Revista Colombiana de Matemáticas
Volumen 43(2009)1, páginas 19-34

El teorema de Cayley revisitado

The theorem of Cayley revisited

J. Andrés Montoya

Universidad Industrial de Santander, Bucaramanga, Colombia

Resumen. En este artículo probamos que no existe un $N \in \mathbb{N}$ tal que todo grupo finito puede ser embebido en $GL_{\mathbb{C}}(N)$.

Palabras y frases clave. Grupos finitos, representaciones de grupos, caracteres de grupos.

2000 Mathematics Subject Classification. 20C15, 20C30.

Abstract. In this paper we prove that there not exists $N \in \mathbb{N}$ such that any finite group can be embedded into $GL_{\mathbb{C}}(N)$.

Key words and phrases. Finite groups, linear representations, group characters.

1. Introducción: Definición del problema

Notación 1. *Dado $n \in \mathbb{N}$, el símbolo S_n denotará al grupo simétrico de orden n, esto es, S_n denotará al grupo de las permutaciones del conjunto $[n] := \{1, \ldots, n\}$.*

Dado α un cardinal, diremos que G es un α-grupo si y solo si todo grupo H de cardinal menor que α está embebido en G. El Teorema de Cayley [3] afirma que, dado G un grupo finito, si $|G| \leq n$, entonces G está inmerso en S_n, (en símbolos $G \prec S_n$), i. e. para todo $n \in \mathbb{N}$ se tiene que S_n es un $n+1$-grupo. Una pregunta natural es la siguiente: ¿existe un grupo H tal que si G es finito, $G \prec H$? o, lo que es lo mismo, ¿existen ω-grupos?

Es fácil dar una respuesta afirmativa a esta pregunta. Sea S_ω el grupo de permutaciones del conjunto $\mathbb{N}$, note que para todo $n \in \mathbb{N}$ se tiene que $S_n \prec S_\omega$. Es claro que esto implica que S_ω es un ω-grupo. Note por otro lado que S_ω no es lo que podríamos llamar un grupo elemental, dado que, entre otras cosas, sus elementos son objetos infinitos y su operación es no computable. ¿Existe un

grupo elemental que sea un ω-grupo? En este trabajo no intentaremos dar una definición de grupo elemental, a cambio consideraremos una clase de grupos a la que hemos dado en llamar la clase de los *grupos aritméticos*. En el artículo se prueba que no existen ω-grupos aritméticos, siendo este el resultado principal del presente escrito. Desde el punto de vista técnico la prueba se reduce a probar que no existe un campo $\mathbb{F}$ y un número natural k tal que todo grupo finito esté embebido en $GL_{\mathbb{F}}(k)$. Para probar este resultado técnico, el primer paso (sección 2) consiste en probar que si existiera un campo $\mathbb{F}$ y un número natural k tal que $GL_{\mathbb{F}}(k)$ es un ω-grupo, entonces $GL_{\mathbb{C}}(k)$ también sería un ω-grupo. El siguiente paso de nuestra prueba consiste en mostrar que no existe k tal que $GL_{\mathbb{C}}(k)$ es un ω-grupo; para tal fin usaremos algunas herramientas y conceptos de la teoría de representación de grupos finitos, conceptos que introduciremos en las secciones 3 y 4 de este artículo. La sección 5 contiene el argumento central de la prueba, quedando solo pendiente la verificación de una interesante desigualdad combinatoria, cuya demostración es el contenido de la sección 6.

Creemos que una de las virtudes del escrito es la interesante *combinación de todas las formas de lucha* presente en el desarrollo de los argumentos. El lector encontrará que para probar el resultado central del artículo hemos usado argumentos propios de la teoría de modelos, el álgebra lineal, la teoría de grupos, la teoría de representación de grupos finitos, la combinatoria y la computación[1].

Definición 1. *Un grupo G es un grupo aritmético si y solo si G pertenece a alguna de las tres familias listadas a continuación:*

1. $\{G : G \subset (V, +)\}$*, donde* $(V, +)$ *es el grupo aditivo de un espacio vectorial finito dimensional.*
2. $\{G : G \subset (\mathbb{F}^*, \times)\}$*, donde* $\mathbb{F}$ *es un campo y* $(\mathbb{F}^*, \times)$ *denota el subgrupo multiplicativo de* $\mathbb{F}$*.*
3. $\{G : G \subset GL_{\mathbb{F}}(k)\}$*, donde* $k \in \mathbb{N}$*,* $\mathbb{F}$ *es un campo y* $GL_{\mathbb{F}}(k)$ *es el grupo lineal de las* $\mathbb{F}$*-matrices invertibles de* $k \times k$*.*

Intuitivamente la clase de los grupos aritméticos es la clase de los grupos *concretos*. Un grupo aritmético es un grupo cuyos elementos son arreglos (objetos) numéricos finitos y cuya operación es una operación algebraica natural, (concreta, fácil y computable).

[1]Para probar, en la sección 6, la desigualdad combinatoria antes mencionada, nos vimos forzados a realizar una dispendiosa verificación computacional con la ayuda de un equipo de computo, lo cual puede recordar a algunos la famosa prueba de Appell-Haken del teorema de los cuatro colores; es importante anotar que nuestro resultado es muchísimo más modesto. También es importante anotar que el grado de dependencia de nuestra prueba en estos recursos computacionales es mucho menor que en el caso de Appell-Haken; esto convierte a nuestra prueba (para mal) en un caso mucho menos espectacular de demostración asistida por computador, pero a su vez (para bien) en una prueba mucho menos polémica.

