Universidad Autónoma de Zacatecas

Unidad Académica de Matemáticas

Sobre raíces k-ésimas en el grupo simétrico y en el grupo alternante

TESIS

QUE PARA OBTENER EL TÍTULO DE:

Maestra en Ciencias

PRESENTA:

Betsy Melany Licón Rodríguez

DIRECTOR DEL TRABAJO:
Dr. Luis Manuel Rivera Martínez

Zacatecas, Zac. Diciembre 2018

Índice

Introducción

Sea G un grupo y k un entero positivo. Para un elemento g de G, decimos que h es una raíz k-ésima de g si se cumple que $h^k = g$. Es un problema clásico determinar cuando un elemento de G tiene o no raíz k-ésima en G y en su caso calcular el número de dichas raíces (ver, por ejemplo, [7, 9, 10, 17, 18, 27, 28]). Uno de los grupos más estudiados en este sentido es el grupo simétrico que consiste de todas las biyecciones de un conjunto finito X de carnalidad n y la composición de funciones como operación binaria. El grupo simétrico se denota por S_n y a sus elementos se les conoce como permutaciones. Es conocido que las permutaciones se pueden clasificar en permutaciones pares y permutaciones impares. El conjunto de las permutaciones pares es un subgrupo del grupo simétrico al cual se le conoce como grupo alternante y se denota por A_n. En los artículos [4, 5, 6, 8, 20, 21, 24, 25, 33, 34] se pueden encontrar resultados relacionados con raíces en el grupo simétrico.

Se conocen caracterizaciones que permiten determinar cuando una permutación tiene raíz k-ésima, por ejemplo en el libro de Wilf [35] aparece una que se atribuye a A. Knofmacher y R. Warlimontel. Otra demostración similar aparece en el artículo publicado en 2009 por Annin et al. [3]. Para el caso del grupo alternante también se conocen resultados al respecto. Pournaki [23] da una caracterización de las permutaciones pares que tienen raíz cuadrada en A_n y en Annin et al. [3] presentan las condiciones necesarias y suficientes para que una permutación par tenga raíz k-ésima par.

Existen varias fórmulas para calcular el número de raíces en el grupo simétrico [15, 21, 25]. Para este trabajo se hizo un análisis a detalle del artículo "On the number of mth roots of permutations" publicado en 2012 por Leaños et al. [15], y en el capítulo 2 se presentan muchos de los resultados expuestos en dicho artículo así como una demostración ligeramente distinta al teorema de su resultado principal (fórmula sobre el número de raíces m-ésimas de una permutación), misma que ellos solo bosquejan.

La determinación del número de dichas raíces puede tener diversas aplicaciones. Se conocen aplicaciones en la teoría matemática de la música [12], en criptografía [1, 13] y en problemas relacionados con la teoría de representaciones del grupo simétrico. En este último caso, la fórmula del número de raíces cuadradas de una permutación, aparece en los artículos [2, 19] asociadas a problemas sobre modelos de Gelfand.

A nuestro conocimiento no se han publicado resultados generales sobre el número de raíces pares de permutaciones en el grupo alternante (se conocen resultados para el caso de la permutación identidad [20]) por lo que se considera importante obtener

resultados sobre este problema.

La contribución principal de esta tesis es la siguiente:

- Se obtienen fórmulas exactas para calcular el número de raíces k-ésimas, pares e impares, para casos particulares de permutaciones. Posteriormente se conjuntan estas fórmulas en una sola para calcular el número de raíces pares de cualquier permutación par (sección 3.2.2).
- Se obtienen funciones generadoras exponenciales para el número de raíces k-ésimas (pares o impares) de permutaciones de cierto tipo (sección 3.2.2).

Wilf describe en [35] a una función generadora como un tendedero en el que colgamos una sucesión de números para su visualización. Está concepción se refiere al hecho de que podemos "codificar" todos los elementos de una sucesión posiblemente infinita mediante una sola función, la función generadora de dicha sucesión. De lo anterior es la importancia de obtener funciones generadoras.

Capítulo 1

Preliminares

En este capítulo se introduce la terminología, definiciones y notación básicas sobre las que se desarrolla el resto de la tesis. La primera sección se centra en exponer definiciones y conceptos básicos, así como resultados clásicos o conocidos respecto al grupo simétrico. La segunda sección se enfoca en la teoría básica sobre funciones generadoras exponenciales que es de utilidad en el presente trabajo.

1.1 Conceptos básicos sobre el grupo simétrico

El contenido de esta sección tiene la intención de brindar la información necesaria para familiarizarse con el principal objeto de estudio de esta tesis: el grupo simétrico. El material presentado a continuación aparece en muchos textos clásicos que abordan al grupo simétrico, este texto en su mayoría está basado en los libros de Rotman [26] y Sagan [29].

En lo que sigue, usaremos $[n]$ para denotar al conjunto $\{1, ..., n\}$.

Definición 1.1. *El* ***Grupo Simétrico****, S_n, consiste de todas las funciones biyectivas de $[n]$ sobre $[n]$ junto con la composición de funciones como multiplicación. A estas funciones biyectivas se les conoce como* ***permutaciones****.*

Nota:. *En esta tesis se hará la composición de dos permutaciones α y β de la siguiente manera:*

$$(\alpha\beta)(x) = \alpha(\beta(x))$$

Definición 1.2. *Un* ***punto fijo*** *de la permutación $\sigma \in S_n$ es un punto $i \in [n]$ tal que $\sigma(i) = i$.*

Un tipo especial de permutaciones son las conocidas como ciclos.

Definición 1.3. *Sean $a_1, \ldots, a_\ell$ enteros distintos entre 1 y n. Sea $\sigma \in S_n$, tal que*

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_{\ell-1}) = a_\ell, \sigma(a_\ell) = a_1$$

*y todo $x \in [n] - \{a_1, \ldots, a_\ell\}$ es un punto fijo, entonces decimos que σ es un ℓ-**ciclo**; o también decimos que es un ciclo de **longitud** ℓ. Se denota a σ por $(a_1\, a_2 \ldots\, a_\ell)$.*

Cualquier 1-ciclo fija a todos los elementos de $[n]$ y por tanto es igual a la identidad, que se denota por Id. A un 2-ciclo se le llama **transposición**.

Notación. *Si $\alpha = (a_1 \ldots a_\ell)$ es un ℓ-ciclo, usaremos* $\mathrm{set}(\alpha)$ *para denotar al conjunto $\{a_1, \ldots, a_\ell\}$. Diremos que α tiene al elemento a, o que a es un punto o elemento en el ciclo α, si $a \in \mathrm{set}(\alpha)$.*

La siguiente definición es importante para la expresión de permutaciones.

Definición 1.4. *Dos ciclos $\alpha, \beta \in S_n$ son **disjuntos** si para cada $x \in [n]$ tal que $\alpha(x) \neq x$ entonces $\beta(x) = x$ y, de manera recíproca, si para todo $y \in S_n$ tal que $\beta(y) \neq y$ se tiene que $\alpha(y) = y$. Decimos que una familia de ciclos $\alpha_1, \ldots, \alpha_h \in S_n$ son **disjuntos** si cualesquiera dos ciclos α_i y α_j, con $i \neq j$, son disjuntos.*

Por supuesto que la definición anterior admite que exista $z \in [n]$ tal que $\alpha(z) = z = \beta(z)$.

El siguiente teorema nos permite expresar a toda permutación en términos de ciclos, es un resultado clásico y se enuncia sin demostración. Si el lector lo desea puede consultar una demostración en [11], en las secciones 1.3 (descomposición) y 4.1 (unicidad).

Teorema 1.5. *Cualquier permutación $\sigma \in S_n$ es un ciclo o bien un producto de ciclos disjuntos, y dicho producto es único salvo reordenamiento de los factores.*

El teorema anterior da una manera particularmente útil de representar a una permutación.

Definición 1.6. *La **factorización completa** de una permutación σ es la representación de σ como producto de ciclos disjuntos y que contiene un 1-ciclo (i) para todo punto fijo i de σ.*

Existen diferentes formas de denotar a las permutaciones.

Notación. *Si σ es una permutación en S_n, existen tres diferentes formas para expresar a este elemento:*

- *Notación de doble línea:*

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

- *En notación de lista o en una línea:*

$$\sigma = \sigma(1)\, \sigma(2) \ldots \sigma(n)$$

- *Notación cíclica:*

$$\sigma = \alpha_1\, \alpha_2 \cdots \alpha_k,$$

donde los $\alpha_1, \alpha_2, \ldots, \alpha_k \in S_n$ *y son los ciclos que aparecen en la factorización completa de* σ*.*

Nota: *Existe una convención respecto a omitir los* 1*-ciclos en la notación cíclica de una permutación.*

El ejemplo a continuación nos ilustra el empleo de la notación antes descrita.

Ejemplo 1.1.1. *Si* $\sigma \in S_6$ *está dada por*

$$\sigma(1) = 2 \qquad \sigma(2) = 3 \qquad \sigma(3) = 1 \qquad \sigma(4) = 5 \qquad \sigma(5) = 4 \qquad \sigma(6) = 6.$$

Entonces usando la notación de dos lineas tenemos que

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 4 & 6 \end{pmatrix},$$

con la notación de una línea o de lista

$$\sigma = 231546$$

y con la notación cíclica

$$\sigma = (1\,2\,3)(4\,5)$$

La siguiente definición nos permite describir a las permutaciones en función de la agrupación de sus ciclos por longitudes. Como se verá en los capítulos posteriores, está descripción de las permutaciones resulta muy conveniente para simplificar el lenguaje de este escrito.

Definición 1.7. *Diremos que* $\sigma = \sigma_1 \ldots \sigma_m$ *es la* ***factorización completa por longitudes*** *de* σ*, si la factorización completa de* σ *se puede expresar como* $\sigma_1 \cdots \sigma_m$*, en donde cada* $\sigma_i \in S_n$ *expresa el producto de todos los ciclos disjuntos de longitud* ℓ_i *de* σ*.*

La última definición se ejemplifica enseguida.

Ejemplo 1.1.2. *La permutación* $\sigma = (1\,2\,3\,4)(5\,6)(7\,8)(9\,10\,11)(12\,13\,14) \in S_{18}$*, tiene la siguiente factorización completa por longitudes*

$$\sigma = \sigma_1\sigma_2\sigma_3\sigma_4,$$

donde $\sigma_1 = (15)(16)(17)(18)$*,* $\sigma_2 = (5\,6)(7\,8)$*,* $\sigma_3 = (9\,10\,11)(12\,13\,14)$ *y* $\sigma_4 = (1\,2\,3\,4)$*.*

La definición que sigue está directamente asociada con la factorización completa de una permutación.

Definición 1.8. *Diremos que una permutación es de* **tipo de ciclo** *(o simplemente de* **tipo***)* $\mathbf{c} = (c_1, \ldots, c_n)$ *si en su factorización completa tiene* c_ℓ *ciclos de longitud* ℓ*, para cada* $\ell \in [n]$ *y* $n = \sum_{\ell=1}^{n} \ell c_\ell$*. En ocasiones también diremos que una permutación* σ *es del* **tipo** $(\ell_1)^{m_1} \ldots (\ell_j)^{m_j}$ *para indicar que* σ *tiene exactamente* $m_i > 0$ *ciclos de longitud* ℓ_i *en su factorización completa.*

Ejemplo 1.1.3. *La permutación* $\sigma = (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9\ 10) \in S_{12}$ *es de tipo* $(2, 0, 2, 1, 0, 0, 0, 0, 0, 0, 0, 0)$ *o del tipo* $(1)^2(3)^2(4)^1$*.*

El lema 1.9 y teorema 1.10 aparecen en el libro "An introduction to the Theory Groups" [26], y se enuncian sin demostración.

Lema 1.9. *Si* $\sigma, \pi \in S_n$*, entonces* $\sigma\pi\sigma^{-1}$ *es la permutación con el mismo tipo de ciclo que* π *la cual es obtenido aplicando* σ *a los elementos en* π*.*

Teorema 1.10. *Las permutaciones* σ *y* π *son conjugadas si y solo si tienen el mismo tipo de ciclo.*

El grupo alternante

Las transposiciones son de particular interés dado que generan a S_n como grupo.

Teorema 1.11. *Cualquier permutación* $\sigma \in S_n$ *es un producto de transposiciones.*

Para ver que cualquier permutación se descompone como producto de transposiciones basta ver que todo ciclo lo hace. Por ejemplo

$$(a_1\, a_2 \ldots a_k) = (a_1\, a_2)(a_2\, a_3) \ldots (a_{k-1}\, a_k)$$

Este tipo de descomposición nos permite clasificar a los elementos del grupo simétrico.

Definición 1.12. *Una permutación* $\sigma \in S_n$ *es una* ***permutación par*** *si es producto de un número par de transposiciones. En otro caso es una* ***permutación impar****.*

La descomposición en transposiciones de una permutación no es única, como tampoco es único el número de transposiciones que integran la descomposición. Sin embargo la paridad del número de transposiciones de la descomposición sí está determinada. Esto último se enuncia en el siguiente teorema.

Teorema 1.13. *Cualquier permutación* $\sigma \in S_n$ *es par, o bien impar.*

Para una demostración se puede consultar el teorema 1.7 en [26]. Los enunciados y definiciones presentados en este apartado dan la pauta para definir al grupo alternante.

Teorema 1.14. *El conjunto de todas las permutaciones pares de* S_n *se denota por* A_n *y es un subgrupo de* S_n*. Al grupo* A_n *se le llama* ***grupo alternante.***

La siguiente observación es relevante pues en el resto de este escrito consideraremos a toda permutación expresada en su factorización completa, a menos que se indique algo distinto.

Observación 1.15.

- *Un ciclo de longitud par es una permutación impar.*
- *Un ciclo de longitud impar es una permutación par.*
- *El producto de dos permutaciones con la misma paridad es una permutación par.*
- *El producto de dos permutaciones con distinta paridad es una permutación impar.*

Raíz k-ésima de una permutación

Como se mencionó antes, dado un grupo, es un problema clásico determinar el número de raíces k-ésimas para un elemento de este grupo. A continuación se formaliza esta idea para el caso en que el grupo dado es el simétrico.

Definición 1.16. *Sea k un entero positivo fijo, diremos que una permutación $\sigma \in S_n$ tiene una **raíz k-ésima** o que σ es una **potencia k-ésima** si existe una permutación τ tal que $\tau^k = \sigma$.*

La siguiente proposición muestra el resultado de elevar un ciclo a una potencia.

Proposición 1.17. *Sea $\alpha = (a_0\, a_1 \dots a_{\ell-1})$ un ℓ-ciclo. Para toda $i, k \geq 0$ se cumple que $\alpha^k(a_i) = a_{(i+k) \bmod \ell}$.*

Demostración: La demostración es por inducción sobre k. Para $k = 1$ se tiene por definición de ciclo que $\alpha(a_i) = a_{(i+1) \bmod \ell}$. Suponemos que se cumple para $k-1$. Entonces

$$\alpha^k(a_i) = \alpha\, \alpha^{k-1}(a_i) = \alpha(a_{(i+k-1) \bmod \ell}) = a_{((i+k-1)+1) \bmod \ell} = a_{(i+k) \bmod \ell}.$$

□

Los siguientes dos lemas son clásicos y serán de utilidad en algunas demostraciones posteriores.

