

TEMat

Aplicación en combinatoria de las representaciones de grupos

✉ Gonzalo Cao Labora
Universitat Politècnica de Catalunya
(UPC)
gonzalocaolabora@yahoo.es

Resumen: El objetivo de este artículo es presentar una aplicación del álgebra en la combinatoria. Trataremos la teoría algebraica de representaciones de grupos, que se utiliza en multitud de áreas de las matemáticas (geometría diferencial, análisis armónico, teoría de números...) o incluso en física teórica. Nosotros la utilizaremos en la combinatoria, asociando conceptos algebraicos con conceptos combinatorios. Esto permite probar resultados combinatorios a través de los resultados algebraicos correspondientes. En particular, usaremos la teoría presentada para probar una igualdad combinatoria.

Al igual que en muchas otras partes del álgebra, nos interesará descomponer los objetos (en este caso representaciones) en sus componentes irreducibles. Tendremos el típico resultado de existencia y unicidad y presentaremos herramientas para el cálculo práctico de una descomposición. Por último, construiremos las representaciones irreducibles del grupo simétrico S_n , que están ligadas a objetos combinatorios.

Abstract: The main goal of this article is to introduce an algebraic application in combinatorics. We will deal with the algebraic group representation theory, used over many branches of mathematics (differential geometry, harmonic analysis, number theory...) or even theoretical physics. We will use it in the context of combinatorics, linking algebraic concepts with combinatorial concepts. This allows to prove some combinatorics results through their algebraic analogues. Specifically, we will use this theory to prove a combinatorial equality.

As in other parts of algebra, it is interesting to decompose the objects (representations) into their irreducible components. We will prove typical results about existence and uniqueness and we will present some tools to decompose representations. Finally, we will construct the irreducible representations of the symmetric group S_n , which are closely related to combinatorial objects.

Palabras clave: representaciones de grupos, grupo simétrico, combinatoria algebraica, tablas de Young, particiones, módulos de Specht.

MSC2010: 05E10, 20C30.

Recibido: 23 de febrero de 2018.

Aceptado: 5 de julio de 2018.

Referencia: CAO LABORA, Gonzalo. «Aplicación en combinatoria de las representaciones de grupos». En: *TEMat*, 2 (2018), págs. 67-83. ISSN: 2530-9633. URL: <https://temat.es/articulo/2018-p67/>.

© Este trabajo se distribuye bajo una licencia Creative Commons Reconocimiento 4.0 Internacional <https://creativecommons.org/licenses/by/4.0/>

1. Introducción

Un problema clásico de la combinatoria es el problema de las particiones. Una partición es una descomposición de un número natural, n , en sumas de números naturales. Por ejemplo, $2 + 1 + 1$ es una posible partición de 4, aunque la forma usual de denotarla sería $(2, 1, 1)$. El problema consiste en contar de cuántas maneras es posible realizar estas particiones, es decir, cuántas particiones tiene el número n . En el caso de $n = 3$, lo podemos descomponer como $(1, 1, 1)$, como $(2, 1)$, o como (3) (descomponerlo en un único sumando también es válido). A la cantidad de particiones la llamamos $p(n)$, de forma que, por ejemplo, $p(3) = 3$. Es importante fijarse en que el orden no importa a la hora de hacer particiones. Como $(2, 1)$ es la misma partición que $(1, 2)$, las podemos ordenar siempre en orden decreciente, que será lo que haremos.

Frobenius [2] en el año 1900 demostró que las particiones están asociadas a unas representaciones (que introduciremos más adelante). Alfred Young [7-17] estudió estas representaciones durante la primera mitad del siglo xx, y se dio cuenta de la importancia de introducir diagramas para codificar las particiones. Un diagrama de Young es una colección de n recuadros, donde en cada fila ponemos la cantidad correspondiente a uno de los números de la partición. Estas filas han de estar ordenadas por tamaño y alineadas a la izquierda. Podemos ver todos los posibles diagramas de Young para $n = 3$ en la figura 1.

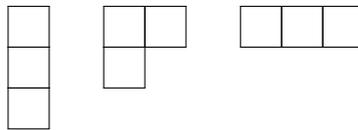


Figura 1: Diagramas de Young para $n = 3$. Se corresponden con las particiones $(1, 1, 1)$, $(2, 1)$ y (3) , respectivamente.

Otros objetos interesantes en combinatoria son las permutaciones. Al conjunto de permutaciones de n elementos se lo llama **grupo simétrico** y se denota por \mathcal{S}_n . Las permutaciones descomponen de forma única en ciclos disjuntos, lo que permite denotarlas a través de ellos. Por ejemplo, la permutación $(123)(46) \in \mathcal{S}_6$ envía el 1 al 2, el 2 al 3 y el 3 al 1. El 4 lo envía al 6 y viceversa, y el 5 lo deja fijo. Una operación interesante entre permutaciones es la conjugación. Dos permutaciones σ y τ se dicen conjugadas si existe $\gamma \in \mathcal{S}_n$ tal que $\gamma^{-1} \circ \sigma \circ \gamma = \tau$. Equivalentemente, $\sigma \circ \gamma = \gamma \circ \tau$. Ser conjugados es una relación de equivalencia, y las clases de equivalencia se denominan clases de conjugación.

Este concepto hace de puente entre particiones y permutaciones. Hay tantas particiones de n como clases de conjugación de \mathcal{S}_n (corolario 11). De hecho, a cada permutación le podemos asociar una partición mirando los tamaños de sus ciclos disjuntos. Por ejemplo, una partición de \mathcal{S}_3 que tenga un 2-ciclo y un 1-ciclo (punto fijo) tiene asociada la partición $(2, 1)$ de $n = 3$. Evidentemente, permutaciones diferentes pueden tener la misma partición asociada. Lo que ocurre es que tienen la misma partición asociada si y solo si son conjugadas. Por lo tanto, las clases de conjugación de \mathcal{S}_n van asociadas de forma natural a las particiones, y en consecuencia, van asociadas también a los diagramas de Young.

Esta relación entre permutaciones y diagramas de Young es la que hace realmente importantes los diagramas de Young. En realidad, estos diagramas ya habían sido introducidos previamente por Ferrers en 1871. La novedad que introdujo Young es la posibilidad rellenarlos con los números del 1 al n (sin repetirlos). Esta idea permite que las permutaciones puedan actuar sobre los diagramas, permutando los números del diagrama. A estos diagramas de Young rellenos con números los llamamos tablas de Young. Si, además, las filas y columnas están ordenadas (de menor a mayor), decimos que son tablas estándar de Young. Por ejemplo, hay 4 tablas estándar de Young para $n = 3$, como se ve en la figura 2. También podemos dejar que las permutaciones actúen sobre las tablas; por ejemplo, cuando (23) actúa sobre la primera tabla de la figura 2, obtenemos la segunda tabla.

Ahora podemos hacer la siguiente observación. De las tres particiones que hay para $n = 3$, una tiene dos tablas estándar; otra, una, y la otra, una. Y ocurre que si sumamos los cuadrados de estos números, $2^2 + 1^2 + 1^2 = 6 = 3!$, obtenemos la cantidad de elementos de \mathcal{S}_n , que es $n!$. Podemos hacer lo mismo para otros valores de n . Para $n = 4$ se obtienen cinco particiones, con dos, tres, tres, una y una tablas estándar, y

1	2
3	

1	3
2	

1
2
3

1	2	3
---	---	---

Figura 2: Tablas estándar de Young para $n = 3$. Para la partición $(2, 1)$ hay dos posibles tablas estándar, mientras para las particiones $(1, 1, 1)$ y (3) solo hay una tabla estándar posible.

vuelve a ocurrir que $2^2 + 3^2 + 3^2 + 1^2 + 1^2 = 24 = 4!$. Con $n = 5$ obtenemos siete particiones con seis, cinco, cinco, cuatro, cuatro, una y una tablas estándar, y tenemos que $6^2 + 5^2 + 5^2 + 4^2 + 4^2 + 1^2 + 1^2 = 120 = 5!$.

La teoría de representaciones aplicada al grupo simétrico nos permitirá probar esta igualdad (corolario 19). Tras introducir las representaciones, utilizaremos sus caracteres para probar que $|\mathcal{S}_n| = \sum n_i^2$. Los n_i , que son la cantidad de tablas estándar, coincidirán con las dimensiones de unas representaciones, cada una asociada a una partición (o diagrama de Young). La construcción explícita de estas representaciones nos permitirá ver que las dimensiones n_i se corresponden a la cantidad de tablas estándar.

2. Representaciones lineales de grupos

Un grupo consiste en un conjunto G con una operación \cdot tal que dados dos elementos $a, b \in G$, nos devuelve $a \cdot b \in G$. Esta operación ha de ser asociativa, tener elemento neutro y todo elemento ha de tener inverso. Por ejemplo, las permutaciones con la composición son un grupo, que es el grupo simétrico. Otro ejemplo es el conjunto de matrices invertibles $n \times n$ sobre \mathbb{C} , que es un grupo con el producto de matrices. Este grupo se denota por $GL_n(\mathbb{C})$, y también se puede pensar como aplicaciones lineales invertibles de V en sí mismo (donde V es un \mathbb{C} -espacio vectorial de dimensión n). La idea de una representación del grupo G consiste en trasladar la estructura de G a este grupo concreto: $GL_n(\mathbb{C})$. Si utilizamos lenguaje de aplicaciones en lugar de lenguaje matricial, el grupo se denotará por $GL(V)$. Hablaremos de matrices o aplicaciones lineales indistintamente, según sea conveniente. En particular, omitiremos el \circ de la composición, ya que desde el punto de vista matricial es simplemente un producto.

Definición 1. Una **representación** de un grupo G en un espacio vectorial V consiste en una aplicación $\rho: G \rightarrow GL(V)$ tal que

$$\rho_{ab} = \rho_a \rho_b \quad \forall a, b \in G. \quad \blacktriangleleft$$

Como vemos, la matriz asociada al elemento ab es el producto de la de a con la de b . En lenguaje de aplicaciones, la aplicación lineal de ab es la de b compuesta con la de a . En un contexto general de teoría de grupos, este tipo de aplicaciones entre grupos se denomina **homomorfismo de grupos** (la particularidad de este caso es que el espacio de llegada es $GL(V)$). Aunque esta definición es totalmente general, nosotros consideraremos grupos G finitos y espacios vectoriales V de dimensión finita y sobre \mathbb{C} .