Comentario 1. *Los grupos aritméticos, tal como los hemos definido, corresponden en gran medida a los grupos que pueden ser construidos usando las operaciones de un campo. Los grupos de la primera familia son los grupos que pueden ser construidos a partir de la suma de un campo, los grupos de la segunda familia son los grupos definibles a partir de la multiplicación de un campo, y finalmente los grupos de la tercera familia son los grupos que pueden ser definidos usando simultáneamente la suma y la multiplicación de un campo.*

Comentario 2. *Note que S_ω es un $\aleph_1$ grupo, i.e. si G es un grupo enumerable, entonces $G \prec S_\omega$. Para verificar esta afirmación basta adaptar la prueba del teorema de Cayley al caso de grupos enumerables. ¿Es S_ω un $2^{\aleph_0}$ grupo? Esta pregunta es uno de los problemas consignados en el famoso Libro Escocés*[2] *[5]. Dada $\alpha \in S_f$, definimos $sop(\alpha) := \{i \in \mathbb{N} : \alpha(i) \neq i\}$. En [4] Kallman prueba que si $S_f := \{\alpha \in S_\omega : sop(\alpha) \text{ es finito}\}$, entonces $\frac{S_\omega}{S_f}$ no está embebido en S_ω, y esto claramente implica que S_ω no es un $2^{\aleph_0}$ grupo. Adicionalmente Kallman prueba que para todo $n \in \mathbb{N}$ y para todo campo $\mathbb{F}$, si $|\mathbb{F}| \leq 2^{\aleph_0}$, entonces $GL_{\mathbb{F}}(k) \prec S_\omega$.*

Problema 1. *¿Existen ω-grupos aritméticos?*

2. Si existe un ω-grupo aritmético, existe un ω-grupo sobre los complejos

En esta sección mostraremos que si existe un ω-grupo aritmético, existe entonces $k \in \mathbb{N}$ tal que $GL_{\mathbb{C}}(k)$ es un ω-grupo.

Lema 1. *Si G es un grupo perteneciente a alguna de las dos primeras familias, en la definición de grupo aritmético, G no es un ω-grupo.*

Demostración. Note simplemente que todo grupo perteneciente a alguna de las dos primeras familias es abeliano. Dado que todo subgrupo de un grupo abeliano es abeliano, ningún grupo abeliano puede ser un ω-grupo. ☑

Lema 2. *Si $G \subset GL_{\mathbb{F}}(k)$ y $\mathbb{F}$ es un campo finito, G no es ω-grupo.*

Demostración. Note simplemente que en este caso G es finito y que todo ω-grupo es infinito. ☑

Comentario 3. *Note que si $G \subset H$ y G es un ω-grupo entonces H es un ω-grupo.*

En lo que sigue probaremos que, si $\mathbb{F}$ es un campo de característica $p \neq 0$ y $k \in \mathbb{N}$, entonces $GL_{\mathbb{F}}(k)$ no es un ω-grupo.

[2] *El Libro Escocés* es un famoso libro en el que se consignaron las conjeturas y problemas propuestos por un nutrido grupo de matemáticos polacos (entre otros Banach, Mazur, Ulam y Kac), que solían reunirse, a lo largo de la década de los 30, a hablar de Matemáticas en un café de Lwov (hoy en día Lviv, en Ucrania) llamado El Café Escocés.

Lema 3. *Dados $k \in \mathbb{N}$, $\mathbb{F}$ un campo de característica $p \neq 0$, $x \in \mathbb{F}$ y $A \in GL_{\mathbb{F}}(k)$, se tiene que $(A+xI)^p = A^p + x^pI$.*

Demostración. Note que $(A+xI)^p = A^p + x^pI + \sum_{i=1}^{p-1} \binom{p}{i} A^i x^{p-i}$. Note también que, para todo $i \in \{1, \ldots, p-1\}$, el número combinatorio $\binom{p}{i}$ es divisible por p. Lo anterior implica que $\sum_{i=1}^{p-1} \binom{p}{i} A^i x^{p-i} = 0$ y por lo tanto $(A+xI)^p = A^p + x^pI$. ☑

Definición 2. *Sea M una matriz de $n \times n$ con entradas en algún campo $\mathbb{F}$.*

1. *$o(M) = \text{mín}_{i \in \mathbb{N}} \left[M^i = I\right]$; en caso de no existir un tal i diremos que $o(M)$, el orden de M, es igual a ∞.*
2. *$v(M) = \text{mín}_{i \in \mathbb{N}} \left[M^i = 0\right]$; en caso de no existir un tal i diremos que $v(M)$, la nulidad de M, es igual a ∞.*

Lema 4. *Sea $\mathbb{F}$ un campo de característica $p \neq 0$ y sea $M \in GL_{\mathbb{F}}(k)$ tal que $o(M) = p^i$, existe $N \in GL_{\mathbb{F}}(k)$ tal que $p^{i-1} \leq v(N) \leq p^i$.*

Demostración. Note primero que $M^{p^i} = I$ y que por consiguiente $(M-I)^{p^i} = M^{p^i} - I = 0$. Sea $N = M - I$, tenemos que $N^{p^{i-1}} = (M-I)^{p^{i-1}} = M^{p^{i-1}} - I \neq 0$. Por lo tanto $p^{i-1} \leq v(N) \leq p^i$. ☑

A continuación probaremos que si $\mathbb{F}$ es un campo de característica $p \neq 0$, ningún grupo de la forma $GL_{\mathbb{F}}(k)$ es un ω-grupo.

Sea M una matriz de $n \times n$ con entradas en un campo $\mathbb{F}$.

Proposición 1. *Dado $i \in \mathbb{N}$, si $\mathbb{F}^n \neq \ker\left(M^i\right) = \ker\left(M^{i+1}\right)$, entonces $v(M) = \infty$.*

Demostración. Probaremos que $\ker\left(M^{i+1}\right) = \ker\left(M^{i+2}\right)$.

Sea $v \in \mathbb{F}^n - \ker\left(M^{i+1}\right)$, suponga que $M^{i+2}v = 0$; esto implica que $Mv \in \ker\left(M^{i+1}\right)$, pero como $\ker\left(M^i\right) = \ker\left(M^{i+1}\right)$ tenemos que $Mv \in \ker\left(M^i\right)$ y por consiguiente $v \in \ker\left(M^{i+1}\right)$, lo cual es una contradicción, por lo tanto $\ker\left(M^{i+1}\right) = \ker\left(M^{i+2}\right)$.