Lema 1.18. *Sea $\sigma \in S_n$ un ciclo de longitud m y sea k un entero positivo. Si el $\mathrm{mcd}(k, m) = 1$ entonces σ tiene una raiz k-ésima en S_n.*

Demostración: Si $\mathrm{mcd}(m, k) = 1$ entonces, por la propiedad de Bézout, existen enteros a y b tales que

$$am + bk = 1$$

entonces

$$\sigma^1 = \sigma^{am+bk} = \sigma^{am}\sigma^{bk}$$

pero $\sigma^{am} = e$, por tanto

$$\sigma^1 = \sigma^{bk} = (\sigma^b)^k,$$

es decir, σ^b es una raiz k-ésima de σ, en donde b se puede tomar como el entero positivo más pequeño que satisface $bk \equiv 1 \pmod{m}$.

□

Lema 1.19. *Si $\sigma \in S_n$ es un ciclo de longitud m y k un entero positivo, entonces la factorización completa de σ^k tiene $\mathrm{mcd}(m,k)$ ciclos disjuntos, cada uno de longitud $\frac{m}{\mathrm{mcd}(m,k)}$.*

Demostración: Si $m = 1$ entonces σ es la identidad y el lema se cumple. Para $m > 1$, podemos escribir

$$\sigma = (a_0 \dots a_{m-1}).$$

Como todos los puntos fijos de σ (si alguno) son puntos fijos en σ^k, solo nos falta saber que pasa en σ^k con los puntos en $\{a_0, \dots, a_{m-1}\}$. Sea α el ciclo en la factorización completa de σ^k que contiene al elemento a_x, con $0 \leq x \leq m-1$, y ℓ la longitud de α. Por la proposición 1.17 tenemos que $\mathrm{set}(\alpha) = \{a_{(x+rk)(\bmod\ m)} : r \in \mathbb{N}\}$. Notemos que ℓ es el entero positivo más pequeño que satisface $x + \ell k \equiv x (\bmod\ m)$. Como $\ell k \equiv 0 (\bmod\ m)$ tenemos que ℓ debe ser el entero positivo más pequeño tal que $m | \ell k$ por lo que $\ell k = \mathrm{mcm}(k,m)$. Por otro lado $\mathrm{mcm}(k,m) = \frac{km}{\mathrm{mcd}(k,m)}$, entonces $\ell k = \frac{km}{\mathrm{mcd}(k,m)}$ y por tanto $\ell = \frac{m}{\mathrm{mcd}(m,k)}$. Esto implica que σ^k es un producto de ciclos disjuntos de longitud $\frac{m}{\mathrm{mcd}(m,k)}$ y como $|\sigma| = m$, la cantidad de estos ciclos debe ser exactamente $\mathrm{mcd}(m,k)$. □

El siguiente resultado una consecuencia directa de los lemas 1.18 y 1.19.

Corolario 1.20. *Sea $\sigma \in S_n$ un ciclo de longitud m. Si $\mathrm{mcd}(n,k) = 1$, entonces σ tiene una única raíz k-ésima.*

1.2 Funciones Generadoras

Las funciones generadoras nos brindan una manera de "codificar" todos los elementos de una sucesión posiblemente infinita mediante una sola función. En particular las funciones generadoras presentadas en este trabajo nos permiten obtener una serie de valores asosciados al número de raíces k-ésimas para cierto k y cierto tipo de permutaciones. El contenido de esta sección es breve dado que solo se han incluido las definiciones y proposiciones elementales para comprender los resultados que involucran a las funciones generadoras exponenciales en esta tesis. No se incluyen demostraciones, pero éstas se pueden consultar, por ejemplo, en las secciones 7 y 8 del libro de Loehr []. En esta tesis consideramos que el conjunto de los números naturales $\mathbb{N}$ incluye al cero. En esta sección un anillo R se considera no trivial y con unidad.

Partiremos de la definición de series de potencias formales.

Definición 1.21. *Una **serie de potencias formal** en un anillo R es una función $f : \mathbb{N} \to R$. Escribimos $f(n)$ o f_n para el valor de la función en la entrada $n \in \mathbb{N}$.*

Si $\{f(n)\}_{n\geq 0}$ es una serie de potencias formal, se acostumbra denotarla por

$$F(x) = \sum_{n=0}^{\infty} f_n x^n$$

y llamamos a f_n el coeficiente de x^n en F. El conjunto de todas las series de potencias formales sobre R se denota por $R[[x]]$, donde x es un símbolo llamado ***indeterminada*** o ***variable***. Dos series de potencias formales $F, G \in K[[x]]$ son iguales si y solo si $f_n = g_n$ para toda $n \in \mathbb{N}$; esto se sigue de la definición de igualdad de dos funciones con dominio $\mathbb{N}$.

Podemos sumar y multiplicar series formales de potencias.

Definición 1.22. *Dadas $F(x), G(x) \in R[[x]]$. Se define la suma $F(x) + G(x)$ como*

$$\sum_{n\geq 0} f_n x^n + \sum_{n\geq 0} g_n x^n = \sum_{n\geq 0} (f_n + g_n) x^n;$$

y el producto $F(x)G(x)$ se define por

$$\left(\sum_{n\geq 0} f_n x^n\right)\left(\sum_{n\geq 0} g_n x^n\right) = \sum_{n\geq 0}\left(\sum_{i+j=n} f_i g_j\right) x^n.$$

El conjunto de todas las series de potencias formales tiene la siguiente estructura algebraica.

Teorema 1.23. *El conjunto $R[[x]]$ es un anillo conmutativo con las operaciones de suma y producto de potencias formales.*

El anillo $R[[x]]$ no es un campo porque, por ejemplo, x no tiene recíproco, esto es, no existe $F \in R[[x]]$ tal que $x \cdot F = F \cdot x = 1$. Si $F(x)$ es unidad en $R[[x]]$ denotaremos por $F(x)^{-1}$ o $\frac{1}{F(x)}$ a su recíproco. La siguiente proposición nos dice cuando un elemento en $R[[x]]$ tiene recíproco, para R un campo.

Proposición 1.24. *Una serie de potencias formal $F = \sum_{n\geq 0} f_n x^n$ con coeficientes en un campo, tiene un recíproco si y solo si $f_n \neq 0$. En tal caso el recíproco es único.*

El siguiente enunciado es la proposición 5.1.3 del libro Enumerative Combinatorics de Stanley [32] y se usa en la demostración del teorema 2.26.

Teorema 1.25. *Sea K un campo de característica cero y sean $f_i : \mathbb{N} \to K$ funciones, $1 \leq i \leq k$. Definimos $h : \mathbb{N} \to K$ por*

$$h(n) = \sum f_1(|A_1|) f_2(|A_2|) \cdots f_k(|A_k|),$$

donde la suma corre sobre todas las particiones ordenadas débiles $(A_1, A_2, \ldots, A_k)$ *de* $[n]$ *en* k *partes. Sean* $F_i(x)$ *y* $H(x)$ *las funciones generadoras de las sucesiones* $f_i(n)$ *y* $h(n)$*. Entonces tenemos*

$$H(x) = F_1(x) \ldots F_k(x)$$

Como se mencionó al inicio de la sección, podemos codificar los elementos de una serie en una única función, dicha funciń se define con la ayuda de las series de potencias formales.

Definición 1.26. *Sea* $\{a_n\}_{n\geq 0}$ *una serie de números complejos. La* ***función generadora ordinaria*** *de dicha serie es la serie de potencias formal*

$$\sum_{n\geq 0} a_n x^n.$$

Ejemplo 1.2.1. *Para la serie* $\{1\}_{n\geq 0}$ *tenemos que su función generadora ordinaria es*

$$\sum_{n\geq 0} x^n = \frac{1}{(1-x)}$$

porque

$$(1-x)(1+x+x^2+\ldots) = 1$$

Definimos la serie de potencias conocida como exponencial de x por

$$e^x = \sum_{n\geq 0} \frac{x^n}{n!}.$$

Otras series de potencias formales que se usan en este trabajo son el coseno y seno hiperbólicos, que se definen como sigue:

$$\cosh(x) = \sum_{n\geq 0} \frac{x^{2n}}{(2n)!},$$

$$\sinh(x) = \sum_{n\geq 0} \frac{x^{2n+1}}{(2n+1)!};$$

y por tanto se tiene la siguiente identidad

$$e^x = \cosh(x) + \sinh(x).$$

Observación 1.27. *Notemos que* $\cosh(x)$ *(resp.* $\sinh(x)$*) consiste de todos los términos de* e^x *que son potencia par (resp. impar) de* x*.*

Otro tipo de función generadora, la cuál se usa en los resultados de funciones generadoras presentados en esta tesis, se define enseguida.

Definición 1.28. *Sea $\{a_n\}_{n\geq 0}$ una serie de números complejos. La **función generadora exponencial** de dicha serie es la serie de potencias formal*

$$\sum_{n\geq 0} a_n \frac{x^n}{n!}.$$

Ejemplo 1.2.2. *Para la serie $\{1\}_{n\geq 0}$ tenemos que su función generadora exponencial es*

$$\sum_{n\geq 0} \frac{x^n}{n!} = e^x$$

Se puede definir a las series de potencias formales en varias variables.

Definición 1.29. *Una **serie de potencias formal en m variables** con coeficientes en un anillo R es una función $f\colon \mathbb{N}^m \to R$. El conjunto de todas las series de potencias formales en m variables con coeficientes en R se denota por $R[[x_1, \ldots, x_m]]$.*

A una serie $F \in R[[x_1, \ldots, x_m]]$ se denota por

$$F = \sum_{f(n_1,\ldots,n_m)\in\mathbb{N}^m} f(n_1, \ldots, n_m) x_1^{n_1} \ldots x_m^{n_m},$$

en donde a $f(n_1, \ldots, n_m)$ es llamado el coeficiente de $x_1^{n_1} \ldots x_m^{n_m}$.

Ejemplo 1.2.3. *Si $f(n,k) = \binom{n}{k}$, entonces la función generadora multivariable de $f(n,k)$ es*

$$\sum_{k,n\geq 0} f(n,k) x^k y^n = \frac{1}{1 - y(1+x)}.$$

Capítulo 2

Raíces k-ésimas de una permutación

El contenido de este capítulo constituye el marco teórico del presente trabajo de investigación referente a raíces de permutaciones en S_n. En la primer sección se exponen resultados que permiten determinar las existencia de raíces k-ésimas de una permutación y en el caso afirmativo, la construcción de algunas de dichas raíces. La segunda sección de este capítulo expone una serie de resultados relacionados con el conteo de las raíces k-ésimas de una permutación. En particular se presenta una demostración de la fórmula exacta para calcular el número de raíces k-ésimas de una permutación (teorema 1 en [15]) usando funciones generadoras. Dicha demostración fue bosquejada en [15] y aquí se presenta la demostración completa.

2.1 Raíces en el grupo simétrico

Está sección está basada en el artículo de Annin et al. [3] y en ella se expone una caracterización de las permutaciones que tienen raíz k-ésima en S_n. Además, para permutaciones del tipo $(\ell)^c$ que tengan raíz k-ésima se describe un algoritmo para obtener algunas de dichas raíces.

Observación 2.1. *Sea σ una permutación tal que tiene raíz k-ésima. Si $\sigma_1 \dots \sigma_t$ es la factorización completa por longitudes de σ, entonces cualquier raíz k-ésima τ de σ se puede expresar como el producto $\tau_1 \dots \tau_t$, en donde $\tau_i^k = \sigma_i$, para cada i, y las permutaciones $\tau_1, \dots, \tau_t$ son disjuntas por parejas.*

Demostración: Sea ℓ_i la longitud de los ciclos en el producto σ_i. Por hipotesis $\sigma = \tau^k$. Sea $\alpha_1 \dots \alpha_s$ la factorización completa de τ. Notemos que $\tau^k = \alpha_1^k \dots \alpha_s^k$. Por el lema 1.19 la factorización completa de α_i^k es un producto de ciclos disjuntos de longitud $\dfrac{|\alpha_i|}{\text{mcd}(|\alpha_i|, k)}$. Dado que σ_i es igual a un producto de puros ciclos de longitud ℓ_i, entonces podemos elegir τ_i como el producto de todos los α_i tales que α_i^k sea igual un producto

de ciclos de longitud ℓ_i. Con lo anterior, $\tau_i^k = \sigma_i$ y podemos escribir $\tau = \tau_1 \dots \tau_t$ en donde por construcción las permutaciones $\tau_1, \dots, \tau_t$ son disjuntas por parejas. □

Por la observación anterior, para σ una permutación con raíz k-ésima tal que su factorización completa por longitudes es $\sigma_1 \dots \sigma_t$, podemos construir cualquier raíz k-ésima de σ obteniendo todas las raíces τ_i de σ_i; en donde las τ_i serán tales que si $\sigma_i = C_1 \dots C_s$, entonces los puntos que no están en los ciclos $C_1, \dots, C_s$ serán puntos fijos en τ_i. Por lo anterior, necesitamos una manera de construir raíces de permutaciones del tipo $(\ell)^c$ y en la proposición 2.4 se da un algoritmo para ello. Pero antes introducimos notación y definiciones necesarias, que se pueden encontrar en el libro de Schoup [30].

Sea p un primo y m un entero positivo. Denotaremos por $e(p, m)$ a la máxima potencia de p que divide a m. Usando esta notación la definición del máximo común divisor de los enteros positivos a y b queda como

$$\operatorname{mcd}(a, b) = \prod_{p \in \mathcal{P}} p^{\min\{e(p,a), e(p,b)\}},$$

en donde $\mathcal{P}$ es el conjunto de los primos. La siguiente observación sigue directamente de la definición de $e(p, m)$.

Observación 2.2. *Sean a y b enteros positivos. Entonces*

$$e(p, \operatorname{mcd}(a, b)) = \min\{e(p, a), e(p, b)\},$$

y

$$e(p, ab) = e(p, a) + e(p, b).$$

Definición 2.3. *Sean l y k enteros positivos. El* **paréntesis** *de la pareja (l, k) esta dado por*

$$((l, k)) = \prod_{p_j | l} p_j^{e(p_j, k)},$$

donde los p_j son primos .

