rangle_* = \langle P(f), P(h) \rangle$, para cualesquiera $f, h \in V^*$.

Podemos entonces utilizar la unitariedad de ρ y las propiedades mencionadas del mapa de Riesz para demostrar que $\langle \rho^*(g)(f), h \rangle_* = \langle f, \rho^*(g)^{-1}(h) \rangle_*$ para todos $f, h \in V^*$ y $g \in G$. Es decir, para ver que ρ^* es unitario.

Teoría Espectral de ρ_d^*

Primero note que como los operadores $\rho(g)$ y $\rho^*(g)$ son unitarios entonces sus valores propios tienen norma 1.

Más concretamente, tenemos que si $v \in V$ es un vector propio con valor propio λ de $\rho(g)$ entonces v y $\tau(v)$ son vectores propios de $\rho(g^{-1})$ y $\rho^*(g)$ respectivamente con valor propio $\bar{\lambda}$. Similarmente, si $f \in V^*$ es un vector propio con valor propio λ de $\rho^*(g)$ entonces f y $P(f)$ son vectores propios de $\rho^*(g^{-1})$ y $\rho(g)$ respectivamente con valor propio $\bar{\lambda}$. Esto implica en particular que para un $g \in G$ fijo el espectro de $\rho^*(g)$ es igual, teniendo en cuenta multiplicidades, al espectro de $\rho(g^{-1})$. Luego, al considerar la unión de los espectros de $\rho(g)$ sobre todo G como multiconjunto esta es igual a la unión de los espectros de $\rho^*(g)$ sobre todo G.

Ahora veamos la relación entre los valores propios de $\rho^*(g)$ y los valores propios de $\rho_d^*(g)$ para un $g \in G$ fijo. Note que para todo $g \in G$ la matriz $\rho^*(g)$ es unitariamente diagonalizable ó, en otras palabras, existe una base $\{y_1, \ldots, y_n\}$ ortonormal de vectores propios de V^*. Para $1 \leq i \leq n$, sea λ_i el valor propio asociado a y_i. Es claro que $B_d = \{y_1^{a_1} y_2^{a_2} \cdots y_n^{a_n} \mid a_1 + \ldots + a_n = d\}$ es una base de $R_d \cong \mathrm{Sym}^d(V^*)$. Además, por como está definida la acción de G en R_d tenemos que

$$\begin{aligned}\rho_d^*(g)(y_1^{a_1} \cdots y_n^{a_n}) &= \rho^*(g)(y_1)^{a_1} \cdots \rho^*(g)(y_n)^{a_n} \\ &= \lambda_1^{a_1} y_1^{a_1} \cdots \lambda_n^{a_n} y_n^{a_n} \\ &= \lambda_1^{a_1} \cdots \lambda_n^{a_n} (y_1^{a_1} \cdots y_n^{a_n}).\end{aligned}$$

Es decir, $y_1^{a_1} \cdots y_n^{a_n} \in R_d$ es un vector propio de $\rho_d^*(g)$ correspondiente al valor propio $\lambda_1^{a_1} \cdots \lambda_n^{a_n}$. Así, todos los valores propios de ρ_d^* son de la forma $\lambda_1^{a_1} \cdots \lambda_n^{a_n}$ donde $a_1 + \ldots + a_n = d$. Denotamos estos valores propios como $\{\tilde{\lambda}_1, \ldots, \tilde{\lambda}_{\tilde{d}}\}$ donde $\tilde{d} = \dim(R_d) = \binom{n+d-1}{d}$. Luego, $[\rho_d^*(g)]_{B_d} = \mathrm{diag}\{\tilde{\lambda}_1, \ldots, \tilde{\lambda}_{\tilde{d}}\}$.

Teorema de Molien

Sean $a_d = \dim_{\mathbb{C}}(R_d^G)$ y $\Phi(t) = \sum_{d \in \mathbb{N}} a_d t^d$ su función generadora. Los *operadores de Reynolds* de las representaciones ρ y ρ_d^* se definen como

$$T : V \to V \quad \text{dado por} \quad v \mapsto \frac{1}{|G|} \sum_{g \in G} \rho(g)(v),$$

$$T_d : R_d \to R_d \quad \text{dado por} \quad f \mapsto \frac{1}{|G|} \sum_{g \in G} \rho_d^*(g)(f).$$

Los operadores de Reynolds son automorfismos de representaciones, hermitianos (auto-adjuntos) e idempotentes. En consecuencia, estos operadores son diagonalizables y sus valores propios son 0 ó 1.

