Anales Acad. Nac. de Cs. Ex., Fís. y Nat., tomo 71 (2019): 49-55.

GRUPOS LIBRES Y EL WINDING INVARIANT

Jonathan A. Barmak

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires – Instituto de Investigaciones Matemáticas Luis A. Santaló, CONICET. Pabellón I, Ciudad Universitaria, 1428 Buenos Aires, Argentina. (email: jbarmak@dm.uba.ar)

Resumen

En esta nota estudiamos el grupo libre F_2 generado por x, y utilizando el winding invariant. Damos una demostración de un resultado de Lyndon y Newman que afirma que $xyx^{-1}y^{-1}$ no es un producto de dos cuadrados. Nuestro enfoque es elemental y dirigido a un público amplio.

Palabras clave: Grupos libres, conmutador, winding number.

Abstract

Free groups and the winding invariant. In this note we study the free group F_2 generated by x, y using the winding invariant. We give a proof of a result by Lyndon and Newman which claims that the commutator $xyx^{-1}y^{-1}$is not a product of two squares. Our approach is elementary and aimed at a general reader.

Key words: Free groups, commutator, winding number.

El objetivo de este trabajo es presentar algunos de los resultados obtenidos en nuestros artículos [1, 2, 3]. La exposición está especialmente dirigida a investigadores de otras áreas y demás interesados fuera del ámbito científico. Al lector con una formación matemática más profunda le aconsejamos consultar la fuente. Intentaremos transmitir las ideas principales a partir de las definiciones de los conceptos más básicos. Las demostraciones serán sencillas y detalladas para que todos puedan seguir los argumentos.

Los grupos son unas de las estructuras algebraicas más elementales, con aplicaciones en todas las ramas de Matemática, en Física, Química y Computación. Un grupo es un conjunto con una operación que cumple determinadas propiedades. Los números enteros, denotados con la letra $\mathbb{Z}$, forman un grupo con la operación $+$: uno puede sumar dos números enteros y obtiene un nuevo entero. La operación $+$ de los enteros cumple la propiedad asociativa: $(a+b)+c=a+(b+c)$. Los paréntesis indican el orden en el que se deben efectuar las operaciones. Otra propiedad que satisfacen los enteros es la existencia de un elemento neutro: el número 0 cumple que $a+0=a$ y $0+a=a$ para cualquier entero a. Además, todo entero tiene un inverso respecto de la operación. Es decir que si a es un entero, existe otro número entero que sumado a a da 0. Por supuesto, es el número que denotamos $-a$. Esas tres propiedades conforman de hecho la definición de grupo. Un grupo es un conjunto G junto con una operación $\circ$ (para cualesquiera dos elementos a, b de G, resulta que $a \circ b$ es un elemento de G) que cumplen

asociatividad, existencia de elemento neutro y existencia de inversos para todo elemento de G. Un grupo distinto de los enteros es por ejemplo el grupo $\mathbb{Z}_2$ que consta sólo de dos elementos: 0 y 1, con la operación denotada $+$ definida de esta forma: $0+0=0, 0+1=1, 1+0=1, 1+1=0$. Es fácil chequear que 0 es el elemento neutro, que el inverso de cada elemento es sí mismo y que la operación es asociativa. Los dos ejemplos que vimos cumplen una propiedad extra que no es requerida por la definición de grupo: la propiedad conmutativa. Tanto en $\mathbb{Z}$ como en $\mathbb{Z}_2$ vale que $a+b=b+a$. Un grupo se dice *abeliano* si cumple esto, que la operación $\circ$ es conmutativa, es decir si $a \circ b = b \circ a$ para cualesquiera elementos a, b. Cuando el grupo no es abeliano (o cuando no sabemos si lo es, o si lo deseamos), los inversos de los elementos no se escriben con un signo $-$ adelante sino con un exponente igual a -1. Así, el inverso de $a \in G$ es a^{-1}. La relación de conmutatividad $a \circ b = b \circ a$ se puede reescribir de otra forma, si multiplicamos la igualdad a derecha por a^{-1} obtenemos $a \circ b \circ a^{-1} = b \circ a \circ a^{-1} = b$. La segunda igualdad se sigue de que $a \circ a^{-1}$ es el neutro del grupo y entonces podemos omitirlo. Multiplicando nuevamente a derecha por b^{-1} obtenemos $a \circ b \circ a^{-1} \circ b^{-1} = b \circ b^{-1} = 0$. Acá notamos con 0 al elemento neutro aunque no es la notación estándar. Cuando uno trabaja con un grupo, para ahorrar tiempo y espacio, suele omitir el símbolo que denota a la operación. Así, para escribir $a \circ b$ simplemente escribe ab. Luego, un grupo es abeliano si cumple la relación $aba^{-1}b^{-1} = 0$ para todos sus elementos. En lugar de $a \circ a$ escribiremos a^2 y en lugar de $a^{-1} \circ a^{-1} \circ a^{-1}$, escribiremos a^{-3}, por ejemplo.