Proposición 2.4 (Algoritmo para construir una raíz k-ésima de una permutación del tipo $(\ell)^c$). *Sean ℓ, k enteros positivos y c un múltiplo de $s := ((\ell, k))$. Si σ es una permutación del tipo $(\ell)^c$, entonces con el siguiente algoritmo se obtiene una raíz k-ésima τ de σ.*

Paso 1 *Tomar una partición $\mathcal{A} = \{A_1, \dots, A_h\}$ del conjunto de todos los ℓ-ciclos de σ, en donde cada parte de $\mathcal{A}$ tenga tamaño s. Nótese que $h = \frac{c}{s}$.*

Paso 2 *Tomar una parte $A_j := \{\alpha_1, \dots, \alpha_s\}$ en $\mathcal{A}$, para $j \in \{1, \dots, h\}$.*

Paso 3 *Considere el ℓ-ciclo $\beta_i = (b_{i1} b_{i2} \dots b_{i\ell})$ tal que $\beta_i^{\frac{k}{s}} = \alpha_i$, para cada ciclo α_i en A_j.*

Paso 4 Construir el ciclo

$$\tau_{A_j} = (b_{11}b_{21}\dots b_{s1}b_{12}b_{22}\dots b_{s2}\dots b_{1\ell}b_{2\ell}\dots b_{s\ell}).$$

Paso 5 Repetir los pasos 2 *al* 4 *para cada parte de* $\mathcal{A}$ *y así obtener* $\tau_{A_1},\dots,\tau_{A_h}$. *Construir* $\tau = \tau_{A_1}\tau_{A_2}\dots\tau_{A_h}$.

Demostración: El Paso 1 se puede hacer porque $c = hs$, para algún $h \in \mathbb{N}$. Para el Paso 2 fijamos una parte $A_j := \{\alpha_1,\dots,\alpha_s\}$ de $\mathcal{A}$. En el Paso 3, podemos tomar a β_i como la raíz $\frac{k}{s}$-ésima de cada α_i de A_j que, por el corolario 1.20, sabemos que existe y es única dado que $\mathrm{mcd}(\ell, \frac{k}{s}) = 1$. Aplicando el lema 1.19 al ciclo β_i, se tiene que este ciclo es de longitud ℓ y podemos escribirlo como $\beta_i = (b_{i1}b_{i2}\dots b_{i\ell})$, para cada $i \in \{1,\dots,s\}$. Para el Paso 4, como los $\alpha_1,\dots,\alpha_s$ son ciclos disjuntos entonces los $\beta_1,\dots,\beta_s$ son también ciclos disjuntos y por eso se tiene que

$$\tau_{A_j} = (b_{11}b_{21}\dots b_{s1}b_{12}b_{22}\dots b_{s2}b_{13}, b_{23}\dots b_{s3}\dots\dots b_{1\ell}b_{2\ell}\dots b_{s\ell}),$$

es un ciclo de longitud ℓs. Notemos que $(\tau_{A_j})^s = \beta_1\dots\beta_s$. Entonces

$$\tau_{A_j}^k = ((\tau_{A_j})^s)^{\frac{k}{s}} = (\beta_1\dots\beta_s)^{\frac{k}{s}} = (\beta_1)^{\frac{k}{s}}\dots(\beta_s)^{\frac{k}{s}} = \alpha_1\dots\alpha_s,$$

y así hemos construído una raíz k-ésima τ_{A_j} del producto $\alpha_1\dots\alpha_s$. Repitiendo los Pasos $2-4$ para cada parte A_j de $\mathcal{A}$ se construye τ como el producto $\tau_{A_1}\dots\tau_{A_h}$, en donde los τ_{A_i}'s son ciclos disjuntos entre si por construcción. Por lo que

$$\tau^k = \tau_{A_1}^k\dots\tau_{A_h}^k = \sigma.$$

obteniendo de esta manera una ráiz k-ésima de σ. □

La raíz construida en el algoritmo anterior es del tipo $(s\ell)^h$, con $h = c/s$ y $s = ((\ell,k))$.

El siguiente teorema proporciona una caracterización de las permutaciones que tienen raíz k-ésima. En el libro de Wilf [35] se menciona que fue demostrado primero por A. Knofmacher y R. Warlimont. La demostración que aqui se presente es una combinación de las dadas en [3] y [35].

Teorema 2.5. *Sea* $\sigma \in S_n$ *y* $k = p_1^{i_1}p_2^{i_2}\dots p_t^{i_t}$ *con* $p_1, p_2, \dots, p_t$ *primos distintos e* $i_j > 0$, *para cada* j. *Entonces* σ *posee una raiz* k*-ésima en* S_n *si y solo si para toda* ℓ *en* $\mathbb{N}$, *el número de ciclos de longitud* ℓ *en la descomposición de* σ *como un producto de ciclos disjuntos es un múltiplo de* $((\ell,k))$.

Demostración: ($\Longleftarrow$) Considérese la factorización completa por longitudes de σ, esto es, $\sigma = \sigma_1\dots\sigma_x$, donde cada σ_i es una permutación del tipo $(\ell_i)^{c_i}$. Si consideramos por separado cada σ_i notemos que estamos en las hipótesis de la proposición 2.4, ya que c_i es un múltiplo de $((\ell_i,k))$. Aplicando el algoritmo de dicha proposición se obtiene una raíz k-ésima τ_i para cada σ_i. Entonces, si tomamos $\tau = \tau_1\dots\tau_x$ se tiene

$$\tau^k = \tau_1^k \dots \tau_x^k = \sigma_1 \dots \sigma_x = \sigma,$$

es decir, τ es una raíz k-ésima de σ.

($\Longrightarrow$) Suponga que σ posee un raíz k-ésima, τ, en S_n. Sea $\tau_1 \dots \tau_m$ la factorización completa de τ, en donde la longitud de τ_i es ℓ_i, para todo i. Entonces $\sigma = \tau^k = \tau_1^k \dots \tau_m^k$, y por el lema 1.19, τ_i^k es un producto de $\text{mcd}(\ell_i, k)$ ciclos disjuntos, cada uno de longitud $\frac{\ell_i}{\text{mcd}(\ell_i,k)}$. Por lo tanto, todos los ciclos de longitud ℓ en σ vienen de ciclos de longitud r en τ, en donde r cumple que $r/\text{mcd}(r,k) = \ell$. De lo anterior tenemos que $r = \ell \cdot \text{mcd}(r,k)$.

Afirmación. *r es un múltiplo de $\ell((\ell,k))$.*

Demostración: Basta demostrar que si p es un primo que divide a $\ell((\ell,k))$, entonces $e\left(p, \ell((\ell,k))\right) = e(p,r)$. Sea p un primo que divide a $\ell((\ell,k))$. Notemos que p divide a ℓ. Ahora usaremos la observación 2.2. Por un lado tenemos que

$$e\left(p, \ell((\ell,k)\right) = e(p,\ell) + e\left(p, ((\ell,k))\right) = e(p,\ell) + e(p,k).$$

Por otro lado, como p divide a ℓ tenemos que p divide a r y por lo tanto

$$e(p,r) = e(p,\ell) + e\left(p, \text{mcd}(r,k)\right) = e(p,\ell) + \text{mín}\{e(p,r), e(p,k)\} = e(p,\ell) + e(p,k),$$

en donde la última desigualdad se cumple porque $e(p,\ell) > 0$. □

De la afirmación se sigue que todos los ciclos de longitud ℓ de σ vienen de ciclos $\alpha_1, \dots, \alpha_h$ en τ cuyas longitudes son múltiplos de $\ell((\ell,k))$. Como cada α_i^k se descompone en una cantidad múltiplo de $((\ell,k))$ de ℓ-ciclos en σ (porque $((\ell,k))$ divide a k), tenemos que el número de ℓ-ciclos en σ es un múltiplo de $((\ell,k))$.

□

2.2 Número de raíces de una permutación

En esta sección presentamos resultados conocidos sobre el número de raíces de permutaciones. La siguiente proposición muestra que permutaciones conjugadas tienen el mismo número de raíces.

Proposición 2.6. *Si σ y π son dos permutaciones con el mismo tipo de ciclo, entonces el número de raíces de σ es igual al número de raíces de π.*

Demostración: Denotemos por $R_n^{(k)}(\pi)$ y $R_n^{(k)}(\sigma)$ el conjunto de las raíces k-ésimas de π y σ, respectivamente. Como σ y π tienen el mismo tipo de ciclo, del teorema 1.10 se sigue que estas permutaciones son conjugadas, es decir, existe $\theta \in S_n$ tal que $\sigma = \theta\pi\theta^{-1}$. Si $\alpha \in R_n^{(k)}(\pi)$, entonces $(\theta\alpha\theta^{-1})^k = \theta\alpha^k\theta^{-1} = \theta\pi\theta^{-1} = \sigma$. Por lo que podemos definir la función

$$f_\theta : R_n^{(k)}(\pi) \longrightarrow R_n^{(k)}(\sigma),$$

dada por $f_\theta(\alpha) = \theta\alpha\theta^{-1}$. Ahora, si $\beta \in R_n^{(k)}(\sigma)$, entonces $(\theta^{-1}\beta\theta)^k = \theta^{-1}\beta^k\theta = \theta^{-1}\sigma\theta = \pi$ y por ello se puede definir la función

$$g_\theta : R_n^{(k)}(\sigma) \longrightarrow R_n^{(k)}(\pi),$$

con $g_\theta(\beta) = \theta^{-1}\beta\theta$.

Notemos que g_θ es función inversa de f_θ, y por lo tanto f_θ es una función biyectiva entre $R_n^{(k)}(\pi)$ y $R_n^{(k)}(\sigma)$. □

Denotaremos por $r_n^{(k)}(\mathbf{c})$ (resp. $r_n^{(k)}(\sigma)$) al número de raíces k-ésimas en S_n de cualquier permutación de tipo de ciclo $\mathbf{c}$ (resp. de la permutación σ). Un problema de interés es determinar el valor de $r_n^{(m)}(\mathbf{c})$. Se tienen al menos tres fórmulas para calcular este número. La primera fue publicada en 1980 por Pavlov [21] y las otras dos fórmulas se presentan en las siguientes secciones.

2.2.1 Fórmula de Roichman

En esta sección presentamos una fórmula para obtener el número de raíces k-ésimas de una permutación debida a Roichman [25]. Primero algunas definiciones.

Definición 2.7. *Se dice que la serie de enteros positivos $(a_1, \ldots, a_k)$ es una **partición** de n si, $\sum_{i=1}^{k} a_i = n$ y además se cumple que $a_1 \geq a_2 \geq \cdots \geq a_k$.*

Definición 2.8. *Sea $\mu = (\mu_1, \ldots, \mu_t)$ una partición de n con t partes distintas. Escribimos*

$$\mu_{(0)} := 0$$

$$\mu_i := \sum_{j=1}^{i} \mu_i \qquad (1 \leq i \leq t)$$

y

$$S(\mu) := (\mu_{(1)}, \ldots, \mu_{(t)}).$$

*Una **permutación** $\pi \in S_n$ es μ-**unimodal** si para todo i, con $0 \leq i < t$, existe ℓ, con $0 \leq l \leq \mu_{i+1}$ tal que:*

$$\pi(\mu_{(i)} + 1) > \pi(\mu_{(i)} + 2) > \cdots > \pi(\mu_{(i)} + l) < \pi(\mu_{(i)} + l + 1) < \cdots < \pi(\mu_{(i+1)})$$

Denotaremos por U_μ al conjunto de permutaciones μ-unimodales en S_n.

Definición 2.9. *Para $n \geq 1$ y $k \geq 0$, escribimos*

$$I_n^k := \{\pi \in S_n : \pi^k = 1\},$$

esto es, I_n^k es el conjunto de raíces k-ésimas de la permutación identidad en S_n. La permutación identidad se denota por 1 o Id.

Definición 2.10. *Sea $\sigma = \sigma_1 \dots \sigma_n$ una permutación, y sea $i < n$ un entero positivo. Decimos que i es un* ***descenso*** *de σ si $\sigma_i > \sigma_{i+1}$.*

El siguiente teorema es de Roichman [25] y su demostración requiere de teoría de representaciones del grupo simétrico, que está fuera del alcance de esta tesis

Teorema 2.11. *Para todo $n \geq 1$, $k \geq 0$, μ una partición de n y $\pi \in S_n$ de tipo de ciclo μ, tenemos*

$$|\{\sigma \in S_n : \sigma^k = \pi\}| = \sum_{\sigma \in I_n^k \cap U_\mu} (-1)^{|Des(\sigma) \setminus S(\mu)|}$$

En el siguiente ejemplo se ilustra la aplicación del teorema anterior.

Ejemplo 2.12.

Para $n = 4$,

$$S_4 = \{1234, 1243, 1342, 1324, 1423, 1432, 2134, 2143, 2341, 2314, 2413, 2431, 3142, 3124, 3421, 3412, 3214, 3241, 4123, 4132, 4231, 4213, 4312, 4321\}.$$

Se tienen las particiones:

$$\begin{aligned} \mu^{(1)} &= (4) \\ \mu^{(2)} &= (3,1) \\ \mu^{(3)} &= (2,2) \\ \mu^{(4)} &= (2,1,1) \\ \mu^{(5)} &= (1,1,1,1) \end{aligned}$$

y los conjuntos de permutaciones $\mu^{(i)}$-unimodales, $i \in \{1,2,3,4,5\}$:

$$U_{\mu^{(1)}} = \{1234, 2134, 3124, 3214, 4123, 4213, 4312, 4321\},$$

$$U_{\mu^{(2)}} = \{1234, 1243, 1342, 2134, 2143, 2341, 3142, 3214, 3241, 4123, 4132, 4231, 4213, 4312, 4321\},$$

$$U_{\mu^{(3)}} = \{1234, 1243, 1342, 1324, 1423, 1432, 2134, 2143, 2341, 2314, 2413, 2431, 3142, 3124, 3421, 3412, 3214, 3241, 4123, 4132, 4231, 4213, 4312, 4321\},$$

$$U_{\mu^{(4)}} = \{1234, 1243, 1342, 1324, 1423, 1432, 2134, 2143, 2341, 2314, 2413, 2431, 3142, 3124, 3421, 3412, 3214, 3241, 4123, 4132, 4231, 4213, 4312, 4321\},$$

$$U_{\mu^{(5)}} = \{1234, 1243, 1342, 1324, 1423, 1432, 2134, 2143, 2341, 2314, 2413, 2431, 3142, 3124, 3421, 3412, 3214, 3241, 4123, 4132, 4231, 4213, 4312, 4321\}.$$

Sea $k = 2$. Entonces

$$I_4^2 = \{\pi \in S_n : \pi^2 = 1\} = \{Id, 2134, 1324, 1243, 4231, 3214, 1432, 2143, 3412, 4321\}.$$

Para $\pi = 2143$ una permutación con tipo de ciclo $\mu^{(3)}$ tenemos que

$$I_4^2 \cap U_{\mu^{(3)}} = \{1234, 1243, 1324, 1432, 2134, 2143, 3412, 3214, 4231, 4321\},$$

y los conjuntos de descensos para cada permutación de $I_4^2 \cap U_{\mu^{(3)}}$ son los siguientes

$$\begin{aligned}
Des(1234) &= \emptyset \\
Des(1243) &= \{3\} \\
Des(1324) &= \{2\} \\
Des(1432) &= \{2, 3\} \\
Des(2134) &= \{1\} \\
Des(2143) &= \{1, 3\} \\
Des(3412) &= \{2\} \\
Des(3214) &= \{1, 2\} \\
Des(4231) &= \{1, 3\} \\
Des(4321) &= \{1, 2, 3\}.
\end{aligned}$$

Como $S(\mu^{(3)}) = \{2, 4\}$, obtenemos

$$\begin{aligned}
|Des(1234) \setminus \{2,4\}| &= |\emptyset \setminus \{2,4\}| = 0 \\
|Des(1243) \setminus \{2,4\}| &= |\{3\} \setminus \{2,4\}| = 1 \\
|Des(1324) \setminus \{2,4\}| &= |\{2\} \setminus \{2,4\}| = 0 \\
|Des(1432) \setminus \{2,4\}| &= |\{2,3\} \setminus \{2,4\}| = 1 \\
|Des(2134) \setminus \{2,4\}| &= |\{1\} \setminus \{2,4\}| = 1 \\
|Des(2143) \setminus \{2,4\}| &= |\{1,3\} \setminus \{2,4\}| = 2 \\
|Des(3412) \setminus \{2,4\}| &= |\{2\} \setminus \{2,4\}| = 0 \\
|Des(3214) \setminus \{2,4\}| &= |\{1,2\} \setminus \{2,4\}| = 1 \\
|Des(4231) \setminus \{2,4\}| &= |\{1,3\} \setminus \{2,4\}| = 2 \\
|Des(4321) \setminus \{2,4\}| &= |\{1,2,3\} \setminus \{2,4\}| = 2
\end{aligned}$$

y así

$$|\{\sigma \in S_4 : \sigma^2 = \pi\}| = 3(-1)^2 + 4(-1)^1 + 3(-1)^0 = 2.$$

2.2.2 Formula de Leaños, et al.

Está sección está basada en el artículo publicado en 2012 por Leaños, et al. [15]. Primero se presentan algunos preliminares y después algunas proposiciones que serán de utilidad para obtener la fórmula sobre el número de raíces k-ésimas de una permutación, que es el resultado principal de dicho artículo. Para la demostración que se presenta en esta tesis se modificaron ligeramente algunas proposiciones que aparecen en el artículo [15], con la intención de obtener primero la función generadora exponencial multivariable del número de raíces k-ésimas de una permutación, y a partir de ella la fórmula deseada; contrario al orden en que se obtienen estos resultados en el artículo antes citado.