Para el lector debe ser claro que podemos insertar el argumento anterior dentro de un argumento inductivo para obtener una prueba del teorema. ☑

De la proposición podemos obtener, de manera inmediata, la siguiente proposición:

Corolario 1. *Dado $k \in \mathbb{N}$ existe $N \in \mathbb{N}$ tal que si $M \in GL_{\mathbb{F}}(k)$, entonces ó $v(M) = \infty$ ó $v(M) \leq N$.*

Demostración. Suponga que para todo $N \in \mathbb{N}$ existe una matriz $M \in GL_{\mathbb{F}}(k)$ tal que $N \leq v(M) \lneqq \infty$. En particular existe $N_0 \in GL_{\mathbb{F}}(k)$ tal que $k+1 \leq v(N_0) \lneqq \infty$. Sea $i = v(N_0)$, note que $\{0\} \subsetneq \ker(N) \subsetneq \ker\left(N^2\right) \subsetneq ... \subsetneq \ker\left(N^{k+1}\right)$. Es claro que esto último es imposible dado que cada uno de los espacios vectoriales $\ker(N), \ker\left(N^2\right), \ldots, \ker\left(N^{k+1}\right)$ es un subespacio del espacio $\mathbb{F}^k$, el cual tiene dimensión k. ☑

Ahora bien, dado p un primo y dado $i \in \mathbb{N}$, el símbolo $\mathbb{Z}_{p^i}$ denotará el grupo multiplicativo cíclico de orden p^i.

Teorema 1. *Si $\mathbb{F}$ es un campo de característica $p \neq 0$ y $k \in \mathbb{N}$, el grupo $GL_{\mathbb{F}}(k)$ no es un ω-grupo.*

Demostración. Suponga que $\mathbb{F}$ es un campo de característica $p \neq 0$ y que $GL_{\mathbb{F}}(k)$ es un ω-grupo. Dado $i \in \mathbb{N}$, tenemos que $\mathbb{Z}_{p^{i+1}} \prec GL_{\mathbb{F}}(k)$. Esto implica que existe $M_i \in GL_{\mathbb{F}}(k)$ tal que $o(M_i) = p^{i+1}$, pero esto implica a su vez la existencia de una matriz $N_i \in GL_{\mathbb{F}}(k)$ tal que $p^i \leq v(N_i) \leq p^{i+1}$, lo cual claramente contradice el corolario anterior. ☑

De lo probado hasta el momento tenemos que si existe un ω-grupo aritmético, existe entonces $\mathbb{F}$, un campo de característica cero, tal que $GL_{\mathbb{F}}(k)$ es un ω-grupo.

Dado $\mathbb{F}$ un campo, usaremos el símbolo $\widetilde{\mathbb{F}}$ para denotar la clausura algebraica de $\mathbb{F}$.

Lema 5. *Si $G \subset GL_{\mathbb{F}}(k)$ es un ω-grupo, entonces $GL_{\widetilde{\mathbb{F}}}(k)$ es un ω-grupo.*

Demostración. Note que para todo campo $\mathbb{F}$ se tiene que $GL_{\mathbb{F}}(k) \subset GL_{\widetilde{\mathbb{F}}}(k)$. ☑

El lema implica que si existe un ω-grupo aritmético, existe entonces $\mathbb{F}$, un campo algebraicamente cerrado de característica cero, tal que para algún $k \geq 1$ se tiene que $GL_{\mathbb{F}}(k)$ es un ω-grupo.

Proposición 2. *Suponga que existen $\mathbb{F}$, un campo algebraicamente cerrado de característica cero, y $k \in \mathbb{N}$ tales que $GL_{\mathbb{F}}(k)$ es un ω-grupo. En este caso $GL_{\mathbb{C}}(k)$ también es un ω-grupo.*

Demostración. Dado G un grupo finito y dado $k \in \mathbb{N}$, existe una sentencia de primer orden $\psi_{G,k}$ tal que para todo $\mathbb{F}$, campo algebraicamente cerrado de característica cero, se tiene lo siguiente:

$$\mathbb{F} \vDash \psi_{G,k} \text{ si y solo si } G \text{ es un subgrupo de } GL_{\mathbb{F}}(k).$$

Dado que la teoría de campos algebraicamente cerrados de característica cero es completa [2], se tiene que: dados $\mathbb{F}$, un campo algebraicamente cerrado de característica cero, $k \in \mathbb{N}$ y G un grupo finito

$$\mathbb{F} \vDash \psi_{G,k} \text{ si y solo si } \mathbb{C} \vDash \psi_{G,k} .$$

Por lo tanto, para todo $\mathbb{F}$ y para todo $k \in \mathbb{N}$, el grupo $GL_{\mathbb{F}}(k)$ es un ω-grupo si y solo si $GL_{\mathbb{C}}(k)$ es un ω-grupo. ☑

Finalmente podemos enunciar el teorema principal de esta sección, cuya prueba es una consecuencia inmediata de todo lo anterior.

Teorema 2. *Si existe un ω-grupo aritmético, existe entonces $k \in \mathbb{N}$ tal que $GL_{\mathbb{C}}(k)$ es un ω-grupo.*

El teorema anterior nos permite reformular nuestro problema de la siguiente manera:

Problema 2. *¿Existe $k \in \mathbb{N}$ tal que $GL_{\mathbb{C}}(k)$ es un ω-grupo? o, lo que es lo mismo, ¿existe $k \in \mathbb{N}$ tal que para todo $n \in \mathbb{N}$, se tiene que $S_n \prec GL_{\mathbb{C}}(k)$?*

Dado G un grupo finito, es fácil ver que $G \prec GL_{\mathbb{C}}(|G|)$. Sea $\{e_g : g \in G\}$ una base de $\mathbb{C}^{|G|}$; dado $g \in G$, tenemos que T_g es la transformación lineal de $\mathbb{C}^{|G|}$ en $\mathbb{C}^{|G|}$ definida por

$$T_g\left(\sum_{h\in G} x_h e_h\right) = \sum_{h\in G} x_h e_{gh} .$$

Es fácil verificar que la función $\mathrm{reg}_G : G \to \mathrm{End}_{\mathbb{C}}\left(\mathbb{C}^{|G|}\right)$ definida por

$$\mathrm{reg}_G(g) = T_g ,$$

es un homomorfismo inyectivo.