Observación 1. Tomando $b = 1$ en la definición vemos que $\rho_1 = \text{Id}$, puesto que $\rho_a = \rho_a \rho_1$. Tomando $b = a^{-1}$ vemos que $\rho_{a^{-1}} = \rho_a^{-1}$, puesto que $\text{Id} = \rho_1 = \rho_a \rho_{a^{-1}}$. \blacktriangleleft

En todo grupo finito ocurre que existe algún valor k tal que $a^k = 1$ (de hecho, $k = |G|$ lo cumple). Como consecuencia, ρ_a compuesta k veces consigo misma será la identidad. Los ejemplos más sencillos de este tipo de aplicaciones tienen un fuerte significado geométrico. Las simetrías, por ejemplo, lo cumplen para $k = 2$. Movimientos directos, como rotaciones de $360^\circ/k$, también lo cumplen. Nuestras representaciones serán colecciones de aplicaciones de este tipo (una por cada $a \in G$).

Ejemplo 1. Sea V un espacio vectorial y sea G un grupo. Si a cada $a \in G$ le asociamos la identidad, tenemos una representación $\rho_a = \text{Id}$. En el caso de que V sea de dimensión 1 la llamaremos **representación trivial**. \blacktriangleleft

Ejemplo 2. Consideremos las permutaciones de tres elementos, \mathcal{S}_3 . Hay seis de ellas: la identidad, tres trasposiciones y dos 3-ciclos. Podemos representar este grupo en el plano \mathbb{R}^2 , como vemos en la figura 3.

Los dos 3-ciclos son (123) y (132) y van asociados a rotaciones de 120° y -120° . Las trasposiciones (12), (13) y (23) son simetrías; por ejemplo, la (12) es la que intercambia los puntos 1 y 2. Aunque el dibujo está en \mathbb{R}^2 , esto también es una representación sobre \mathbb{C}^2 , porque las matrices 2×2 reales que nos dan los automorfismos son también matrices 2×2 complejas. A esta representación sobre \mathbb{C}^2 se la denomina representación **estándar**. Esta representación viene dada en forma matricial de la siguiente manera:

$$\begin{aligned} \rho_{id} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \rho_{(123)} &= \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{pmatrix} & \rho_{(132)} &= \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix} \\ \rho_{(23)} &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} & \rho_{(12)} &= \begin{pmatrix} 1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix} & \rho_{(13)} &= \begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{pmatrix} \end{aligned}$$

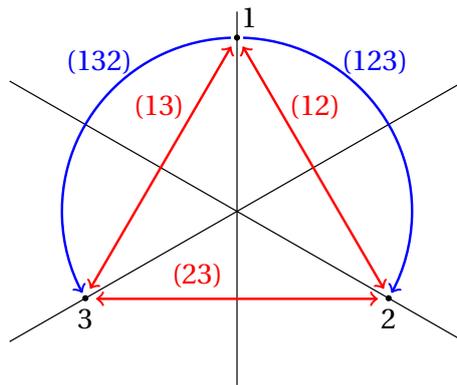


Figura 3: Representación esquemática de los automorfismos de la representación estándar de S_3 sobre \mathbb{R}^2 . En rojo, simetrías (corresponden a trasposiciones) y en azul, rotaciones (corresponden a 3-ciclos). Ver ejemplo 2.

Ejemplo 3. Tomemos el grupo simétrico $G = S_n$ y sea $a \in S_n$ una permutación. Como las permutaciones descomponen en ciclos y los ciclos en trasposiciones, la podemos descomponer en trasposiciones (no de forma única). Si a descompone en una cantidad par de trasposiciones decimos que a es par y que tiene signo $\varepsilon(a) = 1$. Si, por el contrario, descompone en una cantidad impar de trasposiciones, a será impar y su signo será $\varepsilon(a) = -1$. Aunque la descomposición no es única, la paridad de la cantidad de trasposiciones es siempre la misma, de forma que el signo está bien definido. Además, el signo es multiplicativo, es decir, $\varepsilon(a)\varepsilon(b) = \varepsilon(ab)$. De todo esto se deduce que $\rho_a = \varepsilon(a)\text{Id}$ es una representación, para cualquier espacio vectorial V . En el caso de $\dim(V) = 1$ la llamamos representación **alternada**.

Ejemplo 4. Consideremos un \mathbb{C} -espacio vectorial V de dimensión igual a $|G|$. Indexemos los vectores de la base con elementos de G , es decir $\mathcal{B} = \{e_a\}_{a \in G}$. La representación **regular** de G asocia a cada $b \in G$ el automorfismo definido por

$$\rho_b(e_a) = e_{ba}.$$

Como hemos definido ρ_b sobre la base \mathcal{B} , queda completamente definida. Esta representación será de especial importancia, porque guarda toda la información de G como grupo.

Cuando trabajamos con matrices de aplicaciones lineales, suele ser interesante diagonalizarlas, es decir, encontrar una matriz semejante en forma diagonal. Esto lo hacemos a través de los autovectores, que definen rectas invariantes de la aplicación. En el caso de representaciones, tendríamos que diagonalizar simultáneamente todas las matrices ρ_a con $a \in G$. Esto es más complicado, y, en general, no será posible. Aún así, podemos seguir estudiando subespacios invariantes (que no sean necesariamente rectas), y también podemos descomponer ρ a través de sus subespacios invariantes. Para realizar la descomposición queremos que, si W es un subespacio invariante, exista otro subespacio suplementario W^c , también invariante, que nos permita descomponer ρ entre W y W^c . Ahora formalizaremos esta idea.

Definición 2. Decimos que $W \subset V$ es un subespacio **invariante** de ρ si $\rho_a(W) = W$, para todo $a \in G$. Esto es decir que W es subespacio invariante de cada ρ_a como automorfismo.

Definición 3. Decimos que una representación es **irreducible** si no existe ningún subespacio $W \subset V$ invariante que no sea trivial (es decir, $W \neq V$, $W \neq \{0\}$). ◀

Definición 4. Dadas dos representaciones $\rho: G \rightarrow \text{GL}(V_1)$, $\eta: G \rightarrow \text{GL}(V_2)$, definimos su **suma directa** $\rho \oplus \eta: G \rightarrow \text{GL}(V_1 \oplus V_2)$ como la nueva representación

$$(\rho \oplus \eta)_a(u + v) = \rho_a(u) + \eta_a(v) \quad \forall u \in V_1, v \in V_2. \quad \blacktriangleleft$$

Teorema 1 (Maschke). *Toda representación $\rho: G \rightarrow \text{GL}(V)$ se puede descomponer como*

$$\rho = \rho^{(1)} \oplus \rho^{(2)} \oplus \dots \oplus \rho^{(k)},$$

donde todas las $\rho^{(i)}$ son representaciones irreducibles.

Demostración. Si ρ no es irreducible, existe algún $W \subset V$ invariante. Escojámoslo lo más pequeño posible, es decir, que no tenga ningún subespacio invariante dentro. Como W es invariante, $\rho|_W$ es una representación de W (restringimos cada ρ_a al subespacio W) y, como W es lo más pequeño posible, es irreducible. Ahora buscamos un subespacio invariante suplementario W^c para escribir $\rho = \rho|_W \oplus \rho|_{W^c}$. Nos basta con que W^c sea invariante porque, aunque no sea irreducible, podremos aplicarle el mismo razonamiento sucesivamente, hasta obtener solo subespacios irreducibles.

Hemos reducido la demostración a hallar un subespacio W^c , suplementario a W e invariante. Desde una intuición geométrica, nos gustaría coger una especie de W ortogonal, pero no hemos definido ningún producto escalar. Asumamos un producto escalar $\langle \cdot, \cdot \rangle$ y cojamos $W^c = W^\perp$, que es el conjunto de vectores v tales que $\langle v, u \rangle = 0$ para todo $u \in W$. Sea $v \in W^\perp$. Si tuviéramos que $\langle \rho_a(v), \rho_a(u) \rangle = \langle v, u \rangle$ habríamos acabado, porque eso es 0 para todo $u \in W$ y, como $\rho_a(u) \in W = \rho_a(W)$ por ser W invariante, se tendría que $\rho_a(v) \in W^\perp$. La existencia de un producto escalar con $\langle \rho_a(v), \rho_a(u) \rangle = \langle v, u \rangle$ nos la garantiza el lema 2 que presentamos a continuación. ■

Lema 2. *Sea ρ una representación en un espacio vectorial V . Existe un producto escalar $\langle \cdot, \cdot \rangle$ de V tal que*

$$\langle \rho_a(v), \rho_a(u) \rangle = \langle v, u \rangle \quad \forall a \in G, \forall u, v \in V.$$

Demostración. En primer lugar consideremos un producto escalar cualquiera $[\cdot, \cdot]$ (producto respecto de una base cualquiera). Definimos a partir de él un nuevo producto

$$\langle v, u \rangle = \frac{1}{|G|} \sum_{b \in G} [\rho_b(v), \rho_b(u)],$$

es decir, hacemos la media de $[\rho_b(v), \rho_b(u)]$ haciendo que b varíe sobre G . Este nuevo producto cumple la propiedad deseada porque para todo $c \in G$ tenemos que

$$\langle \rho_c(v), \rho_c(u) \rangle = \frac{1}{|G|} \sum_{b \in G} [\rho_{bc}(v), \rho_{bc}(u)] = \frac{1}{|G|} \sum_{a \in G} [\rho_a(v), \rho_a(u)] = \langle v, u \rangle,$$

donde hemos definido $a = bc$. Como b recorre todo G y c es fijo, $a = bc$ variará por todo G . Además, el hecho de que $\langle \cdot, \cdot \rangle$ sea un producto escalar (bilineal, definido positivo y hermítico) se deriva directamente de que $[\cdot, \cdot]$ lo sea. ■