Sea $\sigma_1 \dots \sigma_m$ la factorización completa por longitudes de σ, esto es $\sigma_i = \prod_{j=1}^{c_j} C_i$, para cada i, en donde todos los ciclos C_i son de longitud ℓ_i. Definimos

$$X(\sigma_i) = \{x \in [n] : x \text{ esta en algún ciclo } C_i \text{ de } \sigma_i\}. \tag{2.1}$$

Por la definición de factorización completa por longitudes tenemos que $X(\sigma_i) \cap X(\sigma_j) = \emptyset$, para todo $i \neq j$. Para $f \in S_n$ y $X \subseteq [n]$ tal que $f(X) = X$, usaremos $f|_X$ para denotar la restricción de f al conjunto X. Por la observación 2.1, podemos encontrar todas las raíces de σ obteniendo todas las raíces τ_i' de $\sigma_i|_{X(\sigma_i))}$ en $S_{X(\sigma_i))}$, para cada i, y luego extender a τ_i' a una permutación τ_i en S_n haciendo puntos fijos a todos los elementos en $[n] - X(\sigma_i)$. Por lo anterior obtenemos el siguiente lema que será de utilidad.

Lema 2.13. *Sean k, m y n enteros positivos. Sea $\sigma \in S_n$ y $\sigma_1 \dots \sigma_m$ su factorización completa por longitudes. Entonces*

$$r_n^{(k)}(\sigma) = \prod_{i=1}^{m} r_{X_i}^{(k)}(\sigma_i),$$

en donde $r_{X_i}^{(k)}(\sigma_i)$ es el número de raíces k-ésimas de $\sigma_i|_{X(\sigma_i)}$ en $S_{X(\sigma_i)}$.

Por el lema anterior, para encontrar el número de raíces k-ésimas de una permutación necesitamos encontrar el número de raíces k-ésimas de cada parte de su factorización completa por longitudes, es decir, de permutaciones del tipo $(\ell)^c$. Sea σ una permutación del tipo $(\ell)^c$ tal que tiene raíz k-ésima, esto es c es múltiplo de $((\ell, k))$. Queremos encontrar todas las permutaciones τ tal que $\tau^k = \sigma$. Primero determinaremos las posibles longitudes de los ciclos en la descomposición completa de τ. Si r es longitud de algún ciclo en τ, por la demostración del teorema 2.5 se tiene que $r = \ell \cdot \text{mcd}(r, k)$. Haciendo $g := \text{mcd}(r, k)$, tenemos que $r = g\ell$. Esto es, se deben "agrupar" g ciclos en σ para obtener un ciclo de longitud r en τ (lo anterior se puede hacer siguiendo el algoritmo de la proposición 2.4). Ahora, por la definición de g tenemos que $g = \text{mcd}(g\ell, k)$ y $g \leq c$.

Vamos a definir los siguientes conjuntos con todos los valores posibles de g, en donde el segundo toma en cuenta la restricción de que $g \leq c$. Sean k y ℓ enteros positivos y c un entero no negativo. Sean

$$G_k(\ell) = \{g \ \in \mathbb{Z}^+ : \text{mcd}\,(g\ell, k) = g\}$$

y

$$G_k(\ell, c) = \{g \ \in \mathbb{Z}^+ : \ g \leq c; \ \text{mcd}\,(g\ell, k) = g\}.$$

Se puede verificar que los conjuntos que acabamos de definir son finitos. Ahora, definimos al **vector asociado** a $G_k(\ell, c) = \{g_1, \dots, g_m\}$, en donde $g_1 < \cdots < g_m$, como el vector $\mathbf{g} = (g_1, ..., g_m)$. La ecuación

$$\mathbf{g} \cdot \boldsymbol{\varepsilon} = g_1\varepsilon_1 + \cdots + g_m\varepsilon_m = c,$$

indica que τ tendrá ε_i ciclos de longitud $g_i\ell$, para cada i. Para cualquier conjunto $G_k(\ell, c)$ de cardinalidad $m \geq 1$ definimos el conjunto de vectores:

$$E_k(\ell, c) := \{\boldsymbol{\varepsilon} \ \in \mathbb{N}_0^m \ : \ \mathbf{g} \cdot \boldsymbol{\varepsilon} = c, \ \ \mathbf{g} \text{ es el vector asociado a } \ G_k(\ell, c)\}.$$

Este conjunto de vectores puede ser vacío si la ecuación $\mathbf{g} \cdot \boldsymbol{\varepsilon} = g_1\varepsilon_1 + \cdots + g_m\varepsilon_m = c$ no tiene soluciones enteras.

Las siguientes propiedades sobre los conjuntos $G_k(\ell)$ y $G_k(\ell, c)$ aparecen en el artículo de Leaños et al. [15] y se presentan sin demostración.

Recordemos que $e(p, m)$ denota a la máxima potencia de p que divide a m.

Proposición 2.14. *Sean g, ℓ y k enteros positivos. Entonces $g \in G_k(\ell)$ si y sólo si se cumplen las condiciones 1) y 2):*

1) Cualquier primo p divisor de g divide a k y satisface una de las siguientes condiciones

a) Si p divide a ℓ, entonces $e(p,g) = e(p,k)$,

b) Si p no divide a ℓ, entonces $e(p,g) \leq e(p,k)$,

2) Si p es un primo que no divide a g, entonces p no divide al $\operatorname{mcd}(\ell,k)$.

Proposición 2.15. *Sean k, ℓ y c enteros positivos. Entonces*

1) $((\ell,k))$ pertenece a $G_k(\ell)$.

2) Si $((\ell,k))$ divide a c, entonces $((\ell,k))$ pertenece a $G_k(\ell,c)$

Observación 2.16. *Notemos que si* $g = \operatorname{mcd}(g\ell,k)$ *entonces* $\operatorname{mcd}(\ell,k)$ *divide a g. Una consecuencia es que al menos $((\ell,k))$ es un elemento de $G_k(\ell)$.*

Proposición 2.17. *Si* $\operatorname{mcd}(\ell,k) = 1$, *entonces $G_k(\ell)$ es igual al conjunto de divisores positivos de k.*

Proposición 2.18. *Sean k, ℓ y c enteros positivos. Si $G_k(\ell) = \{g_1,\ldots,g_h\}$, entonces*

$$\operatorname{mcd}(g_1,\ldots,g_h) = ((\ell,k)).$$

Corolario 2.19. *Sean k, ℓ y c enteros positivos. Sea $G_k(\ell,c) = \{g_1,\ldots,g_h\}$. Entonces*

$$\operatorname{mcd}(g_1,\ldots,g_h) = ((\ell,k)).$$

Proposición 2.20. *Sean k, ℓ y c enteros positivos. Sea $G_k(\ell,c) = \{g_1,\ldots,g_h\}$. Entonces $((\ell,k))$ divide a c si y solo si la ecuación*

$$g_1x_1 + \cdots + g_hx_h = c,$$

tiene soluciones enteras no negativas.

La proposición anterior tiene como consecuencia lo siguiente:

Corolario 2.21. *Una permutación de tipo $(\ell)^c$ tiene raíz k-ésima si y solo si la ecuación*

$$g_1x_1 + \cdots + g_hx_h = c,$$

tiene soluciones enteras no negativas, en donde $G_k(\ell,c) = \{g_1,\ldots,g_h\}$.

La siguiente proposición caracteriza las raíces del tipo $(g\ell)^p$ cuando σ es del tipo $(\ell)^c$, para g, p y c enteros.

Proposición 2.22. *Sea σ una permutación del tipo $(\ell)^c$ y p un entero positivo. Entonces σ tiene una raíz k-ésima del tipo $(g\ell)^p$ si y solo si $g \in G_k(\ell)$ y $c = gp$.*

Demostración: Por la proposición 2.18 se tiene que si $g \in G_k(\ell)$, entonces $((\ell, k))$ divide a g, por tanto si $c = gp$, entonces $((\ell, k))$ también divide a c, y por el teorema 2.5 se sigue que σ tiene raíz k-ésima. Ahora, como $g = \text{mcd}(g\ell, k)$ (porque $g \in G_k(\ell)$) tenemos que g divide a k y al ser c múltiplo de g, podemos aplicar el algoritmo de la proposición 2.4, usando g en lugar de s (la demostración de que dicho algoritmo funciona es análoga a la de la proposición 2.4), para obtener una raíz k-ésima del tipo $(g\ell)^p$ para σ.

Recíprocamente, si σ tiene una raíz k-ésima τ del tipo $(g\ell)^p$, entonces para cada ciclo C en τ, C^k es un producto de $\text{mcd}(g\ell, k)$ ciclos de longitud $\ell = g\ell/\text{mcd}(g\ell, k)$ en σ, esto es $g = \text{mcd}(g\ell, k)$. Por lo que $g \in G_k(\ell)$. Además, como obtenemos $\text{mcd}(g\ell, k) = g$ ciclos de longitud ℓ en σ por cada $g\ell$-ciclo en τ, tenemos que $c = gp$. □

Sea c un entero no negativo y p un entero positivo. Para σ cualquier permutación del tipo $(\ell)^c$ y k, g enteros positivos fijos, denotamos por $f_{k,\ell,g,p}(c)$ al número de raíces k-ésimas de σ que son del tipo $(g\ell)^p$.

Ejemplo 2.23. Para $k = 2$ y $\sigma = (123)(456)$, tenemos que $\ell = 3$. Como $c = 2$, $(g, p) \in \{(2, 1), (1, 2)\}$. Para $g = 2$, $p = 1$, las raíces cuadradas de la forma $(g\ell)^p$ son

$$\begin{aligned}
\tau_1 &= (142536) \\
\tau_2 &= (243516) \\
\tau_3 &= (341526) \\
\tau_4 &= (415263) \\
\tau_5 &= (516243) \\
\tau_6 &= (614253),
\end{aligned}$$

esto es $f_{2,3,2,1}(2) = 6$. Para $g = 1, p = 2$ tenemos que $\tau_7 = (132)(465)$ es una raíz cuadrada de tipo $(3)^2$ de σ. De hecho $f_{2,3,1,2}(2) = 1$. Se puede verificar que las permutaciones $\tau_1, \ldots, \tau_7$ son todas las raíces cuadradas de σ.

Ahora se presenta un resultado, que es una generalización de la proposición 7 en [15].

Proposición 2.24. *Sean ℓ, k, g, p enteros positivos fijos. Sea c un entero no negativo y σ cualquier permutación del tipo $(\ell)^c$. Si $g \in G_k(\ell)$ y $c = gp$, entonces*

$$f_{k,\ell,g,p}(c) = \frac{(gp)!\ell^{p(g-1)}}{g^p p!},$$

y $f_{k,\ell,g,p}(c) = 0$ en cualquier otro caso.

Demostración: Si $g \notin G_m(\ell)$ o $c \neq gp$, por la proposición 2.22 tenemos que $f_{k,\ell,g,p}(c) = 0$. Ahora, si $g \in G_m(\ell)$, por la proposición 2.18 tenemos que $((k,\ell))$ divide a g y por el teorema 2.5 sigue que σ tiene raíz k-ésima. Sea τ cualquier raíz k-ésima de σ. De los gp ciclos en σ necesitamos construir p ciclos de longitud $g\ell$ para τ. Esto lo haremos tomando cualquier partición no ordenada $\mathcal{A}$, con exactamente p partes, del gp-conjunto de ℓ-ciclos de σ; y con cada una de estas partes formaremos un ciclo de longitud $g\ell$ para τ. El número de dichas particiones es

$$\frac{(gp)!}{(g!)^p p!}.$$

Si $\{C_1, \ldots, C_g\}$ es una parte de $\mathcal{A}$, con $\mathcal{A}$ cualquiera de las particiones mencionadas arriba, necesitamos organizar los elementos de los ciclos $C_1, \ldots, C_g$ en un ciclo D que cumpla que $D^k = C_1 \ldots C_g$. Para esto aplicamos el algoritmo de la proposición 2.4, usando g en lugar de s (como se indico en la demostración de la proposición 2.22), a todos los posibles ordenamientos circulares de los ciclos $C_1, \ldots C_g$ y a todos los posibles ordenamientos circulares de los elementos de cada ciclo. Con lo anterior obtenemos todos los posibles ciclos D de τ correspondientes a la parte $\{C_1, \ldots, C_g\}$, que serán $(g-1)!\ell^{g-1}$. Como tenemos p partes en $\mathcal{A}$, obtenemos $((g-1)!\ell^{g-1})^p$ conjuntos $\{D_1, \ldots, D_p\}$ diferentes de ciclos D_i, con los cuales podemos construir las diferentes raíces k-ésimas $D_1 \cdots D_p$ de σ. Por lo tanto, si repetimos el procedimiento anterior para cada una de las particiones que estamos considerando, obtenemos que para σ el número de raíces k-ésimas del tipo $(g\ell)^p$ es

$$\frac{(gp)!}{(g!)^p p!}((g-1)!\ell^{g-1})^p = \frac{(gp)!\ell^{p(g-1)}}{g^p p!}.$$

□

La siguiente proposición nos da una función generadora exponencial para la fórmula de la proposición anterior para $g \in G_m(\ell)$ fijo. Primero notemos que por la proposición anterior tenemos que $f_{k,\ell,g,p}(c) \neq 0$ si y solo si $g \in G_k(\ell)$ y $c = gp$, por lo que tenemos que p depende de c para que σ tenga raíces del tipo $(g\ell)^p$.