El problema con la familia de embebimientos $\{\mathrm{reg}_G : G \text{ es un grupo finito}\}$ es que la dimensión del espacio de llegada crece linealmente con el tamaño de G. La pregunta es si podemos poner freno a este crecimiento en la dimensión y embeber todo grupo finito en un único grupo de la forma $End_{\mathbb{C}}(V) \simeq GL_{\mathbb{C}}(\dim(V))$ (con V un espacio vectorial complejo finito dimensional).

Definición 3.

1. *Dado G un grupo finito, una representación de G es un homomorfismo $\rho : G \to End_{\mathbb{C}}(V)$, donde V es un vectorial complejo finito dimensional.*
2. *Dada $\rho : G \to End_{\mathbb{C}}(V)$ una representación de G, la dimensión de ρ es igual a* $\dim(V)$.

3. *Una representación $\rho : G \to End_{\mathbb{C}}(V)$ es cierta si y solo si ρ es inyectiva.*

Ejemplo 1. *Dado G un grupo finito, $reg_G(g)$ es una representación cierta de G de dimensión $|G|$.*

Permítannos reformular una vez más el problema que consideramos en este escrito.

Problema 3. *¿Existe $N \in \mathbb{N}$ tal que todo grupo finito tiene una representación cierta de dimensión a lo más N?*

3. Representaciones lineales

En esta breve sección introduciremos los conceptos fundamentales de la teoría de representaciones lineales de grupos finitos. Adicionalmente enunciaremos uno de los teoremas fundamentales de la teoría, el teorema de Maschke. Para mayor información el lector puede consultar [1].

Definición 4.

1. *Dadas $\rho_1 : G \to End_{\mathbb{C}}(V)$ y $\rho_2 : G \to End_{\mathbb{C}}(W)$ dos representaciones de G, un morfismo de ρ_1 en ρ_2 es una transformación lineal $T : V \to W$ tal que $\rho_2 T = T\rho_1$.*

2. *Dadas $\rho_1 : G \to End_{\mathbb{C}}(V)$ y $\rho_2 : G \to End_{\mathbb{C}}(W)$ dos representaciones de G, diremos que ρ_1 y ρ_2 son representaciones equivalentes si y solo si existe un isomorfismo lineal $T : V \to W$ tal que $\rho_2 T = T\rho_1$.*

3. *Dadas $\rho_1 : G \to End_{\mathbb{C}}(V)$ y $\rho_2 : G \to End_{\mathbb{C}}(W)$, la suma directa de ρ_1 y ρ_2, que denotaremos $\rho_1 \oplus \rho_2$, es la representación de G en $V \oplus W$ dada por*
$$(\rho_1 \oplus \rho_2)\, g = \rho_1(g) + \rho_2(g).$$

4. *Dada $\rho : G \to End_{\mathbb{C}}(V)$ una representación y dado $W \subset V$ tal que, para todo $g \in G$, $\rho(g)(W) \subset W$, diremos que $\rho \restriction_W$ es una subrepresentación de G.*

5. *Una representación $\rho : G \to End_{\mathbb{C}}(V)$ es irreducible si y solo si ρ no contiene subrepresentaciones propias.*

Uno de los teoremas fundamentales de la teoría de representaciones de grupos finitos es el teorema que enunciamos a continuación

Teorema 3 (Teorema de Maschke). *Toda representación de G es una suma directa de representaciones irreducibles.*

Para una prueba el lector puede consultar [1]. Note que si ρ es reducible y ρ es igual a $\bigoplus_{i \leq s} \rho_i$, entonces para todo $i \leq s$, $\dim(\rho) \geq \dim(\rho_i)$. Ahora, como lo que buscamos estudiar son las representaciones ciertas de G de la menor

dimensión posible, podemos y debemos concentrar nuestra atención en las representaciones irreducibles de G; esto nos permite reformular nuestro problema una vez más.

Problema 4. *¿Existe $N \in \mathbb{N}$ tal que para todo $n \in \mathbb{N}$, el grupo S_n tiene una representación cierta irreducible de dimensión a lo más N?*

Este problema, tal como lo acabamos de formular, es el problema que trataremos en lo que queda del escrito.

4. Representaciones irreducibles de S_n

El propósito de esta sección es esbozar la teoría de las representaciones lineales de los grupos simétricos y enunciar los resultados fundamentales concernientes a las representaciones irreducibles de tales grupos.

Dadas $\alpha, \beta \in S_n$, diremos que α y β son conjugadas, (usaremos la notación $\alpha \sim \beta$ para indicar que α y β son conjugadas), si y solo si existe $\eta \in S_n$ tal que $\alpha = \eta\beta\eta^{-1}$. Usaremos el símbolo $[\alpha]$ para denotar la clase de α, donde la clase de α es el conjunto $\{\beta \in S_n : \alpha \sim \beta\}$. Recuerde que dada $\alpha \in S_n$, la permutación α es igual a un producto de ciclos disyuntos [3]. Sean $c_1, \ldots, c_m$ ciclos disyuntos en S_n y tales que

1. $\alpha = c_1 \circ \cdots \circ c_m$.
2. $|c_1| \geq \cdots \geq |c_m| \geq 1$, donde $|c_i|$ denota la longitud de c_i.
3. $n = |c_1| + \cdots + |c_m|$.

Definición 5. *La estructura de ciclos de α es el vector $(|c_1|, \ldots, |c_m|)$.*

Teorema 4. *Dadas $\alpha, \beta \in S_n$, tenemos que $\alpha \sim \beta$ si y solo si α y β tiene la misma estructura de ciclos.*

Para una prueba el lector puede consultar [3].

Note que existe una biyección entre las clases de conjugación de S_n, los tipos de estructuras de ciclos de permutaciones en S_n y las particiones de n, donde una *partición* de n es un vector de enteros positivos $(n_1, \ldots, n_m)$ tal que

1. $n_1 \geq \cdots \geq n_m \geq 1$.
2. $n = n_1 + \cdots + n_m$.