Ejemplo 5. Consideremos $V = \mathbb{C}^3$ con una base $\mathcal{B} = \{e_1, e_2, e_3\}$ y el grupo simétrico $G = \mathcal{S}_3$. Sea ρ_a el automorfismo que lleva e_1 a $e_{a(1)}$, lleva e_2 a $e_{a(2)}$ y lleva también e_3 a $e_{a(3)}$. Dichas ρ forman una representación, que puede parecer la regular, pero no lo es (la regular sería de dimensión $|\mathcal{S}_3| = 6$). Podemos ver esta representación esquemáticamente en la figura 4 (viendo únicamente la parte real, es decir, el corte en \mathbb{R}^3). Hay dos subespacios invariantes: la recta $\langle(1, 1, 1)\rangle$ y el plano perpendicular $x_1 + x_2 + x_3 = 0$. La representación restringida a la recta $\langle(1, 1, 1)\rangle$ es la trivial del ejemplo 1. La representación restringida al plano $x_1 + x_2 + x_3 = 0$ es la representación estándar que introdujimos en el ejemplo 2. ◀

Ejercicio 6. Se puede ver que la representación regular del ejemplo 4 para el grupo simétrico \mathcal{S}_n contiene tanto a la representación trivial como a la representación alternada (de los ejemplos 1 y 3). ◀

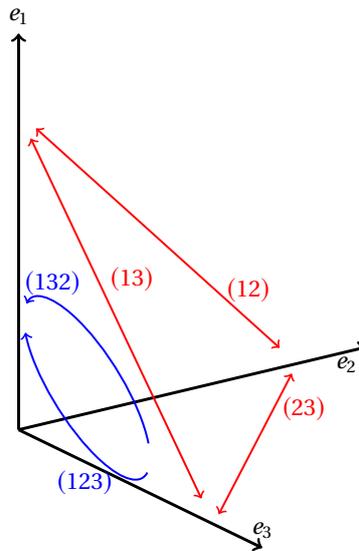


Figura 4: Dibujo esquemático de automorfismos de una representación sobre \mathbb{R}^3 . En rojo, simetrías (corresponden a trasposiciones) y en azul, rotaciones (corresponden a 3-ciclos).

Ejemplo 7. Es importante ver que la descomposición dada en el teorema 1 no es necesariamente única. Cojamos una representación de dimensión $n > 1$, donde $\rho_a = \text{Id}$. Cualquier recta es invariante, por lo que hay infinitas posibilidades para descomponer en n rectas invariantes. Más adelante veremos que lo que sí son únicas son las representaciones que obtenemos en estos subespacios. Por ejemplo, aquí obtenemos siempre n representaciones triviales, independientemente de las rectas escogidas. ◀

Aunque se desvíe de nuestro objetivo, vale la pena comentar que hemos utilizado de forma fundamental la finitud de G para promediar y obtener nuestro producto en el lema 2. Esto permite descomponer ρ como suma de irreducibles, y este resultado no lo tendremos en casos más generales (G infinito). No obstante, si tenemos una integral razonable desde el punto de vista de G , podemos tomar promedios con integrales y todo funciona exactamente igual. Para ello es necesario exigir otras propiedades como, por ejemplo, que G sea un grupo topológico localmente compacto. Para más detalles se puede consultar el libro de Kowalski [4], en concreto, la primera parte del teorema 5.2.11.

3. El lema de Schur

Pensando en forma matricial, el teorema 1 dice que, en una cierta base, todas las matrices ρ_a están descompuestas en bloques. Estos bloques vienen definidos por los subespacios invariantes. Por tanto, lo lógico será estudiar la representación en esta base, donde podemos limitarnos a estudiar cada una de las representaciones irreducibles que componen ρ . Para ello, pasaremos por estudiar sus relaciones.

La relación natural entre dos representaciones ρ y η es una aplicación lineal g tal que $\rho_a g = g \eta_a$ para todo $a \in G$. A dicha g la llamaremos morfismo de ρ a η . En el caso de que g sea biyectiva, será un isomorfismo de ρ a η , y recuperamos el concepto de que ρ y η sean equivalentes (isomorfas). En el lenguaje de teoría de categorías esta g no es más que una transformación natural entre ρ y η , vistos como funtores de G a $\text{Vec}_{\mathbb{C}}$. Existe un resultado muy importante sobre estos morfismos de representaciones.

Teorema 3 (Lema de Schur, [6]). Sean $\rho: G \rightarrow \text{GL}(V_1), \eta: G \rightarrow \text{GL}(V_2)$ dos representaciones irreducibles. Entonces tenemos que:

- Si g es morfismo de ρ a η , o bien g es isomorfismo o bien $g \equiv 0$.
- Si h es morfismo de ρ a ρ (endomorfismo de ρ), entonces es una homotecia $h = c \cdot \text{Id}$.

Demostración. Empecemos por el primer apartado. Al ser g morfismo, $\rho_a g = g \eta_a$, lo cual implica que $\ker(g)$ e $\text{Im}(g)$ son subespacios invariantes de η_a y ρ_a , respectivamente. Pero como ρ y η son irreducibles, sus subespacios invariantes son $\{0\}$ o el total. Si el núcleo es 0 y la imagen es el total, estamos ante un isomorfismo (y, por tanto, ρ y η serían equivalentes). En cualquier otro caso la aplicación es nula.

Situémonos ahora en la segunda parte, donde h es endomorfismo de ρ . Observemos que si h cumple que $h\rho_a = \rho_a h$, entonces $\hat{h} = h - c \cdot \text{Id}$ también cumple que $\hat{h}\rho_a = \rho_a \hat{h}$. Como estamos en \mathbb{C} , siempre podemos escoger c para que \hat{h} tenga un autovalor nulo (tomando c un autovalor de h). Pero entonces \hat{h} no es isomorfismo y, por la primera parte, $\hat{h} = 0$. Es decir, $h = c \cdot \text{Id}$, como queríamos. ■

Ejemplo 8. Consideremos una representación ρ no irreducible en V y sea h la proyección ortogonal (según el producto escalar del lema 2) sobre uno de los subespacios invariantes W . Descomponiendo un v cualquiera entre W y W^\perp y teniendo en cuenta que W^\perp también es invariante, tenemos que

$$h(\rho_a(v)) = h(\rho_a(w + w^\perp)) = h(\rho_a(w)) + h(\rho_a(w^\perp)) = \rho_a(w) + 0 = \rho_a(h(v)).$$

De esta forma, h es un endomorfismo de ρ y, como no es $c \cdot \text{Id}$, no cumple el teorema 3. Esto ocurre porque ρ no es irreducible; de hecho, esto prueba que ρ es irreducible si y solo si cumple la segunda parte del teorema 3. ◀

Observación 2. Sean ρ y η las representaciones del teorema 3 (representaciones irreducibles cualesquiera) y sea $g: V_1 \rightarrow V_2$ una aplicación lineal cualquiera. Si consideramos \hat{g} definida por

$$\hat{g} = \sum_{a \in G} \eta_a^{-1} g \rho_a,$$

se cumple que \hat{g} está bajo las hipótesis del teorema 3. Es decir, $\eta_b^{-1} \hat{g} \rho_b = \hat{g}$ para todo $b \in G$. ◀

Esto nos da mucha información, porque escogiendo una g cualquiera, tendremos que \hat{g} será 0 si ρ y η no son equivalentes. Por otro lado, si $\rho = \eta$, tendremos que \hat{g} será una homotecia. Escribiendo esto en forma matricial podemos concluir información sobre las trazas de las matrices ρ_a y η_a . El desarrollo formal es algo pesado pero no especialmente difícil. El lector interesado puede intentarlo por su cuenta o consultar el libro de Serre [6].

Proposición 4. Si ρ y η son dos representaciones irreducibles no equivalentes de G , entonces

$$\sum_{a \in G} \overline{\text{Tr}(\eta_a)} \text{Tr}(\rho_a) = 0.$$

Proposición 5. Si ρ es una representación irreducible de G , entonces

$$\sum_{a \in G} \overline{\text{Tr}(\rho_a)} \text{Tr}(\rho_a) = |G|.$$

4. Caracteres

Las proposiciones 4 y 5 indican un sentido de ortonormalidad entre las funciones $\text{Tr}(\rho_a)$ (siendo a el argumento). Para seguir este camino, definimos estas funciones y el producto adecuado.

Definición 5. Dada una representación $\rho: G \rightarrow \text{GL}(V)$, su carácter será la función $\phi: G \rightarrow \mathbb{C}$ dada por $\phi(a) = \text{Tr}(\rho_a)$. ◀

Definición 6. Dadas dos funciones $\phi, \psi: G \rightarrow \mathbb{C}$, definimos su producto escalar como

$$(\phi|\psi) = \frac{1}{|G|} \sum_{a \in G} \overline{\phi(a)} \psi(a). \quad \blacktriangleleft$$

Observación 3. Las proposiciones 4 y 5 hacen que los caracteres de representaciones irreducibles sean ortonormales respecto del producto que acabamos de definir. ◀

Al ser los caracteres ortogonales, una pregunta natural es qué subespacio vectorial generan (pues serán base ortogonal de este subespacio). Por el hecho de ser trazas de representaciones cumplirán $\phi(aba^{-1}) = \phi(b)$, ya que $\text{Tr}(\rho_a \rho_b \rho_a^{-1}) = \text{Tr}(\rho_b)$ al ser la traza un invariante en álgebra lineal. Como ya comentamos en la introducción, al elemento aba^{-1} se lo llama conjugado de b . Vemos que dos elementos conjugados de G tienen la misma imagen por ϕ .

Definición 7. La **clase de conjugación** de un elemento $b \in G$ son todos los elementos de G de la forma aba^{-1} . Una función $\phi: G \rightarrow \mathbb{C}$ que cumple que

$$\phi(aba^{-1}) = \phi(b) \quad \forall a, b \in G$$

se denomina **función de clase**. Es decir, una función de clase será aquella que sea constante sobre cada clase de conjugación. En particular, los caracteres son funciones de clase. ◀

Ejemplo 9. Consideremos la representación regular $\rho: G \rightarrow \text{GL}(V)$ del ejemplo 4. Su carácter $\phi(a) = \text{Tr}(\rho_a)$ será 0 para $a \neq 1$ (ya que cada vector de la base e_b lo envía a uno diferente e_{ab}). Por el contrario, para $a = 1$ tenemos que $\phi(1) = |G|$ (ya que deja fija toda la base). Por tanto, $\phi(a) = |G|\delta_1(a)$, donde δ_1 es una función que vale 1 en el elemento neutro de G y 0 en el resto de elementos. ◀

Ejemplo 10. Tomemos $G = S_3$. Tiene 3 clases de conjugación: la identidad, las trasposiciones y los 3-ciclos. En el cuadro 1 podemos ver los valores que toma el carácter en cada clase de conjugación. Lo hemos hecho para la representación trivial (ejemplo 1), la representación alternada (ejemplo 3) y para la representación estándar (ejemplo 2). El cálculo de ϕ para la trivial y alternada es trivial y para la estándar lo podemos hacer tomando trazas en las matrices del ejemplo 2. Observamos que ϕ es constante sobre cada clase de conjugación. Además, como todas son irreducibles, los caracteres han de ser ortonormales, y así es. ◀

Cuadro 1: Caracteres de las representaciones irreducibles de S_3 .