Proposición 2.25. *Sean ℓ y k enteros positivos fijos. Sea $g \in G_m(\ell)$ fijo. Entonces*

$$\sum_{c \geq 0} f_{k,\ell,g,p}(c)\frac{t_\ell^c}{c!} = \exp\left(\frac{\ell^{(g-1)}}{g} t_\ell^g\right).$$

Demostración: De la proposición 2.24 se tiene que $f_{k,\ell,g,p}(c) \neq 0$ si y solo si $c = gp$ por lo que

$$\begin{aligned}\sum_{c\geq 0} f_{k,\ell,g,p}(c)\frac{t_\ell^c}{c!} &= \sum_{p\geq 0} f_{k,\ell,g,p}(gp)\frac{t_\ell^{gp}}{(gp)!}\\ &= \sum_{p\geq 0}\frac{(gp)!\ell^{p(g-1)}}{g^p p!}\frac{t_\ell^{gp}}{(gp)!}\\ &= \sum_{p\geq 0}\frac{\ell^{p(g-1)}}{g^p}\frac{t_\ell^{gp}}{(p)!}\\ &= \exp\left(\frac{\ell^{(g-1)}}{g}t_\ell^g\right).\end{aligned}$$

□

Con lo anterior podemos obtener una función generadora exponencial mutivariable (en las variables $t_1, t_2, ...$) para el número de raíces k-ésimas de una permutación de tipo $\mathbf{c} = (c_1, \ldots, c_n)$.

Teorema 2.26. *Sean k, n enteros positivos y $c_1, \ldots, c_n$ enteros no negativos. Para $n = c_1 + 2c_2 + \cdots + nc_n$, el coeficiente de $\frac{t_1^{c_1}\ldots t_n^{c_n}}{c_1!\ldots c_n!}$ en la expansión de*

$$\exp\left(\sum_{\ell\geq 1}\sum_{g\in G_m(\ell)}\frac{\ell^{g-1}}{g}t_\ell^g\right), \tag{2.2}$$

es el número de raíces k-ésimas de una n-permutación del tipo $\boldsymbol{c} = (c_1, \ldots, c_n)$.

Demostración: Sea $F(t_\ell)$ la función generadora del número de raíces k-ésimas de una permutación del tipo $(\ell)^c$. Por el lema 2.13 tenemos que la función generadora exponencial en las variables $t_1, t_2, ...$ para el número de raíces de permutaciones esta dada por

$$\prod_{\ell\geq 1} F(t_\ell).$$

Vamos a encontrar a $F(t_\ell)$ para una longitud fija ℓ, esto es para permutaciones σ del tipo $(\ell)^c$, con $c \geq 1$. Sea $G_k(\ell) = \{g_1, \ldots, g_m\}$. Por el corolario 2.21 tenemos que σ tiene raíz k-ésima τ si y solo si

$$g_1x_1 + \cdots + g_mx_m = c_\ell$$

tiene soluciones enteras no negativas, en donde una solución $(p_1, \ldots, p_m)$ de la ecuación anterior indica que τ es del tipo $(g_1\ell)^{p_1} \ldots (g_m\ell)^{p_m}$. Vamos a construir todas las raíces de σ con el siguiente procedimiento. Sea $\mathcal{A}$ el conjunto de todas las particiones débiles del conjunto de todos los ciclos en σ. Tomar $\{A_1, \ldots, A_m\} \in \mathcal{A}$ y para cada parte $A_i = \{\alpha_1, \ldots, \alpha_c\}$ construir raíz k-ésima del tipo $(g_i\ell)^{p_i}$ en S_X para $\sigma|_X$, en donde

$X = X(\alpha_1) \cup \cdots \cup X(\alpha_c)$ (el conjunto $X(\beta)$ se define en la ecuación 2.1). El número de tales raíces sera $f_{k,\ell,g_i,p_i}(c)$. Por la proposición 2.24 tenemos que el número de raíces de σ es igual a

$$\sum_{\{A_1,\ldots,A_m\}\in\mathcal{A}} f_{k,\ell,g_1,p_1}(|A_1|)\cdots f_{k,\ell,g_m,p_m}(|A_m|)$$

Por lo que estamos en las condiciones del teorema 1.25. Por lo tanto

$$\begin{aligned} F(x_\ell) &= \prod_{i=1}^{|G_k(\ell)|} \exp\left(\frac{\ell^{g_i-1}}{g_i} t_\ell^{g_i}\right) \\ &= \prod_{g\in G_k(\ell)} \exp\left(\frac{\ell^{g-1}}{g} t_\ell^{g}\right). \end{aligned}$$

Así, la función generadora buscada es

$$\prod_{\ell\geq 1} F_{x_\ell} = \prod_{\ell\geq 1}\prod_{g\in G_k(\ell)} \exp\left(\frac{\ell^{g-1}}{g} t_\ell^{g}\right),$$

que es igual a

$$\exp\left(\sum_{\ell\geq 1}\sum_{g\in G_k(\ell)} \frac{\ell^{g-1}}{g} t_\ell^{g}\right).$$

□

El siguiente teorema en [15] muestra un fórmula exacta para el número de raíces k-ésimas de cualquier permutación.

Teorema 2.27. *Sea k un entero positivo, sea σ una permutación del tipo $\mathbf{c} = (c_1, \ldots, c_n)$. Sea $r_k^{(n)}(\mathbf{c})$ el número de raíces k-ésimas de σ, entonces*

$$r_n^{(k)}(\mathbf{c}) = \prod_{\substack{\ell=1\\ c_\ell\neq 0}}^{n} c_\ell! \left(\sum_{\varepsilon\ \in E_k(\ell,c_\ell)} \prod_{i=1}^{|G_k(\ell,c_\ell)|} \frac{\ell^{(g_i-1)\varepsilon_i}}{{g_i}^{\varepsilon_i}\varepsilon_i!}\right), \tag{2.3}$$

donde $\mathbf{g} = (g_1, ..., g_m)$ el vector asociado a $G_k(\ell, c_\ell)$.

Demostración: Buscaremos los coeficientes de nuestro interés en la expansión de la función generadora de la proposición anterior, esto es para n entero positivo y $c_1, \ldots, c_n$ enteros no negativos tales que $n = c_1 + 2c_2 + \cdots + nc_n$, queremos el coeficiente de $\frac{t_1^{c_1}\ldots t_n^{c_n}}{c_1!\ldots c_n!}$ en la expansión de

$$\exp\left(\sum_{\ell\geq 1}\sum_{g\in G_k(\ell)} \frac{\ell^{g-1}}{g} t_\ell^{g}\right). \tag{2.4}$$

Para cualquier ℓ, los únicos factores en (2.4) que contribuyen al exponente de t_ℓ son los factores en

$$\prod_{g\in G_k(\ell)} \exp\left(\frac{\ell^{g-1}}{g} t_\ell^g\right),$$

que es igual a

$$\prod_{g\in G_k(\ell)} \left(\sum_{j\geq 0} \frac{\ell^{(g-1)j}}{g^j} \frac{t_\ell^{gj}}{j!}\right). \tag{2.5}$$

Queremos el coeficiente de $t_\ell^{c_\ell}$ ($c_\ell \neq 0$) en la expansión de (2.5). Pero dicho coeficiente viene de los productos $t_\ell^{g_1 j_1} \dots t_\ell^{g_m j_m}$ en (2.5) tales que $c_\ell = g_1 j_1 + \cdots + g_m j_m$, donde $m = |G_k(\ell)|$, $\mathbf{g} = (g_1 \dots g_m)$ el vector asociado de $G_k(\ell)$ y $(j_1, \dots, j_m)$ es cualquier solución no negativa de la ecuación $g_1 x_1 + \cdots + g_m x_m = c_\ell$, con $x_i = j_i$.

Por lo anterior, el coeficiente para cualquier $t_\ell^{c_\ell}$ es

$$\sum_{g_1 j_1 + \cdots + g_m j_m = c_\ell} \prod_{i=1}^{m} \frac{\ell^{(g_i-1)j_i}}{g_i^{j_i}} \frac{1}{j_i!}.$$

Para encontrar el coeficiente de $t_\ell^{c_\ell}/c_\ell!$ multiplicamos la expresión previa por $c_\ell!$

El coeficiente de $\frac{t_1^{c_1} \dots t_n^{c_n}}{c_1! \dots c_n!}$ viene de la ecuación(2.4) cuando se corre a ℓ de 1 a n y este coeficiente es

$$\prod_{\substack{\ell=1 \\ c_\ell \neq 0}}^{n} c_\ell! \sum_{g_1 j_1 + \cdots + g_m j_m = c_\ell} \prod_{i=1}^{m} \frac{\ell^{(g-1)j}}{g^j} \frac{1}{j!}$$

La prueba concluye al cambiar $g_1 j_1 + \cdots + g_m j_m = c_\ell$ en el índice de la suma por $\boldsymbol{\varepsilon} \in E_k(\ell, c_\ell)$, donde $\boldsymbol{\varepsilon} = (j_1, \dots, j_m) \in E_k(\ell, c_\ell) = \{\boldsymbol{\varepsilon} \in \mathbb{N}_0^m : g_1 j_1 + \cdots + g_m j_m = c_\ell\}$. □

Los siguientes ejemplos ilustran la aplicación de la fórmula 2.3.

Ejemplo 2.28.

Para $n = 4$, $k = 2$ y la permutación $\sigma = (12)(34)$, se tienen los conjuntos:

$$G_2(2,2) = \{2\}$$

y

$$E_2(2,2) = \{(1)\}.$$

Entonces el número de raíces de σ es

$$r_4^{(2)}(\sigma) = 2!(1) = 2$$

Ejemplo 2.29.
Para $n = 7$, $k = 2$ y la permutación $\sigma = (12)(34)(5)(6)(7)$, se tienen los conjuntos:

$$\begin{aligned} G_2(1,3) &= \{1,2\}, \\ G_2(2,2) &= \{2\} \end{aligned}$$

y

$$\begin{aligned} E_2(1,3) &= \{(1,1)(3,0)\}, \\ E_2(2,2) &= \{(1)\}. \end{aligned}$$

Entonces el número de raíces de σ es

$$r_7^{(2)}(\sigma) = 3![(1)(\frac{1}{2}) + (\frac{1}{6})(1)] \cdot 2!(1) = 8$$

2.2.3 Raíces cuadradas en S_n

La fórmula 2.3 puede parecer complicada de aplicar. En esta sección veremos el caso cuando $k = 2$, lo que será de utilidad en el capítulo 3.

La siguiente observación, consecuencia del lema 1.19, se usará en algunas demostraciones.

Observación 2.30. *Para el caso $k = 2$ se tiene:*

1. *El cuadrado de un ciclo de longitud $2j + 1$ es un ciclo de longitud $2j + 1$.*

2. *El cuadrado de un ciclo de longitud $2j$ es un producto de dos ciclos de longitud j, es decir, si τ es una raíz cuadrada de σ (si alguna), un ciclo de longitud par $2j$ en σ solo puede ser obtenido al elevar al cuadrado un ciclo de longitud $4j$ en τ.*

La fórmula para raíces cuadradas de cualquier permutación queda como sigue.

Proposición 2.31. *Sea σ cualquier permutación del tipo $\boldsymbol{c} = (c_1, \ldots, c_n)$, entonces $r_2^{(n)}(\boldsymbol{c}) = \prod_{\ell=1}^{n} r_2(\ell, c_\ell)$, donde*

$$r_2(\ell, c) = \begin{cases} \sum_{i=0}^{\lfloor c/2 \rfloor} \frac{c!}{(c-2i)!i!}(\ell/2)^i & \text{si } \ell \text{ es impar} \\ \frac{c!}{(c/2)!}(\ell/2)^{c/2} & \text{si } \ell \text{ y } c \text{ son pares} \\ 0 & \text{si } \ell \text{ es par y } c \text{ es impar} \end{cases}$$

Demostración: Cuando ℓ es un entero impar y $k = 2$ sigue que $G_2(\ell) = G_2(\ell, c) = \{1, 2\}$, $\mathbf{g} = (1, 2)$ y $E_2(\ell, c) = \{(x, y) \in \mathbb{N}_0^2 : x + 2y = c\}$. Entonces del teorema 2.27 se sigue que

$$r_n^{(k)}(\ell, c) = c! \sum_{i=0}^{\lfloor c/2 \rfloor} \frac{\ell^i}{2^i i!(c-2i)!}.$$

Si ℓ es par, entonces las raíces de una permutación de tipo $(\ell)^{c_\ell}$ son del tipo $(2\ell)^{c_\ell/2}$ (por la observación 2.30 (2)). Si $c = 2p$, para algún $p \in \mathbb{N}$ entonces $\{2\} = G_2(\ell)$ y por la proposición 2.24 se tiene que

$$\frac{(2p)!}{2^p p!}\ell^{p(2-1)} = \frac{c!}{2^{c/2}(c/2)!}(\ell)^{c/2} = \frac{c!}{(c/2)!}(\ell/2)^{c/2}.$$

Finalmente, sabemos que para ℓ par, una permutación del tipo $(\ell)^{c_\ell}$ tiene una raíz cuadrada si y sólo si c_ℓ es par por lo que se obtiene el resultado deseado cuando k es par y c es impar.

□

La fórmula anterior aparece en los artículos [2, 19] (relacionados a problemas sobre modelos de Gelfand en teoría de representaciones del grupo simétrico) en donde los autores la demuestran de manera independiente al artículo [15]. La siguiente proposición muestra la función generadora exponencial multivariable para raíces cuadradas.

Proposición 2.32. *Sean n un entero positivo y $c_1, \ldots, c_n$ enteros no negativos. Para $n = c_1 + 2c_2 + \cdots + nc_n$, el coeficiente de $\frac{t_1^{c_1} \ldots t_n^{c_n}}{c_1! \ldots c_n!}$ en la expansión de*

$$\exp\left(\sum_{j \geq 1}\left(t_{2j-1} + \frac{2j-1}{2}t_{2j-1}^2 + jt_{2j}^2\right)\right)$$

es el número de raíces cuadradas de una n-permutación de tipo de ciclo $\mathbf{c} = (c_1, \ldots, c_n)$.

Demostración: Este resultado se sigue del teorema 2.26, reescribiendo la fórmula 2.2 para las raíces cuadradas. Para el caso $k = 2$ se tiene que la ecuación $\operatorname{mcd}(g\ell, k) = g$ sólo se satisface para $g = 1$ o $g = 2$ según sea la paridad de ℓ.