El grupo $\mathbb{Z}_2$ cumple la relación de conmutatividad y también cumple la relación $a^2 = 0$ para cualquier a, pues tanto $0+0$ como $1+1$ son el neutro. Hay grupos que en algún sentido no cumplen ninguna relación, los denominados *grupos libres*. Estos son un poco más difíciles de describir que los ejemplos anteriores. El grupo libre de rango 2 se denota F_2 y sus elementos son las palabras en las letras x, y y sus inversos. Así, algunos elementos de F_2 son $xyxyx, x^3, yx^{-5}y^{-1}x^2$, por ejemplo. La operación de F_2 es fácil de definir: es simplemente la concatenación. Así $xyxyx \circ yx^{-5}y^{-1}x^2 = xyxyxyx^{-5}y^{-1}x^2$ y también $xyxyx \circ x^3 = xyxyx^4$. Al concatenar dos palabras, puede haber cancelación. Por ejemplo $xyx \circ x^{-1}y^2x = xy^3x$ y también $y^2xy^{-3} \circ y^3x^{-1}y^{-1} = y$. Uno puede verificar que la operación es asociativa. El elemento neutro es la palabra vacía, que no tiene ninguna letra, y el inverso de una palabra es la misma palabra leída en sentido inverso y con los exponentes cambiados por sus opuestos. Así, el inverso de $y^2xy^{-3}x^{-4}$ es $x^4y^3x^{-1}y^{-2}$.

El grupo F_2 no es abeliano, puesto que ni siquiera x e y conmutan, ya que $xyx^{-1}y^{-1}$ es una palabra no trivial (es decir, no es equivalente a la palabra vacía por medio de cancelaciones).

Si bien los grupos libres se definen fácilmente y son los más simples que existen en el sentido de no cumplir relaciones, hay todavía muchos problemas abiertos que los conciernen y se estudian en la actualidad [4]. Varios de estos problemas se investigan no sólo con herramientas algebraicas y combinatorias sino por medio de ideas geométricas y topológicas.

A modo de ejemplo, en [5] Lyndon y Newman consideran la siguiente pregunta: es la palabra $c = xyx^{-1}y^{-1}$ un producto de dos cuadrados en F_2? Es decir, existen palabras $u, v \in F_2$ tales que $c = u^2v^2$? Es interesante observar que c sí es un producto de **tres** cuadrados. A saber, si tomamos $u = x, v = x^{-1}y, w = y^{-1}$, entonces

$$u^2v^2w^2 = x^2(x^{-1}y)^2y^{-2} = x^2x^{-1}yx^{-1}yy^{-2} = xyx^{-1}y^{-1}.$$

Para entender la dificultad de un problema es recomendable pensarlo por cuenta propia antes de leer una solución. Justamente al encontrarse con las dificultades es que uno aprende. Aún si no halla una respuesta, la lectura posterior de una solución le será mucho más provechosa, porque su cabeza ya sabrá en dónde estaban los obstáculos y así capitalizará las ideas nuevas.

Lyndon y Newman proponen en [5] tres demostraciones distintas de que la respuesta a su pregunta es negativa: c no es un producto de dos cuadrados.
Cabe señalar que, aunque en ese entonces no se sabía, existe hoy un método general que permite decidir cuándo una palabra dada es un producto de 2 cuadrados utilizando la noción de Wicks word [6].

A continuación definiremos el *winding invariant*, un invariante que presentamos en [2] para estudiar diferentes cuestiones relacionadas con grupos libres y los llamados grupos *metabelian.* Veremos a modo de ejemplo que el winding invariant puede ser usado para obtener una demostración alternativa y más conceptual del resultado de Lyndon y Newman. Esta demostración es más simple que la original y que otras demostraciones posteriores.