Representación	id	(12)	(13)	(23)	(123)	(132)
Trivial	1	1	1	1	1	1
Alternada	1	-1	-1	-1	1	1
Estándar	2	0	0	0	-1	-1

Teorema 6. Las funciones de clase forman un espacio vectorial. Los caracteres de las representaciones irreducibles de un grupo G sobre \mathbb{C} forman una base ortonormal del espacio de funciones de clase.

Demostración. Es trivial que las funciones de clase son un espacio vectorial con la suma de funciones y el producto por escalar. Ya hemos visto que los caracteres de representaciones irreducibles son ortonormales, y falta ver que generan todo el espacio de funciones de clase. Supongamos que generan el espacio $W \subset V$ dentro del espacio V de funciones de clase. Queremos probar que $W = V$, y para ello veremos que $W^\perp = \{0\}$. Sean $\phi^{(i)}$ los caracteres de representaciones irreducibles y sea ψ ortogonal a todas ellas. Veamos que $\psi = 0$. Para eso, utilizaremos la representación regular del ejemplo 4. Sea ρ la representación regular. Por el teorema 1, ρ descompone en las representaciones irreducibles $\rho^{(j)}$, de caracteres $\phi^{(j)}$ (puede haberlas repetidas). Por hipótesis, $(\psi|\phi^{(j)}) = 0$. Consideremos la función

$$f^{(j)}(x) = \sum_{a \in G} \overline{\psi(a)} \rho_a^{(j)}(x).$$

Por un lado, tenemos que $\text{Tr}(f^{(j)}) = (\psi|\phi^{(j)}) = 0$. Por otro lado, $f^{(j)}$ es un morfismo de la representación irreducible $\rho^{(j)}$, ya que

$$\rho_b^{(j)} f^{(j)} \rho_b^{(j)-1} = \sum_{a \in G} \overline{\psi(a)} \rho_{bab^{-1}}^{(j)} = \sum_{c \in G} \overline{\psi(b^{-1}cb)} \rho_c^{(j)} = \sum_{c \in G} \overline{\psi(c)} \rho_c^{(j)} = f^{(j)},$$

donde hemos tomado $c = bab^{-1}$ y usado que ϕ es función de clase. Como $\rho^{(j)}$ es irreducible, el teorema 3 afirma que $f^{(j)} = k \cdot \text{Id}$, pero como $\text{Tr}(f^{(j)}) = 0$, necesariamente $f^{(j)} = 0$. Ahora bien, si definimos f para la representación regular como

$$f(x) = \sum_{a \in G} \overline{\psi(a)} \rho_a(x),$$

está claro que f es suma de las $f^{(j)}$ (ya que ρ es suma de las $\rho^{(j)}$). Como todas las $f^{(j)}$ son nulas, $f \equiv 0$. En particular,

$$0 = f(e_1) = \sum_{a \in G} \overline{\psi(a)} \rho_a(e_1) = \sum_{a \in G} \overline{\psi(a)} e_a.$$

Como los e_a son una base, cada coeficiente conjugado es $\overline{\psi(a)} = 0$ y, por tanto, $\psi \equiv 0$. Como cualquier función de clase ψ ortogonal a las $\phi^{(j)}$ es nula, las $\phi^{(j)}$ generan todo el espacio de funciones de clase. ■

Corolario 7. *La representación regular contiene todas las representaciones irreducibles.*

El corolario se deriva directamente de la demostración del teorema, porque solo hemos usado las representaciones irreducibles contenidas en la regular.

Corolario 8. *Sean $\rho^{(i)}$ las representaciones irreducibles, sea η una representación cualquiera, y sea $\eta = n_1 \rho^{(1)} \oplus \dots \oplus n_k \rho^{(k)}$ su descomposición por el teorema 1 (donde n_i significa que cada $\rho^{(i)}$ aparece n_i veces). Estos n_i se pueden calcular mediante $n_i = (\varphi | \phi^{(i)})$, donde φ es el carácter de η . Además, esto implica la unicidad de la descomposición del teorema 1, salvo isomorfismo.*

Demostración. Para ver que $n_i = (\varphi | \phi^{(i)})$, simplemente ejecutamos el producto y usamos ortonormalidad:

$$(\varphi | \phi^{(i)}) = (n_1 \phi^{(1)} + \dots + n_k \phi^{(k)} | \phi^{(i)}) = n_1 (\phi^{(1)} | \phi^{(i)}) + \dots + n_k (\phi^{(k)} | \phi^{(i)}) = n_i.$$

Esto es válido para cualquier descomposición de η . Por tanto, todas las descomposiciones consisten en repetir n_i representaciones equivalentes a $\rho^{(i)}$. Es decir, la única descomposición de η es $n_1 \rho^{(1)} \oplus \dots \oplus n_k \rho^{(k)}$, salvo isomorfismo. ■

Corolario 9. *Hay tantas representaciones irreducibles de G como clases de conjugación.*

Demostración. De hecho, si V es el espacio de funciones de clase, tenemos que

$$\# \text{ representaciones irreducibles de } G = \dim(V) = \# \text{ clases de conjugación de } G.$$

La primera igualdad se deduce de que las $\phi^{(i)}$ son una base de V , y hay tantas como representaciones irreducibles. La segunda igualdad proviene de que los elementos de V son exactamente las funciones que son constantes sobre cada clase de conjugación. De esa manera, una posible base de V son las funciones que valen 1 en una clase de conjugación y 0 en el resto. Evidentemente, hay tantas funciones de ese tipo como clases de conjugación. ■

Corolario 10. *Supongamos que cada $\rho^{(i)}$ aparece n_i veces en la representación regular ρ . Entonces tenemos la fórmula*

$$|G| = \sum_{i=1}^k n_i^2.$$

Demostración. Sea ϕ el carácter de ρ . Calculemos $(\phi | \phi)$ de dos maneras. Tenemos que

$$(\phi | \phi) = (n_1 \phi^{(1)} + \dots + n_k \phi^{(k)} | n_1 \phi^{(1)} + \dots + n_k \phi^{(k)}) = \sum_{i=1}^k n_i^2.$$

Pero por otro lado, al ser ρ la representación regular, tenemos que $\text{Tr}(\rho_a) = \delta_1 |G|$ (ejemplo 9). De ahí deducimos que

$$(\phi | \phi) = \frac{1}{|G|} \sum_{a \in G} \overline{\text{Tr}(\rho_a)} \text{Tr}(\rho_a) = \frac{1}{|G|} \sum_{a \in G} \delta_1 |G|^2 = \frac{1}{|G|} |G|^2 = |G|.$$

Como ambos resultados de $(\phi | \phi)$ han de ser iguales, tenemos la fórmula deseada. ■

Ejemplo 11. Continuemos el ejemplo 10. Teníamos tres representaciones irreducibles de \mathcal{S}_3 (la trivial, la alternada y la estándar). Por el corolario 9 sabemos que estas tres ya son todas (ya que hay tres clases de conjugación de \mathcal{S}_3 : la identidad, la de trasposiciones y la de 3-ciclos). Tenemos sus caracteres $\phi^{(i)}$ en el cuadro 1 y, por otro lado, tenemos el carácter $\phi = |\mathcal{S}_3| \delta_1$ de la representación regular (ejemplo 9).

El corolario 8 nos permite decir que la representación regular descompone como $\rho = n_1 \rho^{(1)} \oplus n_2 \rho^{(2)} \oplus n_3 \rho^{(3)}$, donde cada n_i viene dado por $(\phi|\phi^{(i)})$. Usando que $\phi = |\mathcal{S}_3| \delta_1$ y recordando que δ_1 es nula salvo para el neutro de \mathcal{S}_3 obtenemos

$$n_i = (\phi|\phi^{(i)}) = \frac{1}{|\mathcal{S}_3|} \sum_{a \in \mathcal{S}_3} |G|\overline{\delta_1(a)}\phi^{(i)}(a) = \phi^{(i)}(id).$$

Mirando los resultados $\phi^{(i)}(id)$ en el cuadro 1 vemos que tanto la representación trivial como la alternada tienen $n_1 = n_2 = 1$, mientras que la estándar tiene $n_3 = 2$. Por un lado comprobamos el corolario 7, porque se cumple que todo $n_i > 0$, estando cualquier representación dentro de la regular al menos una vez. Por otro lado, comprobamos también el corolario 10, ya que $n_1^2 + n_2^2 + n_3^2 = 1 + 1 + 4 = 6 = |\mathcal{S}_3|$. ◀

Ejemplo 12. En el ejemplo 5 tenemos una representación tridimensional tal que ρ_a envía e_i a $e_{a(i)}$. Claramente, su carácter φ valdrá 3 en la identidad (deja fija la base), 1 en las trasposiciones (deja un elemento de la base fijo) y 0 en los 3-ciclos (no dejan ninguno fijo). Esto permite descomponerla usando la ecuación $n_i = (\varphi|\phi^{(i)})$ del corolario 8. En concreto, siendo i la identidad, t una transposición y c un ciclo, tenemos que

$$\begin{aligned} n_1 &= \frac{1}{6} \left(\overline{\varphi(i)}\phi^{(1)}(i) + 3\overline{\varphi(t)}\phi^{(1)}(t) + 2\overline{\varphi(c)}\phi^{(1)}(c) \right) = \frac{3 \cdot 1 + 3 \cdot 1 \cdot 1 + 2 \cdot 0 \cdot 1}{6} = 1, \\ n_2 &= \frac{1}{6} \left(\overline{\varphi(i)}\phi^{(2)}(i) + 3\overline{\varphi(t)}\phi^{(2)}(t) + 2\overline{\varphi(c)}\phi^{(2)}(c) \right) = \frac{3 \cdot 1 + 3 \cdot 1 \cdot (-1) + 2 \cdot 0 \cdot 1}{6} = 0, \\ n_3 &= \frac{1}{6} \left(\overline{\varphi(i)}\phi^{(3)}(i) + 3\overline{\varphi(t)}\phi^{(3)}(t) + 2\overline{\varphi(c)}\phi^{(3)}(c) \right) = \frac{3 \cdot 2 + 3 \cdot 1 \cdot 0 + 2 \cdot 0 \cdot \frac{-1}{2}}{6} = 1. \end{aligned}$$

Como ya habíamos visto en el ejemplo 5, esta representación descompone en la trivial ($n_1 = 1$) y la estándar ($n_3 = 1$) sin contener ninguna representación alternada ($n_2 = 0$). ◀

5. El caso del grupo simétrico

Como ya comentamos en la introducción, las clases de conjugación de \mathcal{S}_n están asociadas con las particiones de n , de forma que hay $p(n)$ clases de conjugación de \mathcal{S}_n . Recordemos que a la permutación $a \in \mathcal{S}_n$ le podíamos asociar la partición de n que consiste en los tamaños de los ciclos disjuntos en los que descompone a .