Dada $\lambda = (n_1, \ldots, n_m)$ una partición de n, la *tabla de Young* de λ es el arreglo $\mathcal{T}_\lambda$ definido por

1	$\ldots$	$\ldots$	$\ldots$	n_1
$n_1 + 1$	$\ldots$	$\ldots$	$n_1 + n_2$	
$\vdots$		$\vdots$		
$\sum_{j \leq m-1} n_j + 1$	$\ldots$	n		

Sea λ una partición de n y sean $C_{\mathcal{T}_\lambda}$ y $F_{\mathcal{T}_\lambda}$ los subgrupos de S_n definidos por:

$$\begin{aligned} C_{\mathcal{T}_\lambda} &= \{\alpha \in S_n : \alpha \text{ deja invariantes las columnas de } \mathcal{T}_\lambda\} . \\ F_{\mathcal{T}_\lambda} &= \{\alpha \in S_n : \alpha \text{ deja invariantes las filas de } \mathcal{T}_\lambda\} . \end{aligned}$$

Note que $C_{\mathcal{T}_\lambda} \cap F_{\mathcal{T}_\lambda} = \{e\}$ y note que esto implica que $|C_{\mathcal{T}_\lambda} F_{\mathcal{T}_\lambda}| = |C_{\mathcal{T}_\lambda}|\,|F_{\mathcal{T}_\lambda}|$.

Dada λ una partición de n y $\mathcal{T}_\lambda$ su tabla de Young, ω_λ el *simetrizador de Young* asociado a λ es igual a

$$\sum_{p \in C_{\mathcal{T}_\lambda},\ q \in F_{\mathcal{T}_\lambda}} \operatorname{sign}(p) \operatorname{reg}_{S_n}(pq) .$$

Dado $V_\lambda = \operatorname{Im}(\omega_\lambda)$, la representación de Young asociada a λ es la representación $\rho_\lambda : S_n \to \operatorname{End}_{\mathbb{C}}(V_\lambda)$ definida por:

$$\text{Para todo } g \in S_n , \quad \rho_\lambda(g) := \operatorname{reg}_{S_n}(g)\, \omega_\lambda \restriction_{V_\lambda} .$$

Comentario 4. *El álgebra de Frobenius $\mathbb{C}[S_n]$ es el álgebra $\left\{\mathbb{C}^{n!}, +, \times\right\}$, donde $+$ es la suma vectorial en $\mathbb{C}^{n!}$ y $\times$ es la operación de multiplicación definida como sigue: dados $v = \sum_{\alpha \in S_n} v(\alpha)\,\alpha$ y $w = \sum_{\alpha \in S_n} w(\alpha)\,\alpha$ dos elementos de $\mathbb{C}[S_n]$, el producto de v y w, que denotaremos $v \times w$, es igual a $\sum_{\alpha \in S_n} s(\alpha)\,\alpha$, donde $s(\alpha) = \sum_{\beta \in S_n} v(\beta)\, w\left(\beta^{-1}\alpha\right)$.*

A continuación enunciaremos el teorema fundamental de la teoría de representaciones lineales de grupos simétricos. A este teorema lo llamaremos el Teorema de Frobenius en honor al precursor de la teoría. Para más información el lector interesado puede consultar [1].

Teorema 5 (Teorema de Frobenius). *Dado $n \in \mathbb{N}$ se tiene lo siguiente:*

1. *El número de representaciones irreducibles de S_n no equivalentes es igual al número de particiones de n.*
2. *Dada λ una partición de n, la representación ρ_λ es irreducible.*
3. *Dadas λ y μ dos particiones diferentes de n, las representaciones ρ_λ y ρ_μ son no equivalentes.*
4. $\dim(\rho_\lambda) = \frac{n!}{(\omega_\lambda \times \omega_\lambda)(e)}$, *donde ω_λ es la representación dada por*

$$\sum_{p \in C_{\mathcal{T}_\lambda},\ q \in F_{\mathcal{T}_\lambda}} sign(p)\, reg_{S_n}(pq) \ ;$$

el símbolo $\times$ denota la operación de multiplicación en el álgebra de Frobenius $\mathbb{C}[S_n]$ y dado $\phi \in \mathbb{C}[S_n]$, el símbolo $\phi(e)$ denota el coeficiente de ϕ asociado a e.

5. No existen ω-grupos aritméticos

En esta, la sección principal del artículo, mostraremos que no existen ω-grupos aritméticos. Una manera de interpretar este resultado es la siguiente: no existe un grupo elemental en el cual pueda ser embebido todo grupo finito. Tal interpretación resulta de identificar la no definida noción de grupo elemental con la noción de grupo aritmético. Tal identificación no es del todo descabellada dado que la clase de los grupos aritméticos es igual a la clase de lo que podríamos llamar los grupos concretos o numéricos, grupos cuyos elementos son objetos numéricos (elementos de un campo numérico) y cuyas operaciones son operaciones algebraicas naturales.

Lo que mostraremos en esta sección del artículo es que, si $\{\rho_n\}_{n\in\mathbb{N}}$ es una sucesión de representaciones tal que para todo $n \in \mathbb{N}$ se tiene que ρ_n es una representación cierta irreducible de S_n, entonces la sucesión $\{\dim(\rho_n)\}_{n\in\mathbb{N}}$ diverge a infinito. Note que esto claramente implica la no existencia de ω-grupos aritméticos.

Dada $\rho : S_n \to \mathrm{End}_{\mathbb{C}}(V)$ una representación, ρ es un homomorfismo y por lo tanto $\ker(\rho)$ es un subgrupo normal de S_n. Es bien sabido que si n es mayor o igual que 5 los únicos subgrupos normales de S_n son S_n, A_n y $\{e\}$, (para mayor información el lector puede consultar [3]). Esto nos permite clasificar las representaciones irreducibles de S_n, (con $n \geq 5$), en tres grupos, a saber:

1. ρ es de tipo 1 si y solo si $\ker(\rho) = S_n$.
2. ρ es de tipo 2 si y solo si $\ker(\rho) = A_n$.
3. ρ es de tipo 3 si y solo si $\ker(\rho) = \{e\}$.