El exponente total de la letra x en una palabra $w \in F_2$ es la suma de todos los exponentes con los que aparece la letra x en w. Por ejemplo el exponente total de x en $w = x^{-4}yxy^6$ es $exp(x,w) = -3$ y en c es $exp(x,c) = 0$. De manera análoga se define el exponente total de y. Denotamos ${F_2}'$ al subconjunto de F_2 formado por las palabras cuyos exponentes totales de x y de y son ambos cero. Notar que si dos palabras están en ${F_2}'$ también lo está su producto y el inverso de cada una.

Dada una palabra $w \in F_2$, vamos a definir una curva en el plano asociada. En realidad esta curva γ_w es una poligonal contenida en la grilla $\mathbb{R}\times\mathbb{Z} \cup \mathbb{Z}\times\mathbb{R}$, que es un subconjunto del plano. Para construir esta poligonal que comienza en el origen $(0,0)$, hacemos lo siguiente. Leeremos la palabra w y cada vez que encontremos una x nos moveremos una unidad hacia la derecha, mientras que si encontramos una x^{-1} nos desplazaremos hacia la izquierda. Una y nos indicará que debemos ir hacia arriba y una y^{-1}, hacia abajo. Por ejemplo la curva γ_c asociada a $c = xyx^{-1}y^{-1}$ recorre cuatro segmentos de longitud 1: el primero va hacia la derecha, el segundo hacia arriba, el tercero hacia la izquierda y el último hacia abajo. La curva asociada a $u = x^3y^{-2}x^{-1}y^4$ recorre diez segmentos de longitud 1 y en cierto punto se cruza a sí misma, como se ve en Fig. 1.

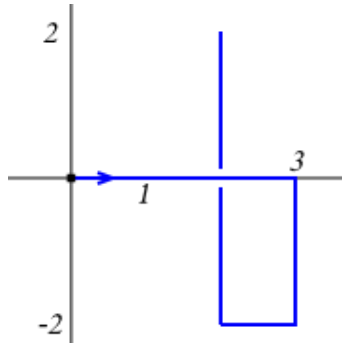

Fig. 1: La curva γ_u en azul termina en el punto (2.2).

Es fácil notar que el punto final de la curva γ_w es $(exp(x,w), exp(y,w))$. Por lo tanto, si $w \in F_2'$, la curva es cerrada.

Definición 1. Dada $w \in F_2'$, para cada par de números enteros (i,j) vamos a definir el número $a_{i,j}$ como la cantidad de vueltas que γ_w da alrededor del punto $\left(i+\frac{1}{2}, j+\frac{1}{2}\right)$ en sentido antihorario. Esto es lo que se conoce como el *winding number* de la curva alrededor de dicho punto.

Hay distintas formas de entender el winding number de γ_w alrededor del punto $p = \left(i+\frac{1}{2}, j+\frac{1}{2}\right)$. Podemos imaginar un observador parado en p y a otra persona A que camina recorriendo la curva. El observador, sin moverse de p, gira sobre sí mismo mirando todo el tiempo a A. El winding number es la cantidad de vueltas que el observador da sobre su eje desde el principio hasta el final del recorrido de A. Una segunda interpretación equivalente del winding number es la siguiente. Podemos trazar una semirrecta horizontal que empieza en p y se extiende indefinidamente hacia la derecha. El winding number de γ_w alrededor de p es la cantidad de veces que la curva atraviesa la semirrecta de abajo hacia arriba menos la cantidad de veces que la atraviesa de arriba hacia abajo.

Ejemplo 2. Sea $w = x^2yx^{-4}yxy^{-2}x$. La curva γ_w aparece en Fig. 2,

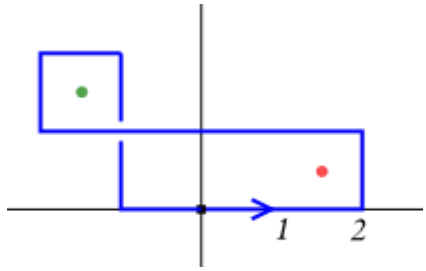

Fig. 2. La curva γ_w en azul, el punto $\left(1+\frac{1}{2}, \frac{1}{2}\right)$ en rojo y $\left(-2+\frac{1}{2}, 1+\frac{1}{2}\right)$ en verde.