Ejercicio 13. Probar que dos permutaciones $a, b \in \mathcal{S}_n$ son conjugadas si y solo si sus ciclos son de los mismos tamaños. ◀

Corolario 11. *Del ejercicio anterior deducimos que hay $p(n)$ clases de conjugación de \mathcal{S}_n .*

Demostración. Por el ejercicio anterior, hay tantas clases de conjugación como posibles permutaciones de \mathcal{S}_n con tamaños de sus ciclos diferentes. Como la suma de tamaños de los ciclos es n , hay exactamente $p(n)$ posibilidades para escoger estos tamaños. ■

De esta manera, cada partición corresponderá a una única clase de conjugación de \mathcal{S}_n y viceversa. Por ejemplo, la clase de conjugación de los c -ciclos va a asociada a la partición $(c, 1, 1, \dots, 1)$. Cada clase de conjugación corresponde a una única representación irreducible por el corolario 9. Uniendo ambas cosas, sabemos que habrá una representación irreducible por cada partición de n , y nuestro objetivo será construirla. Sea λ una partición de n . Lo primero que necesitamos es un espacio vectorial, y este espacio nos lo darán las tablas de Young, de las que hablamos en la introducción. Recordemos que una tabla de Young consiste en un diagrama de recuadros rellenos con los números del 1 al n . La forma del diagrama codifica una partición de n .

También nos será útil considerar tablas donde no nos importe el orden de números en las filas, a las que llamaremos tabloides. Podemos ver estos tabloides como un conjunto cociente de las tablas respecto a una relación de equivalencia \sim . La relación \sim vendría definida por $T \sim S$ si y solo si las filas de T son las mismas que las de S , con la posibilidad de que cada fila esté reordenada. Al tabloide que se obtiene de la tabla T lo denotamos por $\{T\}$, y es la clase de equivalencia de T respecto a \sim .

Definición 8. Denotaremos por V^λ al \mathbb{C} -espacio vectorial libre generado por los tabloides. Es decir, tomaremos \mathbb{C}^m , donde m es la cantidad de tabloides, y denotaremos por $\{T_i\}$ a los elementos de la base, donde $\{T_i\}$ puede ser cualquier λ -tabloide (tabloide con la forma de la partición λ). ◀

Definición 9. Tenemos una representación de \mathcal{S}_n en cada V^λ , simplemente dejando que cada $a \in \mathcal{S}_n$ actúe en cada tabloide, permutando los números de su interior. Dicha representación la denotaremos por ρ (aunque depende de λ) y viene dada por

$$\rho_a(c_1\{T_1\} + \dots + c_k\{T_k\}) = c_1\rho_a\{T_1\} + \dots + c_k\rho_a\{T_k\},$$

donde $\rho_a\{T_i\}$ consiste simplemente en dejar que a permute los números del 1 al n que hay en la tabla T_i . Esto es lo mismo que decir que permute los elementos del tabloide $\{T_i\}$ correspondiente. ◀

Ejemplo 14. Consideremos $n = 3$ y $\lambda = (2, 1)$. Tenemos tres tabloides de Young, que podemos ver en la figura 5 (en los tabloides se omiten las líneas verticales, indicando así que no hay orden por filas). Por tanto $V = \mathbb{C}^3$. Observemos que $\rho_{(23)}\{T_1\} = \{T_1\}$, por lo que existen permutaciones no triviales que fijan un tabloide. También tendríamos, por ejemplo, que $\rho_{(123)}\{T_1\} = \{T_2\}$, o también que $\rho_{(13)}\{T_1\} = \{T_3\}$. Si comprobamos cómo actúa cada ρ_a sobre cada $\{T_i\}$ veremos que esta representación es exactamente igual a la del ejemplo 5 (llamando T_i a lo que antes era e_i). ◀

$$\{T_1\} = \begin{array}{|c|c|} \hline 2 & 3 \\ \hline 1 & \\ \hline \end{array} \quad \{T_2\} = \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & \\ \hline \end{array} \quad \{T_3\} = \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & \\ \hline \end{array}$$

Figura 5: Tabloides de Young de forma $\lambda = (2, 1)$.

Ejemplo 15. Consideremos n cualquiera y $\lambda = (n)$. Como todos los números están en la misma fila, hay un único tabloide de Young y toda ρ_a lo deja fijo, de forma que la representación es la trivial unidimensional. ◀

Ejemplo 16. Consideremos n cualquiera y $\lambda = (1, 1, \dots, 1)$. Como las filas son de un elemento, los tabloides son lo mismo que las tablas, y tenemos $n!$ tabloides. Asociemos a cada tabloide $\{T_a\}$ la permutación $a \in \mathcal{S}_n$ que toma como $a(i)$ el número de la fila i -ésima de T_a . De esta forma, si $\{T_a\}$ tiene asociada $a \in \mathcal{S}_n$, ocurre que $\rho_b\{T_a\}$ tiene asociada ba . Por lo tanto, esta representación es la regular, utilizando $\{T_a\}$ como elementos de la base, en vez de e_a . ◀

Ejercicio 17. Para $n = 3$ hay tres posibles particiones: $(1, 1, 1)$, $(2, 1)$ y (3) . Aplicando los ejemplos 14, 15 y 16 a $n = 3$, vemos que solo $\lambda = (3)$ nos da una representación irreducible, que es la trivial. Se puede probar esto en general, es decir, que solo $\lambda = (n)$ da representaciones irreducibles. Para ello puede ser útil considerar el carácter φ de la representación y ver cómo se traduce la irreducibilidad en términos de φ . ◀

Pese a no ser irreducibles, nuestras representaciones son útiles, porque contienen la representación irreducible asociada a λ que buscamos. Por ejemplo, la partición $\lambda = (1, 1, 1)$ nos da la representación regular, que, aunque no es irreducible, contiene a la representación alternada, que sí es irreducible. De la misma manera, la partición $\lambda = (2, 1)$ nos da la representación del ejemplo 5, que contiene a la representación estándar, que es irreducible. La idea general será construir un subespacio $W^\lambda \subset V^\lambda$ que sea invariante, y de manera que ρ restringida a W^λ sí sea irreducible.

Si el espacio W^λ ha de ser invariante, al aplicarle ρ_a a cualquier elemento de W^λ hemos de permanecer en W^λ . Una manera de aprovechar esto es considerar combinaciones lineales de las ρ_a . Para ello utilizaremos el concepto de signo de permutación introducido en el ejemplo 3. Recordando que el signo es multiplicativo y que $\varepsilon(a) = \pm 1$, se deducen fácilmente otras propiedades, como que $\varepsilon(a) = \varepsilon(a^{-1})$, o también que $\varepsilon(bab^{-1}) = \varepsilon(a)$.

Definición 10. Sea $H \subset \mathcal{S}_n$ un subgrupo de \mathcal{S}_n . Definiremos la función $f_H: V^\lambda \rightarrow V^\lambda$, para una partición λ y un subgrupo H , como

$$f_H\{T\} = \sum_{a \in H} \varepsilon(a)\rho_a\{T\}. \quad \blacktriangleleft$$

Observación 4. Si tenemos un subespacio $U^\lambda \subset V^\lambda$ invariante de ρ , entonces U^λ es subespacio invariante de f_H . Esto ocurre porque U^λ es subespacio invariante de cada ρ_a y f_H es combinación lineal de las ρ_a . ◀

Proposición 12. Si observamos como actúa ρ sobre f_H , tenemos que para todo $b \in \mathcal{S}_n$

$$\rho_b(f_H\{T\}) = f_{bHb^{-1}}(\rho_b\{T\}).$$

En el caso particular de $b \in H$, f_H es endomorfismo de ρ y, además,

$$\rho_b(f_H\{T\}) = f_H(\rho_b\{T\}) = \varepsilon(b)f_H\{T\}.$$

Demostración. Para la primera parte, realizamos el cálculo usando que el signo es multiplicativo:

$$\rho_b(f_H\{T\}) = \sum_{a \in H} \varepsilon(a)\rho_{ba}\{T\} = \sum_{a \in H} \varepsilon(bab^{-1})\rho_{bab^{-1}}(\rho_b\{T\}) = \sum_{c \in bHb^{-1}} \varepsilon(c)\rho_c(\rho_b\{T\}) = f_{bHb^{-1}}(\rho_b\{T\}).$$

Para la segunda parte, observemos que si $b \in H$, tenemos que $bHb^{-1} = H$. Continuando el cálculo,

$$\rho_b(f_H\{T\}) = f_H(\rho_b\{T\}) = \sum_{a \in H} \varepsilon(a)\rho_{ab}\{T\} = \varepsilon(b) \sum_{ab \in H} \varepsilon(ab)\rho_{ab}\{T\} = \varepsilon(b)f_H\{T\}. \quad \blacksquare$$

Vale la pena comentar que, aunque $f_{\mathcal{S}_n}$ sea endomorfismo de ρ (pues siempre ocurre que $b \in \mathcal{S}_n$), el teorema 3 no es aplicable, porque ρ no tiene por qué ser irreducible.

