Facultad de Ciencias

Sobre la homología de grupos de gérmenes de difeomorfismos formales

Tesis

entregada a la Universidad de Chile
en cumplimiento parcial de los requisitos
para optar al grado de

Magíster en Ciencias Matemáticas

por
Javier Pavez
Abril, 2024

Director de Tesis: Dr. Cristóbal Rivas
Co-director de Tesis: Dr. Andrés Navas

Mi nombre es Javier Pavez. Desde que tengo memoria me ha caracterizado la curiosidad, lo cual me ha llevado a desarrollar una fascinación con un amplio elenco de disciplinas e intereses. Por mencionar algunos: la música, la historia, las ciencias naturales y por supuesto, las matemáticas.

Luego de un mediocre inicio persiguiendo la física, me encontré con las matemáticas de una forma en la que nunca había tenido oportunidad de experimentar. Esto me llevó a saltar al programa de matemáticas, decisión de la que no me he arrepentido, y sospecho que nunca lo haré.

Agradecimientos

Agradezco a mis padres, Jorge y Eliana, quienes me han brindado inconmensurable apoyo a lo largo de mi vida. A mis amigos, quienes me han acompañado en penas y alegrías. A los pedagogos y docentes que, en distintas etapas de mi vida, me han nutrido no solo de conocimientos, si no también de practicas, perspectivas y filosofías. En particular al Dr. Luis Arenas, cuyos comentarios y correcciones fueron de gran ayuda para enderezar esta tesis. A mis tutores, por su paciencia y asistencia convirtiendo el caos de mis pensamientos en ideas matemáticas. A mi más cercano compañero, Chester, cuya constante presencia, ánimos y entendimiento han sido indispensables en los catorce años que lleva a mi lado. Y por último, agradezco el poder agradecer tanto.

Resumen

En esta tesis se calcularon las abelianizaciones de los grupos de series de potencias formales con coeficientes enteros $\mathcal{J}_k(\mathbb{Z})$, para $k \geqslant 5$. Esto se logro calculando directamente clases de equivalencia en las correspondientes abelianizaciones, a diferencia de el trabajo de I. K. Babenko y S. A. Bogatyy en [1], en donde los autores dan un morfismo explicito para calcular el caso de $k = 2$. Se espera que los casos restantes puedan ser abarcados directamente por métodos similares a los de esta tesis.

Abstract

In this thesis we compute the abelianization of the formal power series group with integer coeficients $\mathcal{J}_k(\mathbb{Z})$, for $k \geqslant 5$. This was accomplished by dealing directly with the equivalence classes in the corresponding abelianizations, in contrast with the work of I. K. Babenko and S. A. Bogatyy in [1], where the authors give an explcit abelianization morphism for the case $k = 2$. We expect to be able to compute the remaining abelianizations by applying methods similar to those employed in this thesis.

Índice general

Capítulo 1

Introducción

Sea R un anillo conmutativo. Se define su anillo de series de potencias formales como

$$R[[x]] := \left\{ \sum_{i \geqslant 0} \alpha_i x^i \middle| \alpha_i \in R,\ \forall i \in \mathbb{N}_0 \right\},$$

con la suma definida por la suma coeficiente a coeficiente y el producto definido por

$$\begin{aligned} \cdot : R[[x]] \times R[[x]] &\to R[[x]] \\ \left(\sum_{i \geqslant 0} \alpha_i x^i, \sum_{i \geqslant 0} \beta_i x^i \right) &\mapsto \sum_{i \geqslant 0} \left(\sum_{j=0}^{i} \alpha_j \beta_{i-j} \right) x^i. \end{aligned}$$

Notemos que $x^t \cdot x^s = x^{t+s}$ para todo $s, t \in \mathbb{N}_0$, y que por tanto x^0 es la identidad en este anillo.

Por distintas y variadas razones las series de potencias son objetos muy estudiados en diversas áreas de la matemática. En particular cuando R es un espacio topológico, pues podremos definir la evaluación de una serie de potencias $f = \sum_{i \geqslant 0} \alpha_i x^i$ en un elemento $a \in R$ como

$$f(a) := \lim_{N \to \infty} \sum_{i=0}^{N} \alpha_i a^i.$$

cuando tal límite existe. Ejemplos de esto ocurren cuando consideramos R como el cuerpo de números reales $\mathbb{R}$ o el cuerpo de números complejos $\mathbb{C}$

con sus topologías usuales. Estos dos ejemplos son notables por sus fuertes relaciones con el análisis real y complejo, respectivamente. Si bien no siempre estará bien definido, esto nos incita a pensar en los elementos de $R[[x]]$ como funciones de R en sí mismo, pero sujetas a las topología de R, pues claramente no siempre tiene sentido evaluar en un elemento arbitrario de R. Así mismo, pensando en las series de potencias como funciones, podemos preguntarnos qué ocurre al componer una serie de potencias formal con otra. Al igual que antes, esto no siempre tiene sentido, pero un caso notable en el que sí lo tiene es cuando nos restringimos a

$$xR[[x]] := \left\{ \sum_{i \geqslant 0} \alpha_i x^i \in R[[x]] \middle| \alpha_0 = 0 \right\}.$$