Note que existe una única representación irreducible de tipo 1 (módulo isomorfismo), siendo esta la representación $\rho_0 : S_n \to \mathrm{End}_{\mathbb{C}}(\mathbb{C}) \approx \mathbb{C}$ dada por: para todo $\alpha \in S_n$

$$\rho_0(\alpha) = 1\,.$$

Note también que existe una única representación irreducible de tipo 2 (módulo isomorfismo), siendo esta la representación $\rho_1 : S_n \to \mathrm{End}_{\mathbb{C}}(\mathbb{C}) \approx \mathbb{C}$ dada por: para todo $\alpha \in S_n$

$$\rho_1(\alpha) = \begin{cases} 1 & \text{si } \alpha \in A_n\,, \\ -1 & \text{si } \alpha \notin A_n\,. \end{cases}$$

Note finalmente que las representaciones de tipo 3 son precisamente las representaciones irreducibles ciertas que deseamos estudiar.

Por otro lado podemos clasificar las particiones de n en tres grupos de la siguiente manera:

1. $(1, 1, \ldots, 1)$ es la única partición de tipo 1.

2. (n) es la única partición de tipo 2.

3. Toda otra partición es una partición de tipo 3.

Comentario 5. *Note que las particiones de tipo* 3 *son precisamente aquellas particiones cuyas tablas de Young contienen al menos dos filas y al menos dos columnas.*

Recuerde que existe una correspondencia biunívoca entre las representaciones irreducibles de S_n y las particiones de n. Es fácil verificar que la partición $(1,1,\ldots,1)$ corresponde a la representación ρ_0, i.e. si $(1,1,\ldots,1)=\lambda$, entonces $\rho_\lambda=\rho_0$. También es fácil verificar que la partición (n) corresponde a la representación ρ_1. Finalmente tenemos que las particiones de tipo 3 corresponden a las representaciones irreducibles de tipo 3, i.e. dada ρ una representación irreducible cierta, existe λ una partición de tipo 3 tal que $\rho_\lambda=\rho$.

Recuerde que $\dim(\rho_\lambda)=\frac{n!}{(\omega_\lambda\times\omega_\lambda)(e)}$. Lo que probaremos es que si $\{\rho_n\}_{n\geq 5}$ es una sucesión de representaciones irreducibles primitivas, (para todo $n\geq 5$, ρ_n es una representación de S_n) y $\{\lambda_n\}_{n\geq 5}$ es la sucesión de particiones asociada, entonces $\left\{\frac{n!}{(\omega_{\lambda_n}\times\omega_{\lambda_n})(e)}\right\}_{n\geq 5}$ es una sucesión que diverge a infinito. Lo que haremos a continuación es estimar la cantidad $(\omega_\lambda\times\omega_\lambda)(e)$.

Lema 6. $(\omega_\lambda\times\omega_\lambda)(e)\leq|C_{\mathcal{T}_\lambda}||F_{\mathcal{T}_\lambda}|$.

Demostración. Recuerde que ω_λ es igual a $\sum_{p\in C_{\mathcal{T}_\lambda},\ q\in F_{\mathcal{T}_\lambda}}\operatorname{sign}(p)\operatorname{reg}_{S_n}(pq)$, por lo tanto $\omega_\lambda\times\omega_\lambda$ es igual a

$$\sum_{p,p^*\in C_{\mathcal{T}_\lambda},\ q,q^*\in F_{\mathcal{T}_\lambda}}\operatorname{sign}(pp^*)\operatorname{reg}_{S_n}(pqp^*q^*).$$

Sea $A=\{(p,q,p^*,q^*):p,p^*\in C_{\mathcal{T}_\lambda};\ q,q^*\in F_{\mathcal{T}_\lambda}\ \text{y}\ pqp^*q^*=e\}$, note que $(\omega_\lambda\times\omega_\lambda)(e)=\sum_{(p,q,p^*,q^*)\in A}\operatorname{sign}(pp^*)$. Por otro lado, dado que $C_{\mathcal{T}_\lambda}\cap F_{\mathcal{T}_\lambda}=\{e\}$, tenemos que dados $p\in C_{\mathcal{T}_\lambda}$ y $q\in F_{\mathcal{T}_\lambda}$ el conjunto

$$\{(p^*,q^*)\in C_{\mathcal{T}_\lambda}\times F_{\mathcal{T}_\lambda}:pqp^*q^*=e\}$$

tiene tamaño a lo más uno. Tenemos entonces que $(\omega_\lambda\times\omega_\lambda)(e)\leq|A|\leq|C_{\mathcal{T}_\lambda}||F_{\mathcal{T}_\lambda}|$. ☑

Lema 7. *Dada* $\lambda=(n_1,\ldots,n_m)$ *una partición de* n, *se tiene que* $|F_{\mathcal{T}_\lambda}|=\prod_{i\leq m}n_i!$

Demostración. Dadas $F_1,\ldots,F_m$ las filas de la tabla de Young de λ, se tiene que $F_{\mathcal{T}_\lambda}$ es igual a $S_{F_1}\times\cdots\times S_{F_m}$, por lo tanto $|F_{\mathcal{T}_\lambda}|=|S_{F_1}\times\cdots\times S_{F_m}|=\prod_{i\leq m}|S_{F_i}|=\prod_{i\leq m}n_i!$ ☑

Dada $\lambda = (n_1, \ldots, n_m)$ una partición de n, la tabla de Young de λ posee n_1 columnas $C_1, \ldots, C_{n_1}$ que satisfacen lo siguiente:

1. $|C_1| \geq \cdots \geq |C_{n_1}| \geq 1$.
2. $n = \sum_{i \leq n_1} |C_i|$.

Esto es, $(|C_1|, \ldots, |C_{n_1}|)$ también es una partición de n que llamaremos la *partición dual* de λ y que denotaremos con el símbolo λ^*. Note que $C_{\mathcal{T}_\lambda}$ es isomorfo a $F_{\mathcal{T}_{\lambda^*}}$. Lo anterior implica que

$$|C_{\mathcal{T}_\lambda}| = \prod_{i \leq n_1} |C_i|!$$

Dada $\lambda = (n_1, \ldots, n_m)$ una partición, el símbolo $f(\lambda)$ denotará la cantidad $\prod_{i \leq m} n_i!$ y el símbolo $F(\lambda)$ denotará la cantidad $f(\lambda) f(\lambda^*)$. Si ponemos todas las piezas juntas obtenemos el siguiente lema.