Como γ_w da una vuelta alrededor del punto $\left(1+\frac{1}{2}, \frac{1}{2}\right)$, el coeficiente $a_{1,0}$ es igual a 1. Del mismo modo $a_{0,0} = a_{-1,0} = 1$. Alrededor de $\left(-2+\frac{1}{2}, 1+\frac{1}{2}\right)$ la curva también da una vuelta, pero en sentido horario. Por lo tanto $a_{-2,1} = -1$.

Ejemplo 3. Tomemos ahora $w = c^2 = (xyx^{-1}y^{-1})^2$. En este caso la curva da dos vueltas alrededor de $\left(\frac{1}{2}, \frac{1}{2}\right)$, como se ve en Fig. 3.

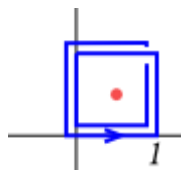

Fig. 3. La curva γ_w de Ejemplo 3.

Luego $a_{0,0} = 2$.

Un polinomio con coeficientes enteros en una variable es una suma formal $a_0 + a_1X + a_2X^2 + \ldots + a_nX^n = \sum a_iX^i$ donde los coeficientes a_i son números enteros. Un polinomio en dos variables es una suma del tipo $\sum a_{i,j}X^iY^j$ de enteros multiplicados por potencias no negativas de X y de Y. Un polinomio de Laurent en dos variables con coeficientes enteros es una suma como la anterior en donde se admiten también potencias negativas. El número $a_{i,j}$ es el coeficiente de (el monomio) X^iY^j.

Los polinomios de Laurent se pueden sumar y multiplicar, del mismo modo que uno hace con los polinomios usuales. Además, dado un polinomio de Laurent P en dos variables con coeficientes enteros, se puede evaluar en cualquier par de números enteros no nulos (n, m) simplemente reemplazando X por n e Y por m. El número $P(n, m)$ resultante es obviamente entero.

Definición 4. Dada $w \in F_2'$, definimos el *winding invariant* de w como el polinomio de Laurent en dos variables $P_w = \sum a_{i,j}X^iY^j$, donde los coeficientes $a_{i,j}$ son los definidos en Definición 1.

En Ejemplo 2 hay sólo cuatro coeficientes $a_{i,j}$ no nulos y el winding invariant de w es $P_w = 1 + X + X^{-1} - X^{-2}Y$. En Ejemplo 3 hay un único coeficiente no nulo y $P_w = 2$. El winding invariant de c es simplemente $P_c = 1$.

Una propiedad simple pero importante que cumple el winding invariant es la siguiente.

Observación 5. Si u y v son dos palabras en F_2', entonces $P_{uv} = P_u + P_v$. Esto se desprende directamente del hecho de que la curva γ_w es la concatenación de γ_u y γ_v. Luego, el coeficiente $a_{i,j}$ de X^iY^j en P_{uv} es la suma del coeficiente de X^iY^j en P_u y el coeficiente de X^iY^j en P_v.

Otra propiedad elemental que necesitaremos es la siguiente.

Proposición 6. Sea $w \in F_2'$ y sea $u \in F_2$. Sean $n = exp(x,u)$ y $m = exp(y,u)$. Entonces el winding invariant de uwu^{-1} es $P_{uwu^{-1}} = X^nY^mP_w$.

Demostración. La curva $\gamma_{uwu^{-1}}$ es una concatenación de tres curvas. La primera de esas curvas es γ_u. La segunda es la curva γ_w pero recorrida no desde el origen, sino comenzando en el final de la curva γ_u (ver Fig. 4). Es decir que es la curva γ_w trasladada según el vector (n, m). Como $w \in F_2'$, esta segunda curva termina en el mismo punto (n, m). Finalmente, la tercera curva en la concatenación es γ_u recorrida en dirección opuesta.