Notemos que $xR[[x]]$ es un subanillo de $R[[x]]$. Esto define una nueva operación:

$$\begin{aligned} \circ : xR[[x]] \times xR[[x]] &\to xR[[x]] \\ \left(\sum_{i \geqslant 1} \alpha_i x^i, \sum_{i \geqslant 1} \beta_i x^i \right) &\mapsto \sum_{i \geqslant 1} \alpha_i \left(\sum_{j \geqslant 1} \beta_j x^j \right)^i, \end{aligned}$$

en donde $\left(\sum_{j \geqslant 1} \beta_j x^j \right)^i$ corresponde a la $i-$ésima potencia de $\sum_{j \geqslant 1} \beta_j x^j$ respecto al producto del anillo $R[[x]]$. El hecho de que esta operación está bien definida se encuentra demostrado como la proposición 4.1 en el apéndice al final de esta tesis.

No es difícil darse cuenta de que esta operación es asociativa y que $f \circ x = f = x \circ f$ para todo $f \in xR[[x]]$. De esta manera, es natural preguntarse por la invertibilidad de un elemento respecto a esta operación. La respuesta es sorprendentemente sencilla: basta con que el coeficiente lineal sea invertible para que la serie de potencias lo sea. Este hecho se encuentra demostrado como la proposición 4.3 del apéndice. De esta manera, tendremos que

$$\widetilde{\mathcal{J}(R)} := \left\{ \sum_{i \geqslant 1} \alpha_i x^i \in xR[[x]] \middle| \alpha_1 \in R^* \right\}$$

es un grupo bajo la composición.

Podemos definir

$$\mathcal{J}(R) := \left\{ f \in \widetilde{\mathcal{J}(R)} \middle| f = x + \sum_{i \geqslant 2} \alpha_i x^i \right\}.$$

Este es es un subgrupo normal de $\widetilde{\mathcal{J}(R)}$ y el cociente $\widetilde{\mathcal{J}(R)}/\mathcal{J}(R)$ es isomorfo a R^*. Es así como, en cierto sentido, se puede decir que el grupo $\mathcal{J}(R)$ concentra buena parte de la información de $\widetilde{\mathcal{J}(R)}$.
Sea $k \geqslant 2$. Dentro de $\mathcal{J}(R)$ podremos encontrar el subgrupo

$$\mathcal{J}_k(R) := \left\{ f \in \mathcal{J}(R) \middle| f = x + \sum_{i \geqslant k} \alpha_i x^i \right\}.$$

Estos serán los grupos en los que trabajaremos, y nos familiarizaremos con ellos más adelante.

El grupo $\mathcal{J}(R)$ tiene una estructura natural de grupo topológico. La definición de grupo topológico, junto con ciertos resultados que usaremos más adelante se encuentran desarrollados en el apéndice de esta tesis. Para hacer evidente dicha estructura, tenemos que partir desde R. Diremos que un anillo R es un anillo topológico si R es un espacio topológico y tanto la suma como el producto son funciones continuas. Si R no tiene una topología se le puede dar la topología discreta, lo cual lo vuelve un anillo topológico. De esta manera podremos darle una topología a $R[[x]]$. Para esto basta identificar este anillo con $R^{\mathbb{N}}$ como conjuntos de la forma natural. Luego, se puede dotar a $R^{\mathbb{N}}$ con la topología producto, es decir, la convergencia viene dada coordenada a coordenada. Dado que identificamos $R^{\mathbb{N}}$ con $R[[x]]$, podemos dotar a este ultimo con la misma topología. Notemos que la suma en $R[[x]]$ está definida como la suma en R coeficiente a coeficiente, mientras que el producto es, coeficiente a coeficiente, una suma finita de productos de R. Esto implica que $R[[x]]$ con la topología producto es un anillo topológico, Así mismo, siendo un subconjunto de $R[[x]]$, podremos dotar a $\mathcal{J}(R)$ con la topología de subespacio. Esto lo vuelve un grupo topológico, pues la operación de composición se determina por sumas y productos en $R[[x]]$.

Por suerte para nosotros y como podría sugerir la notación, no somos los primeros interesados en objetos de este tipo. Si bien el estudio de grupos de series de potencias se remonta a los trabajos de S. Bochner y W.T. Martin en [2] y M. Gôto en [3], es en el trabajo de S. A. Jennings en [4] en donde por primera vez se define y demuestra que $\mathcal{J}(R)$ es un grupo topológico bajo la composición, pero no necesariamente con la misma topología que hemos definido nosotros. Notablemente, los primeros dos trabajos consideran series de potencias en varias variables sobre $\mathbb{C}$ y sobre un cuerpo arbitrario respectivamente, mientras que Jennings considera series de potencias formales sobre un anillo conmutativo cualquiera en una sola variable. Esto le permitió establecer varios resultados básicos, razón por la cual este tipo de grupo suele ser llamado grupo de Jennings en la literatura. Uno de dichos resultados es el siguiente

Proposition 1.1. *El grupo* $[\mathcal{J}_k(R), \mathcal{J}_k(R)]$ *esta contenido en* $\mathcal{J}_{2k}(R)$.