- Si $\ell = 2j - 1$ para algún $j \geq 1$, entonces $G_2(2j-1) = \{1, 2\}$ y

$$\sum_{g \in G_m(\ell)} \frac{\ell^{g-1}}{g} t_\ell^g = t_{2j-1} + \frac{2j-1}{2}t_{2j-1}^2.$$

- Si $\ell = 2j$ para algún $j \geq 1$, entonces $G_2(2j) = \{2\}$ y

$$\sum_{g \in G_m(\ell)} \frac{\ell^{g-1}}{g} t_\ell^g = jt_{2j}^2.$$

Por lo anterior

$$\sum_{\ell\geq 1}\sum_{g\in G_m(\ell)}\frac{\ell^{g-1}}{g}t_\ell^g=\sum_{j\geq 1}\left(t_{2j-1}+\frac{2j-1}{2}t_{2j-1}^2+jt_{2j}^2\right).$$

Por último sustituyendo lo anterior en la fórmula 2.2, se tiene que

$$\exp\left(\sum_{j\geq 1}\left(t_{2j-1}+\frac{2j-1}{2}t_{2j-1}^2+jt_{2j}^2\right)\right).$$

□

A continuación presentamos algunos corolarios en donde se exhiben las funciones generadoras exponenciales para algunos casos.

Sea $r_2(\ell,c)$ el número de raíces cuadradas de cualquier permutación del tipo $(\ell)^c$. De la proposiciiones 2.31 y 2.32 se siguen los siguientes corolarios:

Corolario 2.33. *Si ℓ es par entonces tenemos*

$$r_2(\ell,c)=\begin{cases}\frac{c!}{(c/2)!}(\ell/2)^{c/2} & c \text{ par,}\\ 0 & c \text{ impar,}\end{cases}$$

y la función generadora exponencial es

$$\sum_{k\geq 0}r_2(\ell,c)\frac{x^c}{c!}=\exp\left(\frac{\ell}{2}x^2\right).$$

Corolario 2.34. *Si ℓ es impar se tiene que*

$$r_2(\ell,c)=\sum_{i=0}^{\lfloor c/2\rfloor}\frac{c!}{(c-2i)!i!}(\ell/2)^i$$

y la función generadora exponencial es

$$\sum_{c\geq 0}r_2(\ell,c)\frac{x^c}{c!}=\exp\left(x+\frac{\ell}{2}x^2\right).$$

Capítulo 3

Raíces k-ésimas en el grupo alternante

En este capítulo se presentan algunos resultados conocidos y otros originales respecto a raíces de permutaciones en el grupo alternante. La primer sección se enfoca en las caraterizaciones conocidas sobre raíces pares de una permutación. En la segunda sección se demuestran resultados originales sobre el número de raíces cuadradas pares de permutaciones que pertenecen al grupo alternante. En la sección 3.2.1 se presentan algunas fórmulas exactas y en la sección 3.2.2 funciones generadoras asociadas a algunas de estas fórmulas.

3.1 Caracterización de las raíces k-ésimas en A_n

Esta sección esta basada en el artículo de Annin et al., [3]. Se dan algunas demostraciones de resultados que aparecen como comentarios en dicho artículo y de algunos de sus teoremas principales. La siguiente proposición considera el caso k impar.

Teorema 3.1. *Sea $\sigma \in A_n$ y sea $k \geq 3$ un entero impar. Entonces σ tiene una raíz k-ésima en A_n si y solo si σ tiene una raíz k-ésima en S_n*

Demostración: ($\Longrightarrow$) Es evidente. ($\Longleftarrow$) Suponga que $\sigma = \tau^k$ para alguna $\tau \in S_n$. Si $\tau \in A_n$, terminamos. Si $\tau \notin A_n$, dado que k es impar se tiene que $\tau^k \notin A_n$ lo que contradice el hecho de que $\sigma \in A_n$. Por lo tanto, $\tau \in A_n$.

□

La proposición 3.3 es mencionada en el artículo de Annin et al. [3] donde la plantean como ejercicio para el lector, en este trabajo se da una demostración. Antes, consideremos la siguiente notación.

Observación 3.2. *Sea $\sigma \in S_n$ y $k = p_1^{i_1} p_2^{i_2} \dots p_c^{i_c}$ (con $i_j > 0$ para cada j) entero positivo. Si σ tiene una raíz k-ésima en S_n , entonces por el teorema 2.5, para cada*

$\ell \in \mathbb{N}$ existe un entero $m_\ell \neq 0$ tal que el número de ciclos de longitud ℓ en la expresión como ciclos disjuntos de σ es $m_\ell \cdot s_\ell$, donde $s_\ell = ((\ell, k))$.

Proposición 3.3. *Si $\sigma \in A_n$ tiene una raíz k-ésima en S_n y tiene (al menos) dos puntos fijos en su factorización completa, esto es $m_1 \geq 2$, entonces σ también tiene una raíz k-ésima en A_n.*

Demostración: Sea $\sigma = \tau^k \in A_n$, si $\tau \in A_n$ hemos terminado. Si $\tau \notin A_n$, buscaremos una permutación $\beta \in A_n$ tal que $\beta^k = \sigma$. Dado que σ tiene dos puntos fijos, digamos a_1 y b_1, entonces $\sigma = (a_1)(b_1)\sigma'$. Sea $\tau_1 \dots \tau_q$ la factorización completa de τ. Supongamos que a_1 y b_1 pertenecen a los ciclos $\tau_i = (a_1, a_2, ..., a_l)$ y $\tau_j = (b_1, b_2, ..., b_m)$, respectivamente, en donde puede pasar que $\tau_i = \tau_j$. Por el lema 1.19 los puntos $a_1, \dots, a_\ell, b_1, \dots, b_m$ son puntos fijos en τ^k. En consecuecia se tiene que $\tau^k = (a_1) \dots (a_\ell)(b_1) \dots (b_m)\tau'^k = \sigma$, en donde τ'^k consiste en el resto de los ciclos en la descomposición en ciclos disjuntos de σ. Lo que implica que τ'^k tiene que ser una permutación par.

Tenemos dos casos.

Caso 1. $\tau_i \neq \tau_j$. Es decir

$$\tau = (a_1, \dots, a_\ell)(b_1, \dots, b_m)\tau' = \tau_i \tau_j \tau'.$$

a) Si ℓ, m son ambos impares o ambos pares, entonces $\tau_i \tau_j \in A_n$ y por tanto τ' debe ser impar. Como $\sigma = \tau'^k$ entonces τ'^k debe ser par. Como τ' es impar entonces k es par. Por lo anterior basta tomar $\beta = (a_1, b_1)\tau'$ porque $\beta^k = (a_1, a_s)^k \tau'^k = \tau'^k = \sigma$.

b) Si ℓ, m son uno par y el otro impar, entonces $\tau_i \tau_j$ es impar y eso implica que τ' es par. Por tanto, basta considerar $\beta = \tau'$ pues $\sigma = \tau^k = (a_1, \dots, a_\ell)^k (b_1, \dots, b_m)^k \tau'^k = \tau'^k$.

Caso 2. $\tau_i = \tau_j$. Para este caso supongamos que $b_1 = a_s$ con $2 \leq s \leq l$. Esto es

$$\tau = (a_1, \dots, a_s, \dots)\tau'.$$

a) Si ℓ es impar entonces τ_i es par y por lo tanto τ' debe ser impar. Como en el caso (1-a), k es par y basta tomar $\beta = (a_1, a_s)\tau'$, porque $\beta^k = (a_1, a_s)^k \tau'^k = \tau'^k = \sigma$.

b) Si ℓ es par entonces τ_i es impar y entonces τ' debe ser par, como en el caso (1-b) y por el mismo argumento basta tomar $\beta = \tau'$.

□

Cabe mencionar que la proposición anterior es un corolario del teorema 3.4, que se presenta a continuación y que caracteriza a las raíces k-ésimas pares de permutaciones pares. La demostración que a continuación se presenta es la que aparece en Annin, et al. [3]

Teorema 3.4 (Annin, Jansen, Smith, 2009)**.** *Sea $\sigma \in A_n$ y $k = 2^{i_1}p_2^{i_2}\dots p_c^{i_c}$, con $i_j > 0$ para cada j, en donde $2, p_2, \dots, p_c$ son primos distintos. Entonces σ posee una raíz k-ésima en A_n si y solo si σ posee una raíz k-ésima en S_n, y al menos una de las siguientes dos condiciones se satisface:*

(i) para algún valor impar de ℓ, $m_\ell \geq 2$;

(ii) la suma $m_2 + m_4 + m_6 + \dots$ es par, en donde los m_i son los dados en la observación 3.2.

Demostración: ($\Longleftarrow$)

Por hipótesis $\sigma = \tau^k$ para algún $\tau \in S_n$. Asumimos que se cumple (i). Expresamos a la descomposición en ciclos disjuntos de σ como $\sigma = \sigma_1\sigma_2\sigma'$, donde σ_1 y σ_2 son cada una un producto de s_ℓ ciclos disjuntos de longitud ℓ, con ℓ un impar. Consideremos para cada σ_i la construcción de una raíz k-ésima, τ_i, como en la demostración del teorema 2.5 (usando el algoritmo de la proposición 2.4), con $i \in \{1, 2\}$, de manera que cada τ_i tiene longitud ℓs_ℓ. Dado que ℓ es impar, se tiene que s_ℓ, que es igual a $((\ell, k))$, también es impar, y por tanto $\tau_1\tau_2$ pertenecen a A_n. Notemos que, como $\sigma' = \sigma_1^{-1}\sigma_2^{-1}\sigma$, entonces

$$\sigma' = (\tau_1^{-1})^k(\tau_2^{-1})^k\tau^k = (\tau_1^{-1}\tau_2^{-1}\tau)^k.$$

Definimos $\tau' := \tau_1^{-1}\tau_2^{-1}\tau$ y tenemos $\sigma' = \tau'^k$, es decir, σ' tiene una raíz k-ésima en S_n. Si $\tau' \in A_n$, entonces $\tau_1\tau_2\tau' \in A_n$ y como $(\tau_1\tau_2\tau')^k = \sigma_1\sigma_2\sigma' = \sigma$, queda demostrado que σ tiene una raíz en A_n. Ahora consideremos el caso $\tau' \neq A_n$. Para este caso podemos construir un ciclo τ_{12} de longitud $2\ell s_\ell$ tal que $\tau_{12}^k = \sigma_1\sigma_2$ (usando el algoritmo de la proposición 2.4). Notemos que el ciclo τ_{12} es una permutación impar dado que su longitud es par y por lo tanto $\tau_{12}\tau' \in A_n$; así, como $(\tau_{12}\tau')^k = \tau_{12}^k\tau'^k = \sigma_1\sigma_2\sigma' = \sigma$, queda de nuevo demostrado que σ tiene una raíz k-ésima en A_n.

Supongamos ahora que se satisface (ii). Vamos a construir una raíz k-ésima en A_n para σ considerando las diferentes longitudes de los ciclos de la factorización completa de σ. Denotamos por σ_ℓ al producto de todos los ciclos de longitud ℓ en la representación como ciclos disjuntos de σ. Denotamos por c_ℓ al número de ciclos de longitud ℓ en σ. Dado que σ tiene una raíz k-ésima en S_n, por el Teorema 2.5 sabemos que $c_\ell = m_\ell s_\ell$. Usando el algoritmo de la proposición 2.4 se construye una raíz k-ésima en S_n en forma de un ciclo de longitud ℓs_ℓ para cada grupo de s_ℓ ciclos de longitud ℓ. Por lo tanto, podemos construir una raíz k-ésima para σ_ℓ, digamos τ_ℓ, que es un producto de m_ℓ ciclos disjuntos cada uno de longitud ℓs_ℓ. Para valores impares de ℓ, se tiene que ℓs_ℓ es impar y por ello todas las permutaciones comprendidas en τ_ℓ son permutaciones pares. Por tanto, $\tau_\ell \in A_n$ siempre que ℓ sea impar. Por otro lado, cuando ℓ es par, se sigue que ℓs_ℓ también es par y en este caso todos los ciclos comprendidos en τ_ℓ son impares; de donde se deduce que $\tau_\ell \in A_n$ si y solo si m_ℓ es par. De la condición (ii) se deduce que existe un número impar de valores de ℓ tal que m_ℓ es par y por tanto τ_ℓ es impar. En consecuencia, si hacemos

$$\tau_0 = \prod_{\ell \in \mathbb{N}} \tau_\ell,$$

entonces $\tau_0 \in A_n$ y

$$\tau_0^k = \prod_{\ell \in \mathbb{N}} \tau_\ell^k = \prod_{\ell \in \mathbb{N}} \sigma_\ell = \sigma.$$

Por lo tanto, para este caso también tenemos para σ una raíz k-ésima en A_n.
($\Longrightarrow$)
Supongamos que $\sigma = \tau^k$ para algún $\tau \in A_n$. Obviamente, σ tiene una raíz k-ésima en S_n. Supongamos por contradicción que ambas condiciones, (i) y (ii), fallan. Esto es, asumimos que para todos los valores impares de ℓ, $m_\ell \leq 1$, y que la suma $m_2 + m_4 + m_6 + \ldots$ es impar. Para cada $\ell \in \mathbb{N}$, denotamos por σ_ℓ al producto de todos los ciclos de longitud ℓ en la representación como ciclos disjuntos de σ. Dado que $\tau^k = \sigma$, para cada $\ell \in \mathbb{N}$ podemos encontrar un producto de ciclos disjuntos, τ_ℓ, en la descomposición cíclica de τ tal que $\tau_\ell^k = \sigma_\ell$.

Notemos que si σ no contiene ciclos de longitud ℓ, para algún ℓ dado, podemos asumir que τ_ℓ es la permutación identidad.

Por lo tanto

$$\sigma = \prod_{\ell \in \mathbb{N}} \sigma_\ell$$

y

$$\tau = \prod_{\ell \in \mathbb{N}} \tau_\ell.$$

Para tener la contradicción, es suficiente demostrar que $\tau_\ell \notin A_n$ para un número impar de valores $\ell \in \mathbb{N}$, pues eso implica que $\tau \notin A_n$. Vamos a hacer dicha demostración apoyándonos en dos afirmaciones, en donde se considera la paridad de ℓ.