Lema 8. *Dado $n \in \mathbb{N}$ y dada λ una partición de n, se tiene que $|C_{\mathcal{T}_\lambda}| |F_{\mathcal{T}_\lambda}| = F(\lambda)$.*

Tenemos entonces que para toda partición λ, se tiene lo siguiente:

$$\dim(\rho_\lambda) = \frac{n!}{(\omega_{\lambda_n} \times \omega_{\lambda_n})(e)} \geq \frac{n!}{F(\lambda)}.$$

Recuerde que el principal objetivo de este escrito consiste en probar que no existen ω-grupos aritméticos y que para ello es suficiente probar que no existe $k \in \mathbb{N}$ tal que todo grupo simétrico puede ser embebido en $GL_{\mathbb{C}}(k)$. Para probar esto último basta con probar el teorema combinatorio que enunciamos a continuación y cuya prueba pospondremos hasta la última sección de este artículo.

Teorema 6. *Sea $\{\lambda_n\}_{n \in \mathbb{N}}$ una sucesión tal que, para todo $n \in \mathbb{N}$, λ_n es una partición de n de tipo 3, se tiene entonces que la sucesión $\left\{\frac{n!}{F(\lambda_n)}\right\}_{n \in \mathbb{N}}$ diverge a infinito.*

Corolario 2. *Sea $\{\rho_n\}_{n \in \mathbb{N}}$ una sucesión tal que, para todo $n \in \mathbb{N}$, ρ_n es una representación cierta de S_n, se tiene entonces que la sucesión $\{\dim(\rho_n)\}_{n \in \mathbb{N}}$ diverge a infinito.*

Demostración. Dada $\{\rho_n\}_{n \in \mathbb{N}}$ nuestra sucesión, existe una sucesión $\{\rho_n^*\}_{n \in \mathbb{N}}$ de representaciones ciertas irreducibles y tales que, para todo $n \in \mathbb{N}$, $\dim(\rho_n^*) \leq \dim(\rho_n)$. Para todo $n \geq 5$, la representación ρ_n^* es de tipo 3 y por lo tanto, la

partición λ_n asociada a ρ_n^* es una partición de tipo 3. Tenemos entonces que para todo $n \geq 5$

$$\dim(\rho_n) \geq \dim(\rho_n^*) \geq \frac{n!}{F(\lambda_n)}.$$

Finalmente tenemos que la sucesión $\{\dim(\rho_n)\}_{n\in\mathbb{N}}$ diverge a infinito dado que así lo hace la sucesión $\left\{\frac{n!}{F(\lambda_n)}\right\}_{n\in\mathbb{N}}$. ☑

Del corolario anterior podemos obtener fácilmente la prueba del siguiente teorema, el cual es de por sí el teorema central de este escrito.

Teorema 7. *No existen ω-grupos aritméticos.*

6. Una desigualdad combinatoria

En lo que sigue probaremos que si $\{\lambda_n\}_{n\in\mathbb{N}}$ es una sucesión tal que, para todo $n \in \mathbb{N}$, la partición λ_n (partición de n) es de tipo 3, entonces la sucesión $\left\{\frac{n!}{F(\lambda_n)}\right\}_{n\in\mathbb{N}}$ diverge a infinito.

Lo que probaremos es que si λ es una partición de tipo 3 de $n \geq 16$, entonces $F(\lambda) \leq (n-1)!2$. Esto implica que si $\{\lambda_n\}_{n\in\mathbb{N}}$ es una sucesión de particiones, tal que para todo $n \in \mathbb{N}$, λ_n es una partición de n de tipo 3, entonces la sucesión $\left\{\frac{n!}{F(\lambda_n)}\right\}_{n\geq 16}$ está acotada inferiormente por la sucesión $\left\{\frac{n}{2}\right\}_{n\geq 16}$ que diverge a infinito.

Comentario 6. *Si $\lambda = (n_1, \ldots, n_m)$ es una partición de n se tiene lo siguiente:*

$$F(\lambda) = \left(\prod_{i\leq m} n_i!\right)\left(\prod_{i\leq m} i^{n_i}\right).$$

Para empezar consideraremos las sucesiones λ de tipo 3 que constan de dos sumandos distintos, de ellas probaremos que satisfacen la desigualdad $F(\lambda) \leq (n-1)!2$.

Lema 9. *Dada $\lambda = (m, k)$ una partición de $n \geq 16$, con $m \gneqq k$, se tiene que $F(\lambda) \leq (n-1)!2$.*

Demostración. Note que $F(\lambda) = m!k!2^k$ y que $k \leq \frac{n-1}{2}$. Esto implica que

$$2k \leq m+k-1, \quad 2(k-1) \leq m+k-2 \quad , \ldots, \quad 2\cdot 2 \leq m+1.$$

Tenemos entonces que

$$\begin{aligned} F(\lambda) &= m!(2)(2\cdot 2)(2\cdot 3)\cdots(2\cdot k) \\ &\leq m!(2)(m+1)(m+2)\cdots(m+k-1) \\ &= (n-1)!2. \end{aligned}$$

☑

A continuación probaremos que si $n = mk \geq 16$, con $m, k \geq 2$, entonces la partición $\mu = (m, \ldots, m)$ satisface la desigualdad $F(\mu) \leq (n-1)!2$.

Lema 10. *Dada $\mu = (m, \ldots, m)$ partición de $n = mk$ (con $m, k \geq 2$ y $n \geq 16$), se tiene que $F(\mu) \leq (n-1)!2$.*

Demostración. Note primero que $F(\mu) = (m!)^k (k!)^m$. Probaremos por inducción sobre k que

$$(m!)^k (k!)^m \leq (km-1)!2\,.$$

1. Caso $k = 2$. Note que

   $$(m!)^2 2^m = 1 \cdot 2 \cdot \ldots \cdot m \cdot 2(1) \cdot 2(2) \cdot \ldots \cdot 2(i) \cdot \ldots \cdot 2(m)\,.$$

   Note que para todo $i \leq m-1$, se tiene que $2(i) \leq m+i-1$; tenemos entonces que

   $$2(2)\,2 \leq m+1\,,$$

   dado que $m+1 \geq \frac{n}{2} \geq 8$. Adicionalmente tenemos que

   $$\begin{aligned} 2(m-1) &\leq 2m-2, \\ 2(m) &\leq 2(2m-1)\,. \end{aligned}$$

   Por lo tanto

   $$\begin{aligned} (m!)^2 2^m &= 1 \cdot 2 \cdot \ldots \cdot m \cdot 2(1) \cdot 2(2) \cdot \ldots \cdot 2(i) \cdot \ldots \cdot 2(m) \\ &\leq 1 \cdot \ldots \cdot m \cdot m+1 \cdot \ldots \cdot m+i \cdot \ldots \cdot 2m-2 \cdot 2(2m-1) \\ &= (2m-1)!2\,. \end{aligned}$$

2. (Hipótesis de inducción) Supondremos para todo $k \leq i$, que $(m!)^k (k!)^m \leq (mk-1)!2$.