Observación 5. Fijémonos en la última igualdad de la segunda parte de la proposición. En el caso de $b \in H$ con $\varepsilon(b) = -1$, tenemos que $f_H(\rho_b\{T\}) = -f_H\{T\}$. Pero además existen ciertos $b \in \mathcal{S}_n$ para los que $\rho_b\{T\} = \{T\}$, concretamente, los que solo permutan filas de T . Haciendo esta suposición extra, tenemos que $f_H\{T\} = f_H(\rho_b\{T\}) = -f_H\{T\}$ y, por tanto, $f_H\{T\} = 0$. Estos b de \mathcal{S}_n que permutan filas de T son un subgrupo de \mathcal{S}_n , que denotaremos por $F(T)$. A su versión análoga por columnas la denotamos por $C(T)$. Y, como acabamos de ver, si existe $b \in F(T) \cap H$ con $\varepsilon(b) = -1$, entonces $f_H\{T\} = 0$. ◀

Ahora la idea consiste en utilizar la primera parte de la proposición 12 para construirnos un subespacio invariante. Efectivamente, si nos cogemos el espacio generado por imágenes de f_{H_i} siendo $\{H_i\}$ una familia de subgrupos tal que $bH_jb^{-1} \in \{H_i\}$ para cualesquiera j y $a \in \mathcal{S}_n$, entonces el subespacio $\langle \text{Im}(f_{H_i}) \rangle$ será invariante (por la proposición). La idea clave es tomar un H_T por cada tabloide y conseguir que la imagen de f_{H_T} sea unidimensional (lo más pequeño posible no trivial). Para ello nos interesa que $f_{H_T}\{T\} \neq 0$ y, por tanto, no queremos que $H_T \cap F(T)$ contenga permutaciones impares (por el ejemplo anterior). Pero, por otro lado, nos interesa H_T lo más grande posible porque así la imagen de f_{H_T} será más pequeña (es trivial ver que si $H' \subset H$, la imagen de f_H está contenida en la de $f_{H'}$). Un H maximal (en cierto sentido) que no comparte trasposiciones con $F(T)$ es $H = C(T)$, que es el que tomaremos.

Ejercicio 18. Probar que $C(T)$ es un subgrupo maximal en el siguiente sentido. Cualquier subgrupo H que no comparta permutaciones impares con $F(T)$ contiene, a lo sumo, las mismas trasposiciones que $C(T)$. Puede ser útil probarlo primero solo para un H que no comparta permutaciones impares con $F(T)$ y aplicar luego el teorema de Cauchy sobre la existencia de elementos de orden primo. ◀

Vale la pena comentar que, aunque H puede ser más grande que $C(T)$, al contener las mismas trasposiciones que $C(T)$, se cumple que $\dim(\text{Im}(f_H)) = \dim(\text{Im}(f_{C(T)}))$. Esto puede verse de la definición de f usando que $[H : C(T)]$ es impar o como corolario de la proposición 13 que enunciaremos a continuación.

Proposición 13. La aplicación $f_{C(T)}$ proyecta todo V^λ sobre una única recta, generada por $f_{C(T)}\{T\}$.

Demostración. Gracias a la elección de $H = C(T)$, tenemos que $f_{C(T)}\{T\} \neq 0$. Para verlo basta con desarrollar el sumatorio que define f_H y observar que todos los $\rho_a\{T\}$ que aparecen son tabloides diferentes (luego no pueden cancelarse). Ahora sea $\{S\}$ un tabloide cualquiera y veamos que $f_{C(T)}\{S\}$ es un múltiplo de $f_{C(T)}\{T\}$. En el caso de que existan trasposiciones en $F(S) \cap C(T)$, la observación 5 nos dice que $f_{C(T)}\{S\} = 0$ y, por tanto, es múltiplo de $f_{C(T)}\{T\}$. Falta el caso de que no existan trasposiciones en $F(S) \cap C(T)$, para el que necesitaremos el lema 14, que presentamos a continuación. ◻

Lema 14. Sean T y S dos tablas de Young de forma λ . Supongamos que no existen i, j diferentes que estén en la misma fila de S y misma columna de T (es decir, $\#(ij) \in F(S) \cap C(T)$). Entonces existen $a \in F(S)$ y $b \in C(T)$ tales que $\rho_b(T) = \rho_a(S)$.

Demostración. Consideremos los λ_1 números diferentes que están en la primera fila de S . Por hipótesis, están en las λ_1 columnas diferentes de T (ya que no puede haber dos en la misma columna de T). Por lo tanto, existe una permutación $b_1 \in C(T)$ que lleva estos λ_1 números a la primera fila de T . Observamos que $\rho_{b_1}(T)$ y S tienen los mismos números en su primera fila (aunque estén ordenados diferente). Podríamos seguir este razonamiento con la segunda fila de S y obtener $b_2 \in C(T)$ tal que $\rho_{b_2 b_1}(T)$ y S tengan los mismos números en las dos primeras filas. Procediendo sucesivamente, tenemos $b = b_r \dots b_2 b_1 \in C(T)$ tal que $\rho_b(T)$ y S tienen los mismos números en sus filas. Por lo tanto, como solo se diferencian en el orden de sus filas, existe $a \in F(S)$ tal que $\rho_b(T) = \rho_a(S)$. ■

Este lema permite concluir la demostración de la proposición 13. Considerando los tabloides generados por T y S tenemos que $\rho_b\{T\} = \rho_a\{S\} = \{S\}$ ya que $a \in F(S)$. Por lo tanto, $f_{C(T)}\{S\} = f_{C(T)}\rho_b\{T\} = \varepsilon(b)f_{C(T)}\{T\}$ utilizando la proposición 12.

Definición 11. Definimos el **politabloide** generado por T como $e_T = f_{C(T)}\{T\}$. Al subespacio generado por todos los politabloides e_T se lo llama **subespacio de Specht** y lo denotaremos por W^λ . ◀

Observación 6. Los politabloides son no nulos (en la demostración de la proposición 13 ya explicamos que $f_{C(T)}\{T\} \neq 0$). Pero, además, $f_{C(T)}$ es no idénticamente nula sobre el espacio de Specht porque

$$f_{C(T)}(e_T) = f_{C(T)}^2\{T\} = \sum_{a,b \in C(T)} \varepsilon(ab)\rho_{ab}\{T\} = |C(T)| \sum_{c \in C(T)} \varepsilon(c)\rho_c\{T\} = |C(T)|e_T \neq 0. \quad \blacktriangleleft$$

Ejemplo 19. Sea $n = 3$ y sea $\lambda = (2, 1)$. Consideremos las tablas T_1, T_2 y T_3 de la figura 6. Consideremos $f_{C(T_1)}$, que viene definido por $f_{C(T_1)}(u) = u - \rho_{(13)}(u)$ para cualquier $u \in V^\lambda$. Podemos observar cómo $f_{C(T_1)}\{T_2\} = -f_{C(T_1)}\{T_1\} \neq 0$, ya que estamos en el caso en el que $F(T_2)$ y $C(T_1)$ no comparten trasposiciones. Por otro lado, $f_{C(T_1)}\{T_3\} = 0$, ya que la trasposición (13) está tanto en $C(T_1)$ como en $F(T_3)$. ◀

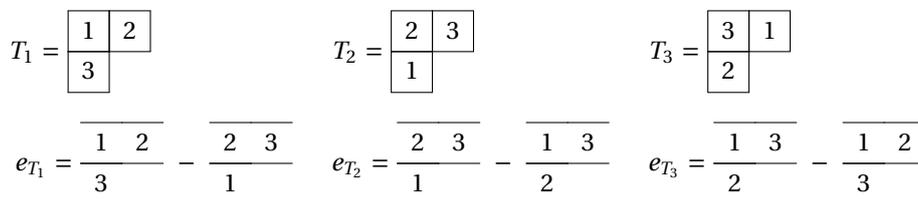


Figura 6: Algunas tablas de Young para $n = 3$ con sus respectivos politabloides.

Ejemplo 20. Continuando con la figura 6, podemos ver los politabloides e_{T_1}, e_{T_2} y e_{T_3} . Por supuesto, existirían otros tres más (ya que hay seis tablas), pero se puede comprobar que son estos tres cambiados de signo. Por lo tanto, estos tres ya generan todo W^λ . Además, podemos ver cómo $e_{T_1} + e_{T_2} + e_{T_3} = 0$, de manera que no son linealmente independientes. Tenemos, por tanto, $\dim(W^\lambda) = 2$. De hecho, la representación sobre W^λ será isomorfa a la estándar. Para verlo, hemos de pensar en los politabloides e_{T_1}, e_{T_2} y e_{T_3} dentro de la figura 3. Se puede comprobar que ρ actúa sobre los e_{T_i} igual que lo hace en la figura 3 sobre los puntos resultantes de girar 30° los puntos 1, 2 y 3. Otra forma más metódica de comprobar que esta representación es isomorfa a la estándar es calcular su carácter y utilizar el corolario 9. ◀

Ejemplo 21. Sea $n = 3$ y sea $\lambda = (1, 1, 1)$. En este caso $C(T) = \mathcal{S}_3 = C(S)$ para cualquier tabla T , por lo que $e_S = f_{C(S)}\{S\} = f_{C(T)}\{S\} \in \langle e_T \rangle$, por la proposición 13, y todos los politabloides están en la misma recta. Es decir, $\dim(W^\lambda) = 1$. De hecho, usando la segunda parte de la proposición 12, tenemos que $\rho_b(e_T) = \rho_b(f_{\mathcal{S}_n}\{T\}) = \varepsilon(b)f_{\mathcal{S}_n}\{T\} = \varepsilon(b)e_T$. Por lo tanto, estamos ante la representación alternada. ◀

Como ya vemos de los ejemplos, aunque los e_{T_i} no son una base (no son independientes), sí que generan un W^λ sobre el cual ρ es irreducible. Las proposiciones 12 y 13 serán las herramientas principales para probarlo. Solo nos falta un pequeño lema sobre el comportamiento de $C(\rho_a(T))$. La demostración se puede intentar como ejercicio. También se puede consultar la demostración en la bibliografía [1, 5].

Lema 15. Sean T una tabla y $a \in \mathcal{S}_n$. Entonces se cumple que $C(\rho_a(T)) = aC(T)a^{-1}$.

Teorema 16. El subespacio de Specht W^λ es un subespacio invariante de ρ . Además, al restringir ρ a W^λ obtenemos una representación irreducible.