A finales de la década de los 80 y principios de la de los 90, los grupos de Jennings recibieron gran atención para los casos en que R es un cuerpo finito (situación en la que son llamados grupos de Nottingham) por su fuerte relación con la teoría de Galois y la teoría de pro $p-$grupos, como puede ser evidenciado en [5], donde R. Camina demuestra que todo pro $p-$grupo con base contable está contenido en $\mathcal{J}(\mathbb{F}_p)$. En esta tesis nos concentraremos en el caso de $\mathcal{J}(\mathbb{Z})$, que a diferencia de los grupos de Nottingham, no es localmente compacto, pues es topológicamente equivalente a $\mathbb{Z}^{\mathbb{N}}$. Esto nos impide usar resultados derivados de la medida de Haar, por lo que tendremos que buscar un acercamiento alternativo para entender que ocurre en este grupo. En el trabajo de I. K. Babenko y S. A. Bogatyy en [1], entre varios otros resultados, los autores demuestran que la abelianización de $\mathcal{J}(\mathbb{Z})$ es isomorfa a $\mathbb{Z}^2 \bigoplus (\mathbb{Z}/2\mathbb{Z})^2$. Concretamente, demostraron que la función

$$\varphi : \mathcal{J}(\mathbb{Z}) \to \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

$$x + \sum_{i \geqslant 2} \alpha_i x^i \mapsto \left(\alpha_2, \alpha_3 - {\alpha_2}^2, \alpha_4 + \alpha_5 + \frac{\alpha_3(\alpha_3+1)}{2} \pmod 2, \alpha_7 + \alpha_5(\alpha_3+1) \pmod 2 \right)$$

es un morfismo sobreyectivo cuyo núcleo es $[\mathcal{J}(\mathbb{Z}), \mathcal{J}(\mathbb{Z})]$.

Tomando inspiración en este resultado, dedicaremos esta tesis a calcular las abelianizaciones de los grupos $\mathcal{J}_k(\mathbb{Z})$, pues veremos que esto nos ofrecerá nuevas intuiciones sobre el producto en estos grupos, cosa que es valiosa, pues determinar la composición de dos series de potencias formales como una serie de potencias formal no es una tarea fácil.
A diferencia del resultado de I.K. Babenko y S.A. Bogatyy, nosotros no daremos un morfismo explícito, si no que calcularemos directamente las clases en $H_1(\mathcal{J}_k(\mathbb{Z}))$. Para hacer esto posible usaremos algunas de las técnicas que los autores mencionados usaron. Entre estas, la más importante será demostrar

que dado $k \geqslant 2$, existe $c_k > k$ tal que $\mathcal{J}_{c_k}(\mathbb{Z}) \subset [\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$. Esto nos da una forma sencilla de verificar cuándo un elemento de $\mathcal{J}_k(\mathbb{Z})$ se encuentra en el grupo derivado, y a través de esto determinar varias propiedades de las clases en $H_1(\mathcal{J}_k(\mathbb{Z}))$. También nos permitirá olvidar la topología de $\mathcal{J}_k(\mathbb{Z})$, lo que aliviará en gran medida los cálculos que haremos.

Nuestro teorema principal es el siguiente:

Theorem 1.2. *Sea $k \geqslant 5$.*
Si $k \equiv 3 \pmod 4$, entonces

$$H_1(\mathcal{J}_k(\mathbb{Z})) \cong \mathbb{Z}^k \bigoplus (\mathbb{Z}/2\mathbb{Z})^{\frac{k+1}{2}}$$

Si $k \equiv 2 \pmod 4$, entonces

$$H_1(\mathcal{J}_k(\mathbb{Z})) \cong \mathbb{Z}^k \bigoplus (\mathbb{Z}/2\mathbb{Z})^{\frac{k+2}{2}}$$

Si $k \equiv 1 \pmod 4$, entonces

$$H_1(\mathcal{J}_k(\mathbb{Z})) \cong \mathbb{Z}^k \bigoplus \mathbb{Z}/4\mathbb{Z} \bigoplus (\mathbb{Z}/2\mathbb{Z})^{\frac{k-3}{2}}$$

Si $k \equiv 0 \pmod 4$, entonces

$$H_1(\mathcal{J}_k(\mathbb{Z})) \cong \mathbb{Z}^k \bigoplus \mathbb{Z}/4\mathbb{Z} \bigoplus (\mathbb{Z}/2\mathbb{Z})^{\frac{k-2}{2}}$$

Si bien el enunciado es para $k \geqslant 5$, de todas formas la gran mayoría de los resultados serán enunciados para $k \geqslant 2$, pues es solo al final y por unos detalles técnicos que se impone esta restricción. Los casos restantes no pudieron ser abordados en esta tesis por restricciones temporales, pero se espera que no presenten nuevas dificultades más allá del tedio que sea calcularlas directamente.

Capítulo 2

Preliminares

2.1 Grupo de Jenninngs

Antes de dar nuevos resultados, nos familiarizaremos con el grupo de Jennings.

No es precisamente sencillo determinar los coeficientes de $f \circ g$ para todo $f, g \in \mathcal{J}(\mathbb{Z})$. Por suerte para nosotros, existen fórmulas que nos permiten estimar los primeros coeficientes de $f \circ g$ y $[f, g]$.