3. (Caso $k = i+1$) Tenemos que

   $$\begin{aligned} (m!)^{i+1} ((i+1)!)^m &= (m!)^i (i!)^m (m!)(i+1)^m \\ &\leq 2((mi-1)!)(mi)(mi+1)\cdots(m(i+1)-1)\,. \end{aligned}$$

   Lo que debemos verificar para terminar la prueba es que:

   $$(m!)(i+1)^m \leq (mi)(mi+1)\cdots(m(i+1)-1)\,. \qquad \text{(Ec. 1)}$$

   Note que

   $$(m!)(i+1)^m = (i+1)(2(i+1))\cdots(m(i+1))\,.$$

   Es claro que, si $l \leq m-1$, entonces $(i+1)l \lneqq mi+l-1$. Es fácil verificar que esto implica la desigualdad (Ec. 1), dado que si $(a_1, \ldots, a_m)$ y $(b_1, \ldots, b_m)$ son dos sucesiones finitas crecientes de números naturales que satisfacen:

- $a_i \lneqq b_i$, para todo $i \leq m-1$.
- $a_m = b_m + 1$.

entonces $\prod_{i \leq m} a_i \leq \prod_{i \leq m} b_i$. ☑

Teorema 8. *Dada λ una partición de n, (con $n \geq 16$), si λ es de tipo 3, se tiene entonces que $F(\lambda) \leq 2(n-1!)$.*

Demostración. La prueba es por inducción sobre n.

1. ($n = 16, 17, \ldots, 23$) La verificación es engorrosa dado el gran número de particiones de $16, 17, \ldots, 22$ y 23; aún así es posible verificar computacionalmente que si λ es una partición de $n \in \{16, 17, \ldots, 23\}$, de tipo 3, entonces $F(\lambda) \leq (n-1)!2$. (El autor realizó tal verificación usando su computador personal y un algoritmo elemental que lista todas las particiones en cuestión y realiza la verificación aritmética correspondiente).

2. (Hipótesis de inducción) Supondremos que para todo n, si $23 \leq n \leq i-1$ y λ es una partición de n de tipo 3, entonces $F(\lambda) \leq (n-1)!2$.

3. ($n = i \geq 24$) Sea $\lambda = (n_1, \ldots, n_k)$ una partición de n de tipo 3, si $k = 2$ el primer lema de esta sección asegura que $F(\lambda) \leq (n-1)!2$. Por otro lado, si $n_1 = n_2 = \cdots = n_k$, el segundo lema de esta sección garantiza que $F(\lambda) \leq (n-1)!2$. Supondremos entonces que $k \geq 3$ y que $n_k \lneqq n_1$. Considere $\xi = (n_1, \ldots, n_{k-1})$, note que ξ es una partición de $n - n_k$ de tipo 3; note también que $n - n_k \geq 16$. De la hipótesis de inducción tenemos que

$$F(\xi) = n_1!...n_{k-1}!1^{n_1}...(k-1)^{n_{k-1}} \leq (n - n_k - 1)!2\,.$$

Además $n_k \leq \frac{n-1}{k}$, esto implica que

$$\begin{aligned} n_k k &\leq n-1, \\ (n_k - 1)\,k &\leq n-2, \\ &\vdots \\ 2k &\leq n - (n_k - 1)\,, \\ k &\leq n - n_k\,. \end{aligned}$$

Por otro lado

$$\begin{aligned} F(\lambda) &= F(\xi)\, n_k!k^{n_k} = F(\xi)\,(1k)\,(2k)...(n_k k) \\ &\leq (n - n_k - 1)!2\,(n - n_k)\,(n - (n_k - 1))...(n-1) \\ &= (n-1)!2\,. \end{aligned}$$

Con esto hemos terminado la prueba del teorema.

☑

Corolario 3. *Sea* $\{\lambda_n\}_{n\in\mathbb{N}}$ *una sucesión tal que para todo* $n \in \mathbb{N}$, λ_n *es una partición de* n *de tipo* 3*, se tiene entonces que la sucesión* $\left\{\frac{n!}{F(\lambda_n)}\right\}_{n\in\mathbb{N}}$ *diverge a infinito.*

Agradecimientos: El autor agradece a la Universidad Industrial de Santander por brindarle las facilidades que hicieron posible la realización de este artículo, en particular el apoyo económico otorgado por medio del proyecto VIE-UIS 5153-07. El autor también quisiera agradecer a los integrantes del seminario *Matemáticas Discretas-UIS,* especialmente a Rafael Isaacs quien en el seminario sugirió un problema similar concerniente a la existencia de ω-grupos.

Referencias

[1] W. Fulton and J. Harris, *Representation theory: A first course*, Springer Verlag, N. Y., 1991.

[2] W. Hodges, *Model theory*, Cambridge University Press, Cambridge M. A., 1993.

[3] T. Hungerford, *Algebra*, Springer Verlag, N. Y., 2000.

[4] R. Kallman, *Every reasonably sized group is a subgroup of* s_ω, Fundamenta Mathematicae **164** (2000), 35–40.

[5] R. Mauldin (ed.), *The scotish book*, Birkhauser, Boston, 1981.

(Recibido en abril de 2008. Aceptado en enero de 2009)

Escuela de Matemáticas, Universidad Industrial de Santander
Carrera 27, Calle 9ª
Bucaramanga
e-mail: juamonto@uis.edu.co