Demostración. En primer lugar veamos que W^λ es invariante. Basta con ver que $\rho_a(e_T) \in W^\lambda$, porque los politabloides son generadores de W^λ . En efecto,

$$\rho_a(e_T) = \rho_a(f_{C(T)}\{T\}) = f_{aC(T)a^{-1}}(\rho_a\{T\}) = f_{C(\rho_a(T))}(\rho_a\{T\}) = e_{\rho_a(T)} \in W^\lambda,$$

donde hemos utilizado la primera parte de la proposición 12 y el lema 15.

Veamos ahora que ρ es irreducible sobre W^λ . Usando el teorema 1 descomponemos $W^\lambda = U_1 \oplus \dots \oplus U_r$. Sea T un tabloide cualquiera; como $\ker(f_{C(T)}) \neq W^\lambda$ (observación 6), existe algún U_i que no está estrictamente contenido en $\ker(f_{C(T)})$. Sea $u \in U_i$ tal que $f_{C(T)}(u) \neq 0$. Por la proposición 13, tenemos que $\text{Im}(f_{C(T)}) = \langle e_T \rangle$ y por la observación 4 tenemos que $f_{C(T)}(u) \in U_i$. De todo ello concluimos que $e_T \in U_i$. Ahora sea S otra tabla cualquiera, y sea $a \in \mathcal{S}_n$ la permutación tal que $\rho_a(T) = S$. Como U_i es invariante, $\rho_a(e_T) \in U_i$, pero, como hemos visto arriba, $\rho_a(e_T) = e_{\rho_a(T)} = e_S$. Por lo tanto, $e_S \in U_i$ para cualquier tabla S , siendo $U_i = W^\lambda$ el único subespacio invariante. ■

Teorema 17. Las representaciones ρ^λ restringidas a los subespacios W^λ son todas las representaciones irreducibles del grupo simétrico \mathcal{S}_n .

Demostración. El corolario 9 unido al hecho de que \mathcal{S}_n tiene $p(n)$ clases de conjugación nos dice que \mathcal{S}_n tiene $p(n)$ representaciones irreducibles. Nosotros hemos construido $p(n)$ representaciones irreducibles, las ρ sobre W^λ , para cada partición λ . Faltaría ver que todas ellas son no equivalentes entre sí. La demostración puede enfocarse como la del teorema 16, pero en este caso viendo que $f_{C(S)} \equiv 0$ sobre V^λ cuando S no proviene de la partición λ . Cuando S era una λ -tabla, teníamos que $\text{Im}(f_{C(S)}) = \langle e_S \rangle$; ahora tendremos que $\text{Im}(f_{C(S)}) = \{0\}$. La prueba de este paso puede consultarse en la bibliografía [3, 5]. ■

Teorema 18. Una posible base para este espacio de politabloides consiste en tomar solo los politabloides generados por tablas estándar.

Recordemos que una tabla es estándar si sus filas y columnas están en orden creciente.

Corolario 19. Para cada λ partición de n , sea n_λ la cantidad de tablas estándar. Entonces, del corolario 10 se deduce que $n! = \sum n_\lambda^2$, ya que los n_λ son también las dimensiones de las representaciones irreducibles.

La demostración del teorema 18 no la haremos y se puede encontrar en la bibliografía [3, 5]. La idea básica consiste en introducir una relación de orden en los tabloides según lo arriba o abajo que están los números. Para comparar $\{T\}$ y $\{S\}$ miramos el número más grande que esté en filas diferentes en ambos, llamémosle i . Si i está más arriba en $\{T\}$ que en $\{S\}$, decimos que $\{T\} < \{S\}$; en caso contrario, $\{S\} < \{T\}$. Esta relación de orden tiene la propiedad de que $\rho_a\{T\} \leq \{T\}$ para tablas estándar. Usando esta propiedad es fácil ver que los politabloides generados por tablas estándar son independientes. Lo que es más difícil es ver que generan todo W^λ . Una posible manera de probarlo es introducir un algoritmo que expresa los politabloides no estándar en función de los estándar: el *straightening algorithm*. Esta es la vía seguida en el artículo de McNamara [5]. Otra manera consiste en probar primero el corolario 19 mediante argumentos combinatorios y deducir, por cálculo de dimensiones, que los politabloides estándar son base de W^λ . Esta vía alternativa se encuentra en el libro de Fulton [3].

Ejemplo 22. En el ejemplo 20 ya vimos que para $\lambda = (2, 1)$ obtenemos un W^λ de dimensión 2, con una posible base $\{e_{T_1}, e_{T_2}\}$. Pero si nos fijamos en la figura 6, las tablas T_1 y T_2 son exactamente las dos únicas tablas estándar para $\lambda = (2, 1)$. Por lo tanto, vemos que se cumple el teorema 18. ◀

Ejemplo 23. Tanto para $\lambda = (3)$ como para $\lambda = (1, 1, 1)$ tenemos una única tabla estándar, siendo $n_{(3)} = n_{(1,1,1)} = 1$. Para $\lambda = (2, 1)$ tenemos dos tablas estándar, de forma que $n_{(2,1)} = 2$. Podemos comprobar cómo

$$\sum_{\lambda} n_{\lambda}^2 = 1^2 + 1^2 + 2^2 = 6 = 3!.$$

Esto no es más que la igualdad combinatoria que habíamos presentado en la introducción. ◀

Ejemplo 24. En los ejemplos de este artículo hemos descrito las tres representaciones irreducibles de \mathcal{S}_3 : la trivial, la alternada y la estándar. Todas ellas están dentro de la regular y, además, cada una está tantas veces como su dimensión (corolario 8). La trivial y la alternada son de dimensión 1 y la estándar es de dimensión 2. Por tanto, podemos visualizar la parte real de la representación regular (en \mathbb{R}^6) visualizando sus tres representaciones irreducibles (para el caso de la estándar, repetida). Podemos ver esto en la figura 7.

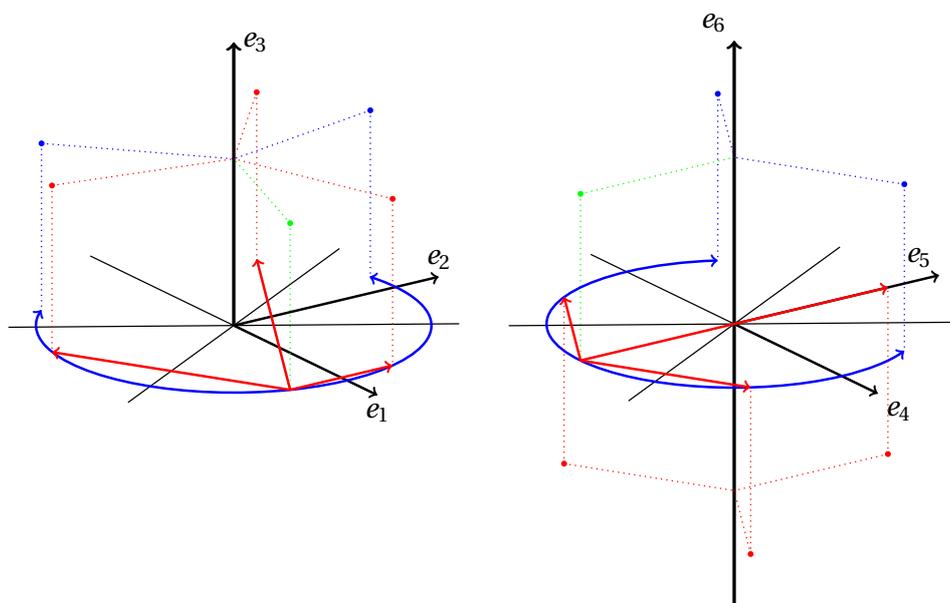


Figura 7: Dibujo esquemático de la representación regular de \mathcal{S}_3 . En la recta $\langle e_3 \rangle$ tenemos la representación trivial y en la recta $\langle e_6 \rangle$ tenemos la alternada. En los planos $\langle e_1, e_2 \rangle$ y $\langle e_4, e_5 \rangle$ tenemos la representación estándar. En verde, un punto genérico de $\mathbb{R}^6 \subset \mathbb{C}^6$. En azul, sus imágenes por los 3-ciclos, y en rojo, sus imágenes por las trasposiciones.

Referencias

- [1] CHOI, Je-Ok. «The Representations of the Symmetric Group». 25 de ago. de 2010. URL: <http://www.math.uchicago.edu/~may/VIGRE/VIGRE2010/REUPapers/Choi.pdf>.
- [2] FROBENIUS, Ferdinand Georg. *Über die Charaktere der symmetrischen Gruppe*. Königliche Akademie der Wissenschaften, 1900. <https://doi.org/10.3931/e-rara-18862>.
- [3] FULTON, William. *Young Tableaux: With Applications to Representation Theory and Geometry*. London Mathematical Society Student Texts. Cambridge: Cambridge University Press, 1996. <https://doi.org/10.1017/CB09780511626241>.
- [4] KOWALSKI, Emmanuel. *Representation Theory*. ETH Zürich, 17 de feb. de 2017. URL: <https://people.math.ethz.ch/~kowalski/representation-theory.pdf>.
- [5] MCNAMARA, Redmond. «Irreducible Representations of the Symmetric Group». Ago. de 2013. URL: <http://math.uchicago.edu/~may/REU2013/REUPapers/McNamara.pdf>.
- [6] SERRE, Jean-Pierre. *Linear representations of finite groups*. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42. Springer-Verlag, New York-Heidelberg, 1977, págs. x+170. <https://doi.org/10.1007/978-1-4684-9458-7>.
- [7] YOUNG, Alfred. «On Quantitative Substitutional Analysis». En: *Proceedings of the London Mathematical Society* 33 (1901), págs. 97-146. ISSN: 0024-6115. <https://doi.org/10.1112/plms/s1-33.1.97>.