Afirmación 3.5. *Para todos los valores impares de $\ell \in \mathbb{N}$, $\tau_\ell \in A_n$.*

Demostración de la afirmación. Supongamos que ℓ es impar. Como se asumió que $m_\ell \leq 1$, para todo ℓ impar, tenemos dos casos para m_ℓ. Si $m_\ell = 0$, entonces τ_ℓ es la permutación identidad, la cual pertenece a A_n. Ahora supongamos que $m_\ell = 1$, esto es, σ tiene exactamente s_ℓ ciclos de longitud ℓ. Vamos a mostrar que τ_ℓ es un ciclo de longitud ℓs_ℓ. Consideremos cualquier ciclo τ_{ℓ_0} de longitud ℓ_0 en la representación cíclica de τ_ℓ. Por el lema 1.19, $\tau_{\ell_0}^k$ consiste de $\mathrm{mcd}(\ell_0, \mathrm{k})$ ciclos disjuntos de longitud $\frac{\ell_0}{\mathrm{mcd}(\ell_0, \mathrm{k})} = \ell$. Luego, dado que $\tau_{\ell_0}^k$ tiene una raíz k-ésima en S_n, por el teorema 2.5, se tiene que el número de ciclos de longitud ℓ en $\tau_{\ell_0}^k$ debe ser un múltiplo de s_ℓ; es decir, $\mathrm{mcd}(\ell_0, \mathrm{k})$ es un múltiplo de s_ℓ. Sin embargo, los ciclos de $\tau_{\ell_0}^k$ están en σ que contiene exactamente s_ℓ ciclos de longitud ℓ y por tanto, $\mathrm{mcd}(\ell_0, \mathrm{k}) = \mathrm{s}_\ell$. Entonces, como $\frac{\ell_0}{\mathrm{mcd}(\ell_0, \mathrm{k})} = \ell$, sabemos que $\ell_0 = \ell s_\ell$. Por lo tanto, τ_ℓ está conformado por un único ciclo de longitud impar ℓs_ℓ; de manera que $\tau_\ell \in A_n$. □

Afirmación 3.6. *Sea $\ell \in \mathbb{N}$ par. Entonces $\tau_\ell \in A_n$ si y solo si m_ℓ es par.*

Demostración de la afirmación. Sea ℓ un entero positivo par. Por definición de m_ℓ, existen $m_\ell s_\ell$ ciclos de longitud ℓ en σ. Supongamos que τ_{ℓ_0} es un ciclo de longitud

ℓ_0 en τ_ℓ. Por lo tanto, $\tau_{\ell_0}^k$ produce $\text{mcd}(\ell_0, k)$ ciclos de longitud $\frac{\ell_0}{\text{mcd}(\ell_0,k)} = \ell$. Ahora mostraremos que ℓ_0 es un múltiplo impar de ℓs_ℓ, esto es, $\ell_0 = \ell s_\ell \cdot r$ con r impar. Para empezar notemos que $\text{mcd}(\ell_0, k) \in G_k(\ell)$ (por la definición de $G_k(\ell)$). Entonces de la proposición 2.18 se sigue que s_ℓ divide a $\text{mcd}(\ell_0, k)$, es decir, $\text{mcd}(\ell_0, k) = s_\ell \cdot r$, para algún entero positivo r. Ahora, de las hipótesis sabemos que 2 divide a s_ℓ y por tanto solo resta demostrar que r es impar. Si h es el máximo exponente de 2 tal que 2^h divide a k, entonces 2^h divide a s_ℓ. Si r fuera divisible por 2 tendríamos que 2^{h+1} divide a $\text{mcd}(\ell_0, k)$, lo cual es una contradicción y por lo tanto r tiene que ser impar.

Por lo anterior, $\tau_{\ell_0}^k$ es el producto de un número impar de ciclos de longitud ℓ. Es decir $\tau_{\ell_0}^k$ es una permutación impar, y como k es par entonces τ_{ℓ_0} es impar, para cada ciclo τ_{ℓ_0} en τ_ℓ. Por lo tanto, $\tau_\ell \in A_n$ si y solo si existe un número par de ciclos τ_{ℓ_0} en τ_ℓ. Luego, dado que cada elemento τ_{ℓ_0} tiene un número impar de múltiplos de s_ℓ ciclos de longitud ℓ y σ_ℓ consiste de $m_\ell s_\ell$ ciclos de longitud ℓ, entoncs existe un número par de ciclos τ_{ℓ_0} en τ_ℓ si y solo si m_ℓ es par. Por lo tanto, $\tau_\ell \in A_n$ si y solo si m_ℓ es par.

□

Dado que $m_2 + m_4 + \ldots$ es impar, existe un número impar de valores de ℓ, ℓ un par positivo, tal que m_ℓ es impar. Por tanto, $\tau_\ell \notin A_n$ para un número impar de valores de ℓ. Como $\tau = \prod_{\ell \in \mathbb{N}} \tau_\ell$, concluímos que $\tau \notin A_n$, una contradicción.

□

El siguiente corolario, aparece como teorema en el artículo de Pournaki, publicado en 2008 (antes del artículo de Annin, et al.) en donde se caracteriza las raíces cuadradas en A_n.

Corolario 3.7. *Para $\sigma \in S_n$ de tipo $\boldsymbol{c} = (c_1, \ldots, c_n)$ se tiene que σ tiene una raíz cuadrada en A_n, si y solo si se satisfacen las siguientes dos condiciones:*

1) c_{2h} es par para todo h, y

2) (a) $\sum_i c_{2i}$ es un múltiplo de 4, o

(b) $c_{2j-1} > 1$ para algún j.

La siguiente observación es útil para entender las raíces cuadradas pares de permutaciones de cierto tipo.

Observación 3.8. *Sea $\sigma \in A_n$ una permutación del tipo $(\ell)^c$.*

1. *Sean ℓ y c pares. Si σ tiene una raíz cuadrada en A_n entonces todas sus raíces cuadradas son pares. De lo contrario, todas sus raíces cuadradas son impares.*

2. *Si ℓ es impar y $c \geq 2$, entonces σ tiene raíces cuadradas pares y raíces cuadradas impares.*

3.2 Resultados originales

En esta sección se presentan resultados originales sobre el número de raíces cuadradas de permutaciones pares. Algunas demostraciones son puramente combinatorias y posteriormente se presentan algunas funciones generadoras exponenciales para ciertos tipos de permutaciones.

3.2.1 Fórmula para el número de raíces cuadradas en A_n de una permutación par

La proposición 3.1 nos permite afirmar que para cuando k es impar el número de raíces k-ésimas en A_n de una permutación par se obtiene usando la fórmula dada por Leaños et al. [15].

Denotamos el número de raíces cuadradas pares (resp. impares) de σ como $rp(\sigma)$ (resp. $ri(\sigma)$).

A continuación se presentan una serie de resultados que nos permite conocer el número de raíces cuadradas pares de un tipo especial de permutaciones, las del tipo $(\ell)^c$. El primero de estos resultados considera el caso ℓ par.

Teorema 3.9. *Sea $\sigma \in A_n$ una permutación del tipo $(\ell)^c$ con ℓ y c pares, entonces el número de raíces cuadradas de σ está dado por*

$$r_n^2(\sigma) = \frac{c!\ell^{c/2}}{2^{c/2}(c/2)!}.$$

Aún más,

- *si $c = 4x$ para algún $x \in \mathbb{N}$, entonces $rp(\sigma) = r_n^2(\sigma)$,*
- *en otro caso, $ri(\sigma) = r_n^2(\sigma)$.*

Demostración: Dado que ℓ es un entero par se sigue que $((\ell, 2)) = 2$ y entonces $G_2(\ell) = \{2\}$. Luego como c es par existe $p \in \mathbb{N}$ tal que $c = 2p$, o bien $p = c/2$. De manera que tomando $g = 2$ estamos en las hipotesis de la proposición 2.24 y por tanto el número de raíces cuadradas de σ está dado por

$$\frac{c!\ell^{c/2}}{2^{c/2}(c/2)!}.$$

Resta demostrar que para σ todas sus raíces están en A_n o bien, todas sus raíces están en el complemento de A_n respecto a S_n, esto es, son impares.

Si τ es una permutación tal que $\tau^2 = \sigma$ y σ es del tipo $(\ell)^c$, por la observación 2.30 (2) se sigue que τ es del tipo $(2\ell)^{c/2}$. Por lo tanto si $c = 4x$, entonces τ se compone de $2x$ ciclos de longitud par, es decir ciclos impares, y por lo tanto es una permutación par. Para el caso cuando c no es múltiplo de 4, dado que por hipótesis c es par se tiene que $c/2$ es impar y por ello τ es un producto de un número impar de ciclos impares, es decir que τ es una permutación impar.

□

Para el caso cuando ℓ es impar se tienen los teoremas 3.10 y 3.12, que nos dan las fórmulas para el número de raíces cuadradas pares e impares, respectivamente.

Teorema 3.10. *Sea $\sigma \in A_n$ una permutación del tipo $(\ell)^c$, con $\ell = 2j+1$, $j \geq 0$, entonces el número de raíces cuadradas pares de σ está dado por*

$$rp(\sigma) = \sum_{i=0}^{\lfloor c/4 \rfloor} \binom{c}{4i} \frac{\ell^{2i}(4i)!}{2^{2i}(2i)!}.$$

Demostración: La fórmula se cumple cuando $c = 1$ porque σ tiene una única raíz cuadrada τ (por la observación 2.30 (1)), que de hecho es un ciclo de longitud ℓ y por lo tanto $\tau \in A_n$.

Si $c > 1$, como $((\ell, 2)) = 1$, se sigue que $G_2(\ell) = \{1, 2\}$. Es decir, cualquier raíz cuadrada $\tau \in S_n$ de σ esta compuesta por ϵ_1 ciclos de longitud ℓ y ϵ_2 ciclos de longitud 2ℓ, en donde

$$\epsilon_1 + 2\epsilon_2 = c.$$

Como la longitud ℓ es impar, los ϵ_1 ciclos de longitud ℓ en τ serán pares y por lo tanto ϵ_1 puede ser cualquier entero positivo. Entonces, para garantizar que τ esté en A_n es suficiente que el número de ciclos impares en τ sea par, esto es, que $\epsilon_2 = 2x$ para algún $x \in \mathbb{N}$. Por lo anterior, como $2\epsilon_2 = 2(2x)$, se tiene que el número total de ciclos en σ que se agruparan por parejas para formar los ciclos de longitud 2ℓ en τ es un múltiplo de cuatro. Esto es

$$\epsilon_1 + 4x = c.$$

Notemos que $4x \leq c$ implica $x \leq c/4$, de hecho $0 \leq x \leq \lfloor c/4 \rfloor$ dado que $x \in \mathbb{N}$.

La factorización completa por longitudes de τ se vera como $\tau'\tau''$, en donde τ' es del tipo $(2\ell)^{2i}$ y τ'' es del tipo $(\ell)^{c-4i}$, para algún $0 \leq i \leq \lfloor c/4 \rfloor$. Para contar las posibilidades de τ primero vamos a contar las posibilidades para τ'. Para un i fijo, $0 \leq i \leq \lfloor c/4 \rfloor$, de los c ciclos de σ elegimos $4i$ ciclos con los cuales se formaran los ciclos de longitud 2ℓ de τ' (se "pegaran" por parejas usando el algoritmo de la proposición 2.4). Tenemos $\binom{c}{4i}$ maneras de elegir estos ciclos. Ahora, notemos que realizar el "pegado" por parejas de estos $4i$ ciclos es lo mismo que obtener las raíces cuadradas del tipo $(2\ell)^{2i}$ de una permutación σ' del tipo $(\ell)^{4i}$. Por lo que estamos en las hipótesis de la proposición 2.24, con $2p = 4i$ y $g = 2$. Por tanto se tienen

$$\frac{\ell^{2i}(4i)!}{2^{2i}(2i)!}$$

raíces cuadradas pares τ' de σ', para una selección dada de $4i$ ciclos de σ. Finalmente, notemos que, por la observación 2.30 (1), τ'' queda determinada de manera única porque es el producto de las raíces de los $c - 4i$ ciclos de σ (que son únicas para cada ciclo) que no se usaron para obtener τ'. Por lo tanto, como i corre de 0 a $\lfloor c/4 \rfloor$, la fórmula para calcular el número de raíces pares de $\sigma \in A_n$ está dada por

$$rp(\sigma) = \sum_{i=0}^{\lfloor c/4 \rfloor} \binom{c}{4i} \frac{\ell^{2i}(4i)!}{2^{2i}(2i)!}$$

□

Corolario 3.11. *El número de raíces cuadradas pares de la permutación identidad en S_n es*

$$\sum_{i=0}^{\lfloor n/4 \rfloor} \binom{n}{4i} \frac{(4i)!}{2^{2i}(2i)!}.$$

El corolario 3.11 es un resultado conocido debido a Moser y Wyman [20], y corresponde a la serie $A000704$ en OEIS [31].

Teorema 3.12. *Sea $\sigma \in A_n$ una permutación del tipo $(\ell)^c$, con $\ell = 2j+1$ y $c > 1$, entonces el número de raíces cuadradas impares de σ está dado por*

$$ri(\sigma) = \sum_{i=0}^{\lfloor (c-2)/4 \rfloor} \binom{c}{2(2i+1)} \frac{(2(2i+1))!\ell^{2i+1}}{2^{2i+1}(2i+1)!}$$

Demostración: Como se mencionó en la demostración del teorema 3.10, tenemos que para $c > 1$, toda raíz cuadrada τ de σ tiene ϵ_1 ciclos de longitud ℓ y ϵ_2 ciclos de longitud 2ℓ, siempre que $\epsilon_1 + 2\epsilon_2 = c$. Por la paridad de ℓ se sigue que no hay restricciones sobre ϵ_1 puesto que todos estos ϵ_1 ciclos son pares y por tanto lo es su producto; de manera que necesitamos que ϵ_2 sea un entero impar para garantizar que $\tau \notin A_n$. Para obtener el número de raíces impares de σ se cuenta de manera análoga a como lo hicimos en la demostración del teorema 3.10, considerando la factorización completa por longitudes $\tau'\tau''$ de τ. Notemos que es suficiente considerar las posibilidades para obtener los ciclos que componen τ' (los de longitud 2ℓ) pues en este caso τ'' también está únicamente determinado. Entonces se cuentan las diferentes maneras en que podemos agrupar un numero impar de parejas de ciclos, parejas que vamos "a pegar" (usando el algoritmo de la proposición 2.4), y también, de cuantas maneras distintas podemos hacer este "pegado" en cada pareja. Como $2\epsilon_2$ es el número total de ciclos de σ que pegaremos por parejas y $\epsilon_2 = 2x+1$, para algún $x \in \mathbb{N}$, entonces se tiene que $2(2x+1) = 4x+2 \leq c$, lo cual implica que $x \leq \lfloor (c-2)/4 \rfloor$. De modo que para un $\epsilon_2 = 2i+1$ fijo, con $0 \leq i \leq \lfloor (c-2)/4 \rfloor$, tenemos $\binom{c}{2(2i+1)}$ maneras de elegir el número total de ciclos de σ que se pegaran por parejas para obtener exactamente $2i+1$ ciclos impares en τ. Procediendo de manera similar que en la demostración del teorema 3.10 tenemos que la fórmula para calcular el número de raíces impares de $\sigma \in A_n$ está dada por

$$ri(\sigma) = \sum_{i=0}^{\lfloor (c-2)/4 \rfloor} \binom{c}{2(2i+1)} \frac{(2(2i+1))!\ell^{2i+1}}{2^{2i+1}(2i+1)!}$$

□

Corolario 3.13. *El número de raíces cuadradas impares de la permutación identidad id está dado por*

$$ri(id) = \sum_{i=0}^{\lfloor (n-2)/4 \rfloor} \binom{n}{4i+2} \frac{(4i+2)!}{2^{2i+1}(2i+1)!}$$

El corolario anterior es un resultado publicado por Moser y Wyman [20]. En la OEIS [31] el número de raíces impares de orden dos esta asociado a la serie $A001465$.