Ahora, recordemos que de la teoría de caracteres se tiene que

$$\dim(R_d^G) = \frac{1}{|G|} \sum_{g \in G} \chi_d(g) = \mathrm{Tr}(T_d)$$

donde $\chi_d : G \to \mathbb{C}$ es el caracter de (R_d, ρ_d^*). De lo anterior es claro que $a_d = \mathrm{Tr}(T_d)$. Sin embargo, esta forma de calcular las dimensiones de R_d^G puede resultar tediosa y complicada. El teorema de Molien nos da una forma sencilla de calcular estos coeficientes.

Teorema de Molien

$$\Phi(t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(\mathrm{Id} - t\rho(g))}.$$

Veamos su prueba. Note que $\det(\mathrm{Id} - t\rho(g))$ sólo depende de los valores propios de $\rho(g)$. Como el determinante es multiplicativo podemos considerar una base en la que $\rho(g)$ sea diagonal para calcularlo. Entonces, por lo visto en la sección anterior, se tendrá que

$$\varphi(t) := \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(\mathrm{Id} - t\rho(g))} = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(\mathrm{Id} - t\rho^*(g))}.$$

Así, el problema se traduce a ver que el coeficiente de t^d en $\varphi(t)$ es $\mathrm{Tr}(T_d)$. Y para esto, de hecho, mostraremos que el coeficiente de t^d en $\frac{1}{\det(\mathrm{Id} - t\rho(g))}$ es $\chi_d(g)$ para todo $g \in G$.

Recordemos que para un $g \in G$ fijo los valores propios de $\rho^*(g)$ son $\lambda_1, \ldots, \lambda_n$. Entonces

$$\begin{aligned}\frac{1}{\det(\mathrm{Id} - t\rho(g))} &= \frac{1}{(1 - t\lambda_1) \cdots (1 - t\lambda_n)} \\ &= \frac{1}{1 - t\lambda_1} \cdots \frac{1}{1 - t\lambda_n} \\ &= (1 + t\lambda_1 + t^2\lambda_1^2 + \ldots) \cdots (1 + t\lambda_n + t^2\lambda_n^2 + \ldots).\end{aligned}$$

Luego, el coeficiente de t^d es

$$\sum_{a_1 + \ldots + a_n = d} \lambda_1^{a_1} \cdots \lambda_n^{a_n} = \sum_{i=1}^{\tilde{d}} \tilde{\lambda}_i = \chi_d(g)$$

concluyendo la demostración.

Aplicación

Ilustremos este hermoso resultado a través de un ejemplo. Considere el grupo de matrices

$$V_4 = \left\{ A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, A_3 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, A_4 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\} \subset \mathrm{GL}(M_{2\times 2}(\mathbb{C}))$$

actuando de forma natural en $\mathbb{C}^2$. Entonces tenemos que

$$\begin{aligned}\det(\mathrm{Id} - tA_1) &= (1-t)^2 & \det(\mathrm{Id} - tA_2) &= (1+t)^2 \\ \det(\mathrm{Id} - tA_3) &= 1 - t^2 & \det(\mathrm{Id} - tA_4) &= 1 - t^2.\end{aligned}$$

Así, por la fórmula de Molien tenemos que

$$\begin{aligned}\Phi(t) &= \frac{1}{4}\left(\frac{1}{(1-t)^2} + \frac{1}{(1+t)^2} + \frac{2}{1-t^2} \right) = \frac{1}{(1-t^2)^2} \\ &= 1 + 2t^2 + 3t^4 + \ldots\end{aligned}$$

Luego, obtenemos que $\dim(R_2) = 2$, $\dim(R_3) = 0$ y $\dim(R_4) = 3$. Es decir, los invariantes de grado 2 son generados por dos polinomios (de hecho, podemos tomar x^2 y y^2 como estos generadores), no hay ningún polinomio invariante de grado 3 y los invariantes de grado 4 son generados por tres polinomios.

Referencias

[Dan 17] Daniel, Alberto. (2017) *An Introduction to Invariant Theory* (Tesis de pregrado). Recuperada de: `http://urn.kb.se/resolve?urn=urn:nbn:se:oru:diva-55454`

[Der 15] Dersken, Harm y Kempfer, Gregor. (2015) *Computational Invariant Theory*, 2^{da} Edición. Springer-Verlag: New York.

[Rom 08] Roman, Steven. (2008) *Advanced linear algebra*, 3^{ra} Edición. Springer-Verlag: New York.

[Sch 17] Schellwat, Holger. (2017) *A Gentle Introduction to a Beautiful Theorem of Molien*. Recuperado de: `https://arxiv.org/abs/1701.04692v1`.