Proposition 2.1. *Sean $f = x + \alpha_m x^m + \alpha_{m+s} x^{m+s} + \cdots$ y $g = x + \beta_n x^n + \beta_{n+r} x^{n+r} + \cdots$ elementos de $\mathcal{J}(\mathbb{Z})$. Sean $t = \text{mín}\{s, r, n-1\}$ y*

$$\gamma_1 = \begin{cases} (m+s)\alpha_{m+s}\beta_n & si\ t = s \\ 0 & si\ t \neq s \end{cases}, \gamma_2 = \begin{cases} m\alpha_m\beta_{n+r} & si\ t = r \\ 0 & si\ t \neq r \end{cases}, \gamma_3 = \begin{cases} \binom{m}{2}\alpha_m{\beta_n}^2 & si\ t = n-1 \\ 0 & si\ t \neq n-1 \end{cases}$$

Se tiene que:

1) *$f \circ g = f + g - x + m\alpha_m\beta_n x^{m+n-1} + (\gamma_1 + \gamma_2 + \gamma_3)x^{m+n+t-1} + R_{f,g}$, donde $R_{f,g} \in x^{m+n+t}\mathbb{Z}[[x]]$.*

2) *Si $m > n$ y $r > s > n$, entonces*

$$[f, g] = x + (m-n)\alpha_m\beta_n x^{m+n-1} + C(m, n)\alpha_m\beta_n^2 x^{m+2(n-1)} + \cdots$$

Donde $C(m, n) = \binom{m}{2} - (m-n)(m+n-1)$.

Demostración.

1) Ver la proposición 2.3 de [1].

2) Vemos que

$$
\begin{aligned}
f \circ g - g \circ f =&(m-n)\alpha_m\beta_n x^{m+n-1} + \binom{m}{2}\alpha_m{\beta_n}^2 x^{m+2(n-1)} + \cdots \\
\Leftrightarrow [f,g] - x = (f \circ g - g \circ f) \circ (g \circ f)^{-1} =&(m-n)\alpha_m\beta_n x^{m+n-1} + C\alpha_m{\beta_n}^2 x^{m+2(n-1)} + \cdots .
\end{aligned}
$$

Por otro lado, tenemos que

$$
\begin{aligned}
[f,g] \circ (g \circ f) =&g \circ f + (m-n)\alpha_m\beta_n (g \circ f)^{m+n-1} + C\alpha_m{\beta_n}^2 (g \circ f) + \cdots \\
=&g + f - x + n\beta_n\alpha_m x^{m+n-1} \\
&+ (m-n)\alpha_m\beta_n (x + \beta_n x^n + \cdots)^{m+n-1} + C\alpha_m{\beta_n}^2 (x + \cdots) + \cdots \\
=&g + f - x + ((n + (m-n)\alpha_m)\beta_n) x^{m+n-1} \\
&+ ((m+n-1)(m-n) + C)\alpha_m{\beta_n}^2 x^{m+2(n-1)} + \cdots .
\end{aligned}
$$

Dado que $[f,g] \circ g \circ f = f \circ g$, podemos igualar coeficiente a coeficiente para ver que

$$\binom{m}{2} = C + (m-n)(m+n-1),$$

de donde se obtiene que C depende solo de m y n, y que es igual a $\binom{m}{2} - (m-n)(m+n-1)$.

$\square$

En algunas ocasiones simplificaremos aún más la formula para $f \circ g$ y escribiremos

$$f \circ g = f + g - x + R$$

con $R \in x^{m+n-1}\mathbb{Z}[[x]]$.
Cabe mencionar que el $l-$esimo coeficiente de $R_{f,g}$ es un polinomio de varias variables evaluado en $\{\alpha_i\}_{i=m}^{l-1}$ y $\{\beta_i\}_{i=n}^{l-1}$.

Un concepto que nos ayudará a evidenciar varias situaciones y cumplirá un rol similar al del grado en los polinomios es el siguiente:

Definition 2.2. Sea $f = x + \sum_{i \geqslant 2} \alpha_i x^i \in \mathcal{J}(\mathbb{Z}) \setminus \{x\}$. Llamaremos nivel de f a

$$nvl(f) := \text{mín}\{i \geqslant 2 | \alpha_i \neq 0\}.$$

Para la identidad se define $nvl(x) = \infty$.
Dicho en palabras, el nivel de un elemento de $\mathcal{J}(\mathbb{Z})$ será la potencia con coeficiente no nulo más pequeña.

Gracias a la proposición 2.1 podemos deducir lo siguiente

Corollary 2.3. *Sean $f, g \in \mathcal{J}(\mathbb{Z})$. Se cumple que:*

a) $nvl(f \circ g) \geqslant \text{mín}\{nvl(f), nvl(g)\}$.

b) $nvl(f^{-1}) = nvl(f)$ *y* $f^{-1} = 2x - f + R$, *con* $R \in x^{2nvl(f)-1}\mathbb{Z}[[x]]$.

c) $nvl(f^l) = nvl(f)$ *y* $f^l = lf - (l-1)x + R_l$, *con* $R_l \in x^{2nvl(f)-1}\mathbb{Z}[[x]]$ *para todo* $l \in \mathbb{Z}^+$.

d) $nvl([f, g]) \geqslant nvl(f) + nvl(g) - 1$.