La siguiente fórmula combina los resultados de los teoremas 3.9, 3.10 y 3.12, y nos permite calcular el número de raíces cuadradas pares de cualquier permutación.

Teorema 3.14. *Sea σ una permutación en A_n cuya factorización completa por longitudes es $\sigma_1 \dots \sigma_m$. Entonces el número de raíces cuadradas pares de σ está dado por*

$$rp(\sigma) = \sum_{\substack{X \subseteq \{1,\dots,m\} \\ |X| \text{ es par}}} \prod_{i \in X} ri(\sigma_i) \prod_{j \in \overline{X}} rp(\sigma_j),$$

en donde $\overline{X} := \{1, \dots, m\} - X$.

Demostración: Toda raíz cuadrada τ de una permutación expresada en su factorización completa por longitudes, $\sigma = \sigma_1 \dots \sigma_m$, puede expresarse como un producto de raíces $\tau_1, \dots, \tau_m$ tal que τ_i es una raíz de σ_i, $i \in \{1, \dots, m\}$. Por los teoremas 3.9, 3.10 y 3.12 tenemos una manera de contar para cada σ_i la cantidad de raíces pares e impares, denotadas por $rp(\sigma_i)$ y $ri(\sigma_i)$ respectivamente, por tanto podemos contar la cantidad de raíces pares de σ considerando productos de raíces τ_i que nos garanticen que el producto sea par. Entonces, $\tau = \tau_1 \dots \tau_m$ es una raíz par de σ si se tiene un número par de τ_i's que sean impares pues eso nos garantiza que el producto total τ de los τ_i sea par. Es decir, si para $X \subseteq \{1, \dots, m\}$ y $\overline{X} = \{1, \dots, m\} - X$ se tiene que $\tau = \tau_X \tau_{\overline{X}}$, con

$$\tau_X = \prod_{i \in X} \tau_i,$$

$$\tau_{\overline{X}} = \prod_{j \in \overline{X}} \tau_j,$$

en donde τ_X es un producto de puras permutaciones τ_i impares, $i \in X$, y $\tau_{\overline{X}}$ es un producto de puras permutaciones τ_j pares, $j \in \overline{X}$. Por lo que τ sera par sólo si se cumple que $|X|$ es par. Así pues, fijando un $X \subseteq \{1, \dots, m\}$ con $|X|$ par, se tiene que la cantidad de raíces cuadradas pares τ de σ de la forma $\tau_X \tau_{\overline{X}}$ está dada por

$$\prod_{i \in X} ri(\sigma_i) \prod_{j \in \overline{X}} rp(\sigma_j).$$

Para contar todas las raíces cuadradas pares de σ resta entonces considerar todas las posibilidades que tenemos para elegir el conjunto X, con $0 \leq |X| \leq m$ y $|X|$ par, y sumar todas las raíces cuadradas de las formas $\tau = \tau_X \tau_{\overline{X}}$ para cada X. Por lo tanto, el número total de raíces cuadradas pares de σ es igual a

$$rp(\sigma) = \sum_{\substack{X \subseteq \{1,\ldots,m\} \\ |X| \text{ es par}}} \prod_{i \in X} ri(\sigma_i) \prod_{j \in \overline{X}} rp(\sigma_j).$$

□

De manera análoga a la demostación 3.14 se demuestra el siguiente teorema.

Teorema 3.15. *Sea σ una permutación en A_n cuya factorización completa por longitudes es $\sigma_1 \ldots \sigma_m$. Entonces el número de raíces cuadradas impares de σ está dado por*

$$ri(\sigma) = \sum_{\substack{X \subseteq \{1,\ldots,m\} \\ |X| \text{ es impar}}} \prod_{i \in X} ri(\sigma_i) \prod_{j \in \overline{X}} rp(\sigma_j),$$

en donde $\overline{X} := \{1, \ldots, m\} - X$.

3.2.2 Algunas funciones generadoras

En esta sección mostraremos algunas funciones generadoras. El siguiente teorema muestra una función generadora para el número de raíces cuadradas pares de cualquier permutación del tipo $(\ell)^c$.

Teorema 3.16. *Para ℓ fijo, la función generadora exponencial del número de raíces cuadradas pares de una permutación σ del tipo $(\ell)^c$ es*

$$\exp\left((\ell \bmod 2)x\right) \cosh\left(\frac{\ell}{2}x^2\right).$$

Demostración: Primero, analicemos los casos respecto a la paridad de ℓ.

Caso 1: Si ℓ es impar, por el corolario 2.34 tenemos que $\exp\left(x + \frac{\ell}{2}x^2\right)$ es la función generadora para el número de raíces cuadradas de σ. Cualquier raíz cuadrada τ de σ es del tipo $\ell^{\epsilon_1}(2\ell)^{\epsilon_2}$, con $c = \epsilon_1 + 2\epsilon_2$ y ϵ_i no negativo. En la función generadora el factor $\exp(x)$ representa el número de maneras de tener ciclos del tipo ℓ^{ϵ_1} en τ y $\exp\left(\frac{\ell}{2}x^2\right)$ el número de maneras de tener ciclos de longitud 2ℓ en τ. Por lo anterior, para que las raíces sean pares basta garantizar que la parte de τ de la forma $(2\ell)^{\epsilon_2}$ sea par, es decir, solo nos interesan las potencias pares de ℓ y por tanto es necesario usar la subserie de potencias pares de la serie exponencial, que es precisamente $\cosh\left(\frac{\ell}{2}x^2\right)$. Así pues, la función generadora de la fórmula para raíces pares y cuando ℓ es impar es

$$\exp(x) \cosh\left(\frac{\ell}{2}x^2\right) \tag{3.1}$$

Caso 2: Si ℓ es par sabemos que las raíces cuadradras τ de σ son todas de la forma $(2\ell)^{\epsilon}$ y por el corolario 2.33 se sigue que la función generadora para el número de raíces de σ es $\exp\left(\frac{\ell}{2}x^2\right)$. Por lo tanto, si queremos contar las raíces cuadradas pares, como antes, tenemos que sustituir a la serie exponencial por la subserie coseno hiperbólico. Entonces la función generadora de la fórmula para raíces pares y cuando ℓ es impar es

$$\cosh\left(\frac{\ell}{2}x^2\right). \tag{3.2}$$

Ahora, necesitamos encontrar una única función generadora sin importar la paridad de ℓ. Notemos que las funciones 3.1 y 3.2 coinciden en $\cosh\left(\frac{\ell}{2}x^2\right)$ pero difieren por el factor $\exp(x)$, por tanto la siguiente función es la función generadora para el número de raíces pares de σ

$$\exp\left((\ell \bmod 2)x\right)\cosh\left(\frac{\ell}{2}x^2\right).$$

□

El siguiente ejemplo muestra el uso de la función generadora del teorema anterior.

Ejemplo 3.2.1. *Para $\ell = 2$, tenemos que la expansión de*

$$\exp\left((\ell \bmod 2)x\right)\cosh\left(\frac{\ell}{2}x^2\right)$$

es

$$1 + \frac{x^4}{2} + \frac{x^8}{24} + \frac{x^{12}}{720} + \frac{x^{16}}{40320} + \frac{x^{20}}{3628800} + \dots$$

que es igual a

$$1 + 12\frac{x^4}{4!} + 1680\frac{x^8}{8!} + 665280\frac{x^{12}}{12!} + \dots$$

De donde se sigue, que si σ es del tipo $(2)^4$ entonces tiene 12 raíces cuadradas pares; si σ es del tipo $(2)^8$ entonces tiene 1680 raíces cuadradas pares, etcétera.

El teorema a continuación expone una función generadora para el número de raíces cuadradas pares de una permutación del tipo $(\ell)^c$.

Teorema 3.17. *Para ℓ fijo, la función generadora exponencial del número de raíces cuadradas impares de una permutación del tipo $(\ell)^c$ es*

$$\exp\left((\ell \bmod 2)x\right)\sinh\left(\frac{\ell}{2}x^2\right)$$

Demostración: La demostración es bastante similar a la del teorema 3.16. Si τ es tal que $\tau^k = \sigma$, entonces sabemos que τ es de la forma $(\ell)^{\epsilon_1}(2\ell)^{\epsilon_2}$, donde $\epsilon_1 + 2\epsilon_2 = c$ y ϵ_i no negativo. Notemos que en la parte $(\ell)^{\epsilon_2}$ de τ, $\epsilon_2 \neq 0$ solo cuando ℓ es impar. Por tanto, garantizar que $\tau \notin A_n$ se reduce a que garanticemos que la parte de τ del tipo $(2\ell)^{\epsilon_2}$ sea impar. Para ello bastará reemplazar en la demostración 3.16 al $\cosh\left(\frac{\ell}{2}x^2\right)$ por $\sinh\left(\frac{\ell}{2}x^2\right)$, dado que esta última es la subserie de potencias impares de la serie exponencial. Por tanto, reproduciendo dicha demostración con esta sustitución tenemos la función generadora deseada

$$\exp\left((\ell \bmod 2)x\right)\sinh\left(\frac{\ell}{2}x^2\right).$$

□

Bibliografía

[1] M. A. Abdelraheem, G. Leander, E. Zenner, Differential cryptanalysis of round-reduced PRINTcipher: Computing roots of permutations, *In Antoine Joux*, Proc. FSE 2011, LNCS, vol. 6733, Springer Verlag (2011), 1-17.

[2] R. M. Adin, A. Postnikov e Y. Roichman, Combinatorial Gelfand Models, *J. Algebra,* **320** (3) (2008), 1311–1325.

[3] S. Annin, T. Jansen and C. Smith, On kth roots in the symmetric and alternating groups, *Pi Mu Epsilon Journal*, **12**, No. 10 (2009), 581-589.

[4] E. A. Bender, Asymptotics methods in enumeration, *SIAM Rev.* 16 (1974), 485–515. Errata: *SIAM Rev.* 18 (1976), 292.

[5] J. Blum, Enumeration of the square permutations in $\mathfrak{S}_n$, *J. Comb. Theory,* (A) **17**, (1974), 156–161.

[6] M. Bóna, A. McLennan and D. White, Permutations with roots, *Random Structures* $\mathfrak{E}$ *algorithms,* **17** (2000), No. 2, 157–167.

[7] I. Z. Bouwer and W. W. Chernoff, Solutions to $x^r = \alpha$ in the symmetric group, *Ars. Combin.* **20** (1985) 83–88.

[8] W. W. Chernoff, Permutations with p^l-th roots, *Disc. Math.*, 125 (1994) 123–127.

[9] I. S. Chowla, I. N. Herstein and W. R. Scott, The solution of $x^d = 1$ in symmetric groups, *Norske Vid. Selsk.* **25**, No. 2, (1952), 29-31,

[10] A. K. Das, On group elements having square roots *Bulletin of the iranian Mathematicas Society*, **31**, No. 2 (2005), 33-36

[11] D. S. Dummit and R. M. Foote, Abstract Algebra. *Prentice Hall Englewood Cliffs*, 3rd edition, 2004.

[12] H. Fripertinger and P. Lackner, Tone rows and tropes, Journal of Mathematics and Music, 9:2, (2015). 111-172.

[13] A. Groch, D. Hofheinz, and R. Steinwandt, A practical attack on the root problem in braid groups, *Contemporary Math.*, **418** (2006), 121–132.

[14] E. Khamseh, M. R. R. Moghaddam, F. G. Russo, and F. Saeedi Elements with r-th roots in finite groups

[15] J. Leaños, R. Moreno, y L. Rivera-Martínez, On the number of mth roots of permutations, *Australas. J. Combin.* **52**, 41–54 (2012).

[16] N. A. Loehr, Bijective combinatorics, *Chapman and Hall/ CRC Press*, Boca Raton, FL, 2011.

[17] M. S. Lucido and M. R. Pournaki, Elements with square roots in finite groups *Algebra Colloq.* **12** (4) (2005), 677-690.

[18] M. S. Lucido and M. R. Pournaki, Probability that an element of a finite group has a square root, *Colloq. Math.* **112** (2008), 147-155.

[19] P. L. Méliot. Asymptotics of the Gelfand models of the symmetric groups. *arXiv. 1009.4047v1*, 2010.

[20] L. Moser and M. Wyman, On the solutions of $x^d = 1$ in symmetric groups. *Canad. J. Math.* (1955) 7, No. 2, 159-168.

[21] A. I. Pavlov, On the number of solutions of the equation $x^k = a$ in the symmetric group S_n, *Mat. Sb.*, **112(154)**(1980), 380–395; English *transl. Math. USSR Sb.*, **40** (1981).

[22] A. I. Pavlov, The number and cycle structure of solutions of a system of equations in substitutions, *Diskretnaya Matematika* (1989) 1, No. 1, 94-104, and No. 2, 143-154 (in Russian).; English *Discrete Math. Appl,* Vol. 1, No. 2, pp. 195-217 (1991)

[23] M. R. Pournaki, On the number of even permutations with roots, *Australas. J.Combin.*, **45** (2009), 37–42.

[24] N. Pouyanne, On the number of permutations admitting an mth root, *Electron. J. Comb.*, **9** (2002), $\#R3$., 1–12.

[25] Y. Roichman, A note on the number of k-roots in S_n, *Sem. Lothar. Combin.* **70** (2014), Article B70i, 5pp.

[26] J. Rotman, An Introduction to the Theory of Groups, 4th edition, *Springer-Verlag*, Berlin, 1995.

[27] A. Sadeghieh y K. Ahmadidelir, n-th Roots in finite polyhedral and centro-polyhedral groups, *Proc Math Sci*, **125** (4) (2015) 125–487.

[28] A. Sadeghieh y H. Dostie, The nth roots of elements in finite groups, *Mathematical Sciences* **2** (2008) 347–356.

[29] B. E. Sagan. The Symmetric Group. Graduate Texts in Mathematics. *Springer*, 2001.

[30] V. Schoup, A Computational Introduction to Number Theory and Algebra, *Cambridge University Press*, 2nd edition, (2008)

[31] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences, http://oeis.org.

[32] R. Stanley, Enumerative combinatorics. Vol. 2, vol. 62 of Cambridge Studies in Advanced Mathematics. *Cambridge University Press*, Cambridge, 1999.

[33] P. Turán, On some connections between combinatorics and group theory, *Colloq. Math. Soc. János Bolyai, P. Erdös, A. Rényi and V. T. Sós, eds.*, North Holland, Amsterdan (1970), 1055–1082.

[34] (warlimont2) R. Warlimont, Permutations with roots, *Arch. Math. (Basel)* **67** (1996), no. 1, 23–34.

[35] H. S. Wilf, Generatingfunctionology, *Academic Press*, San Diego, 2nd edition, (1994).