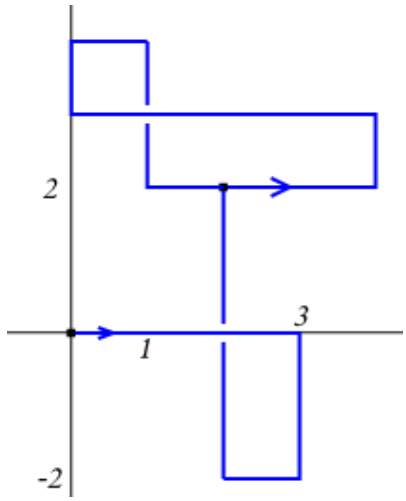

Fig. 4. La curva $\gamma_{uwu^{-1}}$ donde $u = x^3y^{-2}x^{-1}y^4$ es la palabra considerada en Fig. 1 y $w = x^2yx^{-4}yxy^{-2}x$ es la palabra de Ejemplo 2. El winding invariant de uwu^{-1} es $P_{uwu^{-1}} = X^2Y^2(1 + X + X^{-1} - X^{-2}Y) = X^2Y^2 + X^3Y^2 + XY^2 - Y^3$.

Luego los winding numbers que calculemos para la cuva $\gamma_{uwu^{-1}}$ van a ser los mismos que para la curva γ_w, sólo que van a estar desplazados (n, m). Concretamente, si $a_{i,j}$ es el coeficiente del monomio X^iY^j en P_w, entonces $a_{i,j}$ aparecerá en $P_{uwu^{-1}}$ pero como coeficiente de $X^{i+n}Y^{j+m}$. Esto demuestra el resultado.

Con estas herramientas elementales ya estamos listos para dar una demostración del resultado de Lyndon y Newman.

Proposición 7. (Lyndon-Newman). La palabra $c = xyx^{-1}y^{-1} \in F_2$ no es un producto de dos cuadrados.

Demostración. Supongamos que existen $u, v \in F_2$ tales que $c = u^2v^2$. Notemos que $u^2v^2 = (uv)v^{-1}(uv)v$. Como la palabras v^{-1} y v tienen las mismas letras pero con los exponentes opuestos, $exp(x,c) = exp(x,u^2v^2) = 2exp(x,uv)$. Pero el exponente de x en c es 0. Entonces $exp(x,uv) = 0$. Del mismo modo $exp(y,uv) = 0$, lo que prueba que $uv \in F_2{}'$. Por Observación 5, vale $P_c = P_{uv} + P_{v^{-1}(uv)v}$, y por Proposición 6, $P_{v^{-1}(uv)v} = X^nY^mP_{uv}$ para ciertos enteros n, m. Tenemos entonces $P_c = (1 + X^nY^m)P_{uv}$. Por otro lado, recordemos que $P_c = 1$. En la igualdad $1 = (1 + X^nY^m)P_{uv}$ podemos evaluar en el punto $(1,1)$ para obtener $1 = 2P_{uv}(1,1)$. Pero esto es absurdo pues 1 no es un número par.

En [2, 3] investigamos generalizaciones de la pregunta de Lyndon y Newman. Es fácil ver que una palabra w es producto de cuadrados si y sólo si los exponentes de x e y son ambos pares. Pero en ese caso, cuál es la mínima cantidad de cuadrados cuyo producto es w? Qué ocurre si reemplazamos cuadrados por cubos, o potencias cuartas? Este problema está directamente relacionado con los grupos de Burnside, que son aquellos que cumplen la relación w^n para toda

palabra w y un exponente n fijo. Otras aplicaciones del winding invariant exploradas en [1] están relacionadas con la conjetura de Andrews-Curtis, que estudia deformaciones combinatorias de presentaciones de grupos. Estas aplicaciones exceden los objetivos de la presente nota y el lector interesado queda invitado a consultar las referencias.

Referencias

[1] J.A. Barmak. *A counterexample to a strong version of the Andrews-Curtis conjecture*. ArXiv:1806.11493.
[2] J.A. Barmak. *The winding invariant*. ArXiv:1904.10072.
[3] J.A. Barmak. *Invariants for metabelian groups of prime power exponent, colorings and stairs*. ArXiv:2003.04392.
[4] E.I. Khukhro, V.D. Mazurov (Eds). Unsolved Problems in Group Theory, The Kourovka Notebook, No. 19. Institute of Mathematics SO RAN, Novosibirsk (2018); http://math.nsc.ru/~alglog/19tkt.pdf
[5] R.C. Lyndon, M.F. Newman, *Proc. Amer. Math. Soc.* **39**, 267 (1973).
[6] M.J. Wicks. The equation $x^2y^2 = g$over free products. In Proc. of the *Second Congress of the Singapore National Academy of Science* **1973**, 238-248.

Manuscrito recibido el 19 de marzo de 2020.
Aceptado el 27 de marzo de 2020.