Demostración. Sean $f, g \in \mathcal{J}(\mathbb{Z})$. Si $g = x$, entonces *a)* y *d)* se cumplen trivialmente. Si $f = x$, entonces todas las propiedades se cumplen trivialmente. Asumiremos que $f \neq x \neq g$. Sean $m = nvl(f)$ y $n = nvl(g)$. Por definición tenemos que

$$f = x + \alpha_m x^m + \sum_{i \geqslant m+1} \alpha_i x^i,$$

$$g = x + \beta_n x^n + \sum_{i \geqslant n+1} \beta_i x^i$$

y $\alpha_m \neq 0 \neq \beta_n$.

a) Sabemos que

$$f \circ g = f + g - x + R$$

donde $R \in x^{m+n-1}\mathbb{Z}[[x]]$, es decir $R = \sum_{i \geqslant m+n-1} \gamma_i x^i$. Reemplazando podemos reescribir:

$$f \circ g = x + \alpha_m x^m + \beta_n x^n + \sum_{i \geqslant m+1} \alpha_i x^i + \sum_{i \geqslant n+1} \beta_i x^i + \sum_{i \geqslant m+n-1} \gamma_i x^i$$

Siendo m y n mayores que 1, tenemos que $m+n-1 > \text{mín}\{m,n\}$. Así, es claro que $nvl(f\circ g) \geqslant \text{mín}\{m,n\}$, donde la desigualdad estricta se obtiene si y solo si $m=n$ y $\alpha_m = -\beta_n$.

b) Sabemos que $x = f\circ f^{-1}$ y $f\circ f^{-1} = f + f^{-1} - x + R$, donde $R \in x^{m+nvl(f^{-1})-1}\mathbb{Z}[[x]]$. Reemplazando vemos que

$$x = x + f + f^{-1} + R,$$

de donde es claro que

$$f^{-1} = 2x - f - R = x + (-\alpha_m)x^m + \sum_{i\geqslant m+1}(-\alpha_i)x^i - R$$

Siendo $nvl(f^{-1}) \geqslant 2$, tenemos que $m + nvl(f^{-1}) - 1 > m$. De esta manera vemos que $nvl(f^{-1}) = m$.

c) Basta hacer inducción sobre l. El caso base es trivial. Para el paso inductivo, basta notar que

$$f^{l+1} = f^l\circ f = f^l + f - x + R = lf - (l-1)x + f - x + R_l + R = (l+1)f - lx + R_{l+1},$$

donde $R_{l+1} := R + R_l$. Así, para todo $l \in \mathbb{Z}^+$ tendremos que para todo $i \geqslant m$ existen $\gamma_i \in \mathbb{Z}$ tales que

$$f^l = x + l\alpha_m x^m + \sum_{i\geqslant m+1}\gamma_i x^i,$$

de donde es claro que $nvl(f^l) = m$ para todo $l \in \mathbb{Z}^+$.

d) Sabemos que

$$[f,g] = x + (m-n)\alpha_m\beta_n x^{m+n-1} + \sum_{i\geqslant m+n}\gamma_i x^i$$

De donde es claro que si $m \neq n$, entonces $nvl([f,g]) = m+n-1$, mientras que si $m=n$, entonces $nvl([f,g]) > m+n-1$.

$\square$

Esto nos permite reescribir

$$\mathcal{J}_k(\mathbb{Z}) = \{f \in \mathcal{J}(\mathbb{Z}) | nvl(f) \geqslant k\}^1.$$

En particular $\mathcal{J}_2(\mathbb{Z}) = \mathcal{J}(\mathbb{Z})$. Con esta notación es fácil demostrar lo siguiente:

Proposition 2.4. *Sea $k \geqslant 2$. Entonces $\mathcal{J}_k(\mathbb{Z}) \trianglelefteq \mathcal{J}(\mathbb{Z})$.*

Demostración. Sea $k \geqslant 2$ fijo. Primero, dado que $\infty > k$, tendremos que $x \in \mathcal{J}_k(\mathbb{Z})$. Por otro lado, sean $f, g \in \mathcal{J}_k(\mathbb{Z})$. Por definición $\text{mín}\{nvl(f), nvl(g)\} \geqslant k$. Vemos que

$$nvl(f \circ g^{-1}) \geqslant \text{mín}\{nvl(f), nvl(g^{-1})\} = \text{mín}\{nvl(f), nvl(g)\} \geqslant k.$$

Esto demuestra que $\mathcal{J}_k(\mathbb{Z}) \leq \mathcal{J}(\mathbb{Z})$.
Finalmente, sean $f \in \mathcal{J}(\mathbb{Z})$ y $g \in \mathcal{J}_k(\mathbb{Z})$. Notemos que $f \circ g \circ f^{-1} = [f, g] \circ g$. De esta manera, tenemos que

$$nvl(f \circ g \circ f^{-1}) = nvl([f, g] \circ g) \geqslant \text{mín}\{nvl([f, g]), nvl(g)\}$$

Dado que $nvl(f) > 1$, vemos que $nvl([f, g]) \geqslant nvl(f) + nvl(g) - 1 > nvl(g)$. Es decir

$$\text{mín}\{nvl([f, g]), nvl(g)\} = nvl(g) \geqslant k,$$

y por lo tanto $nvl(f \circ g \circ f^{-1}) \geqslant k$. Concluimos que $f \circ g \circ f^{-1} \in \mathcal{J}_k(\mathbb{Z})$, y así mismo, que $\mathcal{J}_k(\mathbb{Z}) \trianglelefteq \mathcal{J}(\mathbb{Z})$. □

De hecho podemos demostrar algo un poco más fuerte

Corollary 2.5. *Sea $k \geqslant 2$. Se cumple que $l \geqslant k$ si y solo si $\mathcal{J}_l(\mathbb{Z}) \trianglelefteq \mathcal{J}_k(\mathbb{Z})$.*

Demostración. Sea $k \geqslant 2$ fijo. Vemos que si $l \geqslant k$, entonces por definición $\mathcal{J}_l(\mathbb{Z}) \subseteq \mathcal{J}_k(\mathbb{Z})$, por lo que $\mathcal{J}_l(\mathbb{Z}) \cap \mathcal{J}_k(\mathbb{Z}) = \mathcal{J}_l(\mathbb{Z})$. Más aun, vemos que $\mathcal{J}_l(\mathbb{Z}) \leqslant \mathcal{J}(\mathbb{Z})$ implica que

$$\mathcal{J}_l(\mathbb{Z}) \bigcap \mathcal{J}_k(\mathbb{Z}) \leq \mathcal{J}_k(\mathbb{Z}) \bigcap \mathcal{J}(\mathbb{Z}),$$

[1] En la literatura los grupos $\mathcal{J}_k(R)$ se suelen indexar con $k - 1$, a diferencia de como lo hemos hecho aquí. El motivo de no seguir la notación usual es ligeramente más profundo que simple estética, como veremos a lo largo de la tesis. De todas formas, la matemática subyacente a todo esto no cambia, pues bastará hacer los traslados correspondientes si se desease adecuar a la indexación usual.

y siendo $\mathcal{J}_k(\mathbb{Z}) \cap \mathcal{J}(\mathbb{Z}) = \mathcal{J}_k(\mathbb{Z})$, tendremos que $\mathcal{J}_l(\mathbb{Z}) \leq \mathcal{J}_k(\mathbb{Z})$.
Por otro lado, vemos que $f\mathcal{J}_l(\mathbb{Z})f^{-1} \subset \mathcal{J}_l(\mathbb{Z})$ para todo $f \in \mathcal{J}(\mathbb{Z})$, así que en particular $f\mathcal{J}_l(\mathbb{Z})f^{-1} \subset \mathcal{J}_l(\mathbb{Z})$ para todo $f \in \mathcal{J}_k(\mathbb{Z})$. Con esto concluimos que $\mathcal{J}_l(\mathbb{Z}) \trianglelefteq \mathcal{J}_k(\mathbb{Z})$.
Por ultimo, si $\mathcal{J}_l(\mathbb{Z}) \trianglelefteq \mathcal{J}_k(\mathbb{Z})$, entonces en particular $\mathcal{J}_l(\mathbb{Z}) \subseteq \mathcal{J}_k(\mathbb{Z})$. Por definición $x + x^l \in \mathcal{J}_l(\mathbb{Z})$, así que en particular $x + x^l \in \mathcal{J}_k(\mathbb{Z})$. Es decir $l \geqslant k$. □

Sean $k \geqslant 2$ y $l \geqslant k$, escribiremos $\mathcal{J}_k^l(\mathbb{Z})$ para referirnos a $\mathcal{J}_k(\mathbb{Z})/\mathcal{J}_l(\mathbb{Z})$.
Ver a $\mathcal{J}(\mathbb{Z})$ como grupo topológico puede ser difícil. Por suerte para nosotros, los subgrupos $\mathcal{J}_k(\mathbb{Z})$ nos permitirán ignorar en gran medida esta topología. Primero, vemos que cumplen una propiedad topológica bastante interesante.

Proposition 2.6. *Sea $k \geqslant 2$. El subgrupo $\mathcal{J}_k(\mathbb{Z})$ es abierto y cerrado en $\mathcal{J}(\mathbb{Z})$.*

Demostración. Fijaremos $k \geqslant 2$. Recordemos que la topología de $\mathbb{Z}[[x]]$ es la que se obtiene al identificarlo con $\mathbb{Z}^{\mathbb{N}}$ por medio de la función

$$\begin{aligned} \varphi : \mathbb{Z}[[x]] &\to \mathbb{Z}^{\mathbb{N}} \\ \sum_{i \geqslant 0} \alpha_i x^i &\mapsto (\alpha_{i-1})_{i \in \mathbb{Z}^+}. \end{aligned}$$

Bajo esta identificación, tendremos que

$$\varphi(\mathcal{J}_k(\mathbb{Z})) = \{(x_i) \in \mathbb{Z}^{\mathbb{N}} | x_1 = 0, x_2 = 1, x_i = 0 \text{ si } 3 \leqslant i \leqslant k-1\}.$$

Por otro lado, consideremos la proyección

$$\begin{aligned} p_{k-1} : \mathbb{Z}^{\mathbb{N}} &\to \mathbb{Z}^{k-1} \\ (x_i)_{i \in \mathbb{Z}^+} &\mapsto (x_1, \ldots, x_{k-1}). \end{aligned}$$

Sabemos que es continua por definición de $\mathbb{Z}^{\mathbb{N}}$. De esta manera, siendo $\mathbb{Z}^{k-1}$ discreto, tenemos que $\{(0, 1, 0 \ldots, 0)\}$ es abierto y cerrado. Por lo tanto

$$(p_{k-1})^{-1}((0, 1, 0, \ldots, 0)) = \{(x_i) \in \mathbb{Z}^{\mathbb{N}} | x_1 = 0, x_2 = 1, x_i = 0 \text{ si } 3 \leqslant i \leqslant k-1\}$$

es abierto y cerrado en $\mathbb{Z}^{\mathbb{N}}$. Esto implica que $\mathcal{J}_k(\mathbb{Z})$ es abierto y cerrado en $\mathbb{Z}[[x]]$.
Finalmente, dado que $\mathcal{J}_k(\mathbb{Z}) \cap \mathcal{J}(\mathbb{Z}) = \mathcal{J}_k(\mathbb{Z})$, tendremos que esto implica que $\mathcal{J}_k(\mathbb{Z})$ es abierto y cerrado en $\mathcal{J}(\mathbb{Z})$. □

Esto tiene dos consecuencias importantes, que serán las que permitirán las simplificaciones mencionadas. La primera requiere definir un poco de notación.

- *Para todo* $n \geqslant 2$ *se define el elemento* $f_n := x + x^n$ *en* $\mathcal{J}(\mathbb{Z})$.
- *Sea* S *un subconjunto de un espacio topológico. Escribiremos* $\overline{S}$ *para denotar a su clausura.*
- *Sea* S *un subconjunto de un grupo. Escribiremos* $\langle S \rangle$ *para denotar al subgrupo generado por* S.

Esto nos permite describir los subgrupos $\mathcal{J}_k(\mathbb{Z})$ *de una manera mucho más cómoda.*

Corollary 2.7. $\mathcal{J}_k(\mathbb{Z}) = \overline{\langle f_n | n \geqslant k \rangle}$

Demostración. Por un lado, es claro que $f_n \in \mathcal{J}_k(\mathbb{Z})$ para todo $n \geqslant k$. Esto implica que

$$\langle f_n | n \geqslant k \rangle \subset \mathcal{J}_k(\mathbb{Z}).$$

Dado que $\mathcal{J}_k(\mathbb{Z})$ es cerrado, esto implica que

$$\overline{\langle f_n | n \geqslant k \rangle} \subset \mathcal{J}_k(\mathbb{Z}).$$

Por otro lado, sea $g \in \mathcal{J}_k(\mathbb{Z})$, con $g = x + \sum_{i \geqslant k} \alpha_i x^i$. Definimos la siguiente sucesión

$$\begin{cases} g_i = (f_k)^{\alpha_k} & \text{para } i \leqslant k \\ g_i = g_{i-1} \circ (f_k)^{\alpha_i - \gamma_{i-1,i}} & \text{para } i > k \end{cases}$$

donde $\gamma_{i,l}$ es el $l-$esimo coeficiente de g_i. Vemos que $\lim g_n = g$. Esto implica que $g \in \overline{\langle f_n | n \geqslant k \rangle}$. Por lo tanto $\mathcal{J}_k(\mathbb{Z}) \subset \overline{\langle f_n | n \geqslant k \rangle}$. Concluimos que se verifica la igualdad. □

La segunda consecuencia es aún más directa

Corollary 2.8. *Sean* $k, l \in \mathbb{Z}^+$. *Si* $l > k \geqslant 2$, *entonces* $\mathcal{J}_k^l(\mathbb{Z})$ *es discreto.*

Demostración. Dado que $\mathcal{J}_l(\mathbb{Z})$ es abierto en $\mathcal{J}(\mathbb{Z})$, tendremos que $\mathcal{J}_l(\mathbb{Z}) = \mathcal{J}_l(\mathbb{Z}) \cap \mathcal{J}_k(\mathbb{Z})$ es abierto en $\mathcal{J}_k(\mathbb{Z})$. Esto es equivalente a que $\mathcal{J}_k^l(\mathbb{Z})$ sea discreto. □

Por esta razón trabajaremos con $\mathcal{J}_k^l(\mathbb{Z})$ siempre que podamos. Caracterizar los elementos de este cociente es relativamente natural como veremos en seguida.

Proposition 2.9. *Sean $k, l \in \mathbb{Z}^+$ tales que $l > k \geqslant 2$ y $p : \mathcal{J}_k(\mathbb{Z}) \to \mathcal{J}_k^l(\mathbb{Z})$ la proyección canónica. Sean $f, g \in \mathcal{J}_k(\mathbb{Z})$, con $f = x + \sum_{i \geqslant k} \alpha_i x^i$ y $g = x + \sum_{i \geqslant k} \beta_i x^i$. Entonces $p(f) = p(g)$ si y solo si $\alpha_i = \beta_i$ para todo $i \in \{k, \ldots, l-1\}$.*

Demostración. Por un lado, si $p(f) = p(g)$, entonces existe $h \in \mathcal{J}_l(\mathbb{Z})$ tal que

$$f = g \circ h = g + h - x + R,$$

donde $R \in x^{k+l-1}\mathbb{Z}[[x]]$. Esto implica que $f - g = h - x + R \in x^l\mathbb{Z}[[x]]$, de donde es claro que $\alpha_i = \beta_i$ para todo $i \in \{k, \ldots, l-1\}$.

Por otro lado, asumiremos que $\alpha_i = \beta_i$ para todo $i \in \{k, \ldots, l-1\}$. Demostraremos que $f^{-1} \circ g \in \mathcal{J}_l(\mathbb{Z})$. Sabemos que el $i-$esimo coeficiente de f^{-1} esta determinado por los coeficientes $\{\alpha_j\}_{j=k}^{i}$. De esta manera, tendremos que los coeficientes de f^{-1} y g^{-1} son iguales hasta el $(l-1)-$esimo coeficiente. Así podremos escribir $f^{-1} = g^{-1} + R$, donde $R \in x^l\mathbb{Z}[[x]]$. Evaluando tendremos que

$$f^{-1} \circ g = (g^{-1} + R) \circ g = (g^{-1} \circ g) + (R \circ g) = x + (R \circ g) \in \mathcal{J}_l(\mathbb{Z}).$$

□

Corollary 2.10. *Sean $k, l \in \mathbb{Z}^+$ tales que $l > k \geqslant 2$ y $p : \mathcal{J}_k(\mathbb{Z}) \to \mathcal{J}_k^l(\mathbb{Z})$ la proyección canónica. Sean $f, g \in \mathcal{J}_k(\mathbb{Z})$. Entonces $p(f) = p(g)$ si y solo si f y g son equivalentes en $\mathbb{Z}[[x]]/x^l\mathbb{Z}[[x]]$.*

Esto nos permite denotar la clase de $f = x + \sum_{i \geqslant k} \alpha_i x^i$ en $\mathcal{J}_k^l(\mathbb{Z})$ como $f + O(x^l)$ ó $x + \sum_{i=k}^{k-1} \alpha_i x^i + O(x^l)$, según sea conveniente, y calcular la clase de $f \circ g$ por medio de las operaciones de $\mathbb{Z}[[x]]/x^l\mathbb{Z}[[x]]$.

Con esto ya tenemos un entendimiento de nuestros grupos $\mathcal{J}_k(\mathbb{Z})$, que si bien es un tanto rudimentario, es un punto de partida que nos permitirá ahondar más respecto a la estructura de sus correspondientes abelianizaciones.

2.2 Lo que necesitaremos

En esta sección presentaremos un resultado que, si bien su demostración puede ser descrita como tediosa, cumplirá un rol central a lo largo de esta tesis.

La idea es la siguiente: Inspirados en el trabajo de I. K. Babenko y S. A. Bogatyy en [1], dado $k \geqslant 2$, buscaremos cotas $c \geqslant k$ tales que $\mathcal{J}_c(\mathbb{Z}) \subset [\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.

Recordemos que $\mathcal{J}_c(\mathbb{Z}) = \overline{\langle f_l | l \geqslant c \rangle}$. Así, para un $c \geqslant k$ dado, nuestro objetivo se traduce a demostrar que $f_l \in [\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$ para todo $l \geqslant c$. Verificar esto no es fácil, por lo que modificaremos ligeramente lo que queremos demostrar.

Proposition 2.11. *Sea $k \geqslant 2$. Si $c \geqslant k$, entonces se cumple que $f_l \in [\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$ para todo $l \geqslant c$ si y solo si para todo $l \geqslant c$, existe un elemento de la forma $x + x^l + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.*

Demostración. Notemos que f_l es en particular un elemento de la forma $x + x^l + \cdots$. Luego, si $f_l \in [\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$ para todo $l \geqslant c$, entonces en particular para todo $l \geqslant c$, existe un elemento de la forma $x + x^l + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.
Por otro lado, asumiremos que para todo $l \geqslant c$, existe un elemento de la forma $x + x^l + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$. Llamaremos g_i al elemento de la forma $x + x^i + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$. Sea $n \geqslant c$, demostraremos que f_n es un limite de productos de los elementos g_i. Definimos la siguiente sucesión:

$$h_i = \begin{cases} g_i & \text{si } i \leqslant n \\ h_{i-1} \circ (g_i)^{-\gamma_{i-1,i}} & \text{si } i > n \end{cases}$$

donde $\gamma_{i,l}$ es el $l-$esimo coeficiente de h_i. Es claro que $\lim h_i = f_n$. Esto implica que $f_n \in [\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$ para todo $n \geqslant c$. □

Lo anterior podría parecer un cambio meramente sintáctico, pero veremos que podemos encontrar elementos que cumplan esta propiedad en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.

Recordemos que, si $f = x + \alpha_m x^m + \alpha_{m+s} x^{m+s} + \cdots$ y $g = x + \beta_n x^n + \beta_{n+r} x^{n+r} + \cdots$ son elementos de $\mathcal{J}(\mathbb{Z})$ tales que $m > n$ y $r > s \geqslant n$, entonces

$$[f,g] = x + (m-n)\alpha_m\beta_n x^{m+n-1} + C(m,