- [8] YOUNG, Alfred. «On Quantitative Substitutional Analysis (Second Paper)». En: *Proceedings of the London Mathematical Society* 34 (1902), págs. 361-397. ISSN: 0024-6115. <https://doi.org/10.1112/plms/s1-34.1.361>.
- [9] YOUNG, Alfred. «On Quantitative Substitutional Analysis». En: *The Journal of the London Mathematical Society* 3.1 (1928), págs. 14-19. <https://doi.org/10.1112/jlms/s1-3.1.14>.
- [10] YOUNG, Alfred. «On Quantitative Substitutional Analysis (Third Paper)». En: *Proceedings of the London Mathematical Society. Second Series* 28.4 (1928), págs. 255-292. ISSN: 0024-6115. <https://doi.org/10.1112/plms/s2-28.1.255>.
- [11] YOUNG, Alfred. «On Quantitative Substitutional Analysis (Fourth Paper)». En: *Proceedings of the London Mathematical Society. Second Series* 31.4 (1930), págs. 253-272. ISSN: 0024-6115. <https://doi.org/10.1112/plms/s2-31.1.253>.
- [12] YOUNG, Alfred. «On Quantitative Substitutional Analysis (Fifth Paper)». En: *Proceedings of the London Mathematical Society. Second Series* 31.4 (1930), págs. 273-288. ISSN: 0024-6115. <https://doi.org/10.1112/plms/s2-31.1.273>.
- [13] YOUNG, Alfred. «Corrigenda. On Quantitative Substitutional Analysis». En: *Proceedings of the London Mathematical Society. Second Series* 31.7 (1930), pág. 556. ISSN: 0024-6115. <https://doi.org/10.1112/plms/s2-31.1.556-t>.
- [14] YOUNG, Alfred. «On Quantitative Substitutional Analysis (Sixth Paper)». En: *Proceedings of the London Mathematical Society. Second Series* 34.3 (1932), págs. 196-230. ISSN: 0024-6115. <https://doi.org/10.1112/plms/s2-34.1.196>.
- [15] YOUNG, Alfred. «On Quantitative Substitutional Analysis (Seventh Paper)». En: *Proceedings of the London Mathematical Society. Second Series* 36 (1934), págs. 304-368. ISSN: 0024-6115. <https://doi.org/10.1112/plms/s2-36.1.304>.
- [16] YOUNG, Alfred. «On Quantitative Substitutional Analysis (Eighth Paper)». En: *Proceedings of the London Mathematical Society. Second Series* 37.1 (1934), págs. 441-495. ISSN: 0024-6115. <https://doi.org/10.1112/plms/s2-37.1.441>.
- [17] YOUNG, Alfred. «On quantitative substitutional analysis (Ninth Paper)». En: *Proceedings of the London Mathematical Society. Second Series* 54 (1952), págs. 219-253. ISSN: 0024-6115. <https://doi.org/10.1112/plms/s2-54.3.219>.

A. Anexo: resolución de ejercicios

Solución del ejercicio 6. Para ver que la representación regular de S_n contiene la representación trivial, lo natural es considerar la recta $\langle(1, 1, \dots, 1)\rangle = V_1$. Parametricemos los puntos de $x \in V_1$ con el número complejo c , donde $x = (c, c, \dots, c)$. Si ρ es la representación regular, $\rho_a(x)$ será el resultado de permutar las coordenadas de x según a . Pero, como todas son iguales, obtendremos (c, c, \dots, c) , independientemente de la permutación $a \in S_n$. Por tanto, V_1 es subespacio invariante, y ρ_a restringida a V_1 es la identidad. Es decir, la representación regular restringida a V_1 es la trivial.

Para ver que ρ contiene la representación alternada, recordemos que en la representación regular las coordenadas van indexadas por permutaciones $\{a_i\} = S_n$. Consideremos la recta $\langle(\varepsilon(a_1), \varepsilon(a_2), \dots, \varepsilon(a_n))\rangle = V_2$. Si consideramos $x = (c\varepsilon(a_1), c\varepsilon(a_2), \dots, c\varepsilon(a_n)) \in V_2$, tenemos que $\rho_b(x)$ será el resultado de permutar las coordenadas de x por $b \in S_n$. De esta forma, la coordenada a_i irá a parar a la coordenada ba_i . Por tanto, el valor de la coordenada i -ésima de $\rho_b(x)$ será $\varepsilon(b^{-1}a_i) = \varepsilon(b)\varepsilon(a_i)$. De ahí se deduce $\rho_b(x) = \varepsilon(b)x$, para todo $x \in V_2$, por lo que V_2 es subespacio invariante, y la representación regular restringida a V_2 es la alternada. ■

Solución del ejercicio 13. Queremos ver que dos permutaciones de S_n son conjugadas si y solo si sus ciclos son del mismo tamaño. Consideremos $a, b \in S_n$ conjugadas, es decir, $ca = bc$, con $c \in S_n$. Esto quiere decir que si a envía i a $a(i)$, b enviará $c(i)$ a $c(a(i))$. Es decir, b hace exactamente lo mismo que a pero sobre la imagen de c .

En particular, si tenemos el ciclo $(i, a(i), a^2(i), \dots, a^k(i))$ en a , tenemos el ciclo

$$(c(i), bc(i), b^2c(i), \dots, b^k c(i)) = (c(i), ca(i), ca^2(i), \dots, ca^k(i))$$

en b , de la misma longitud, y como c es una biyección, los ciclos de a y b son de los mismos tamaños. Recíprocamente, si los ciclos son de los mismos tamaños, podemos construir c que envíe cada ciclo de a a un ciclo de b del mismo tamaño y, además, preservando el orden dentro del ciclo. De esa manera, si $a(i)$ es el siguiente número a i en un ciclo de a , $c(a(i))$ será el siguiente número a $c(i)$ en un ciclo de b . Es decir, $bc(i) = ca(i)$, y como esto es para todo i , entonces, $bc = ca$, siendo a y b conjugados. ■

Solución del ejercicio 17. Supongamos que una partición $\lambda = (n_1, n_2, \dots, n_k)$ nos da una representación ρ irreducible sobre V^λ . Consideremos su carácter φ . Ya sabemos que si ρ es irreducible, entonces $(\varphi|\varphi) = 1$, pero el recíproco también es cierto (trivial por el corolario 8, por ejemplo). Ahora tratemos de calcular $(\varphi|\varphi)$ explícitamente. Para calcular φ , tomamos la base de los tabloides y vemos que

$$\varphi(a) = \text{Tr}(\rho_a) = \# \{ \lambda - \text{tabloides que fijan } a \} = m_a,$$

donde hemos definido m_a como la cantidad de tabloides que fija a . Esta igualdad es más fácil de entender en forma matricial: ρ_a es una matriz llena de ceros excepto en las entradas $(\{T\}, \{S\})$ tales que $\rho_a\{T\} = \{S\}$, donde la matriz tiene entrada uno. Por lo tanto, la traza es la cantidad de unos en la diagonal, es decir, la cantidad de tabloides tales que $\rho_a\{T\} = \{T\}$. Si ahora calculamos $(\varphi|\varphi)$ y aplicamos la desigualdad de medias cuadrática-aritmética,

$$(\varphi|\varphi) = \frac{\sum_a m_a^2}{|\mathcal{S}_n|} \geq \left(\frac{\sum_a m_a}{|\mathcal{S}_n|} \right)^2.$$

La suma de los m_a es fácil de computar utilizando la típica técnica combinatoria de doble conteo: en vez de sumar para a la cantidad de tablas fijas por a , sumaremos para $\{T\}$ la cantidad de permutaciones que fijan $\{T\}$. Esta cantidad es trivialmente $n_1!n_2! \dots n_k!$ (podemos permutar cada fila como queramos). Esa cantidad se suele denotar como $\lambda! = n_1! \dots n_k!$. Tenemos que

$$\sum_{a \in \mathcal{S}_n} m_a = \sum_{\{T\}} \lambda! = \# \{ \lambda - \text{tabloides} \} \lambda! = \# \{ \lambda - \text{tablas} \} = n!.$$

Esto viene de que la cantidad de tablas es la cantidad de tabloides por la cantidad de maneras de ordenar las filas (que es $\lambda!$). Por otro lado, es obvio que hay $n!$ tablas porque hay $n!$ maneras de colocar los n números en la tabla. Ahora ya hemos acabado porque

$$(\varphi|\varphi) \geq \left(\frac{\sum_a m_a}{|\mathcal{S}_n|} \right)^2 = \left(\frac{n!}{n!} \right)^2 = 1,$$

de lo que se deduce que, si ρ es irreducible, estamos en el caso de igualdad de la desigualdad de medias. Dicho caso se alcanza cuando todos los m_a son iguales; en particular, serán iguales a $m_1 = \# \{ \text{tabloides} \}$, ya que $\rho_1 = \text{Id}$ fija todos los tabloides. Luego cualquier ρ_a fija todos los tabloides. Esto implica que los tabloides solo tienen una fila, porque si hubiera dos filas (es decir, $\lambda \neq (n)$), para cualquier tabloide $\{T\}$ podríamos escoger como a una trasposición entre un número de la primera fila y uno de la segunda. Claramente, dicho ρ_a no fijaría $\{T\}$ y estaríamos ante una contradicción. ■

Solución del ejercicio 18. En primer lugar, supongamos un H con más trasposiciones que $C(T)$ pero que no comparte ninguna con $F(T)$. Sea (ij) una trasposición de $H - C(T)$. Es obvio que (ij) no está ni en $C(T)$ ni en $F(T)$ y, por tanto, i y j no comparten ni fila ni columna en T . Sin pérdida de generalidad supongamos que la fila de i es previa a la de j ; entonces, existe una casilla en la tabla que tiene la columna de i y la fila de j . Supongamos dicha casilla ocupada por el número k . Tenemos que $(ik) \in C(T) \subset H$, luego $(ik)(ij)(ik) \in H$ ya que todos los elementos del producto están en H . No obstante, $(ik)(ij)(ik) = (jk) \in F(T)$, y esto contradice que H y $F(T)$ no compartan trasposiciones.

Ahora extrapolemos el resultado a permutaciones impares cualesquiera. Si $F(T)$ y H comparten permutaciones impares, entonces $F(T) \cap H$ no es subgrupo del grupo alternado \mathcal{A}_n . De esta manera, $[F(T) \cap H : F(T) \cap H \cap \mathcal{A}_n]$ es un divisor de $[\mathcal{S}_n : \mathcal{A}_n] = 2$ que no es 1. Por lo tanto, es 2 y tenemos que $|F(T) \cap H|$ es par. Aplicando el teorema de Cauchy para la existencia de elementos primos para $p = 2$ tenemos que existe alguna trasposición en $F(T) \cap H$, lo cual contradice el resultado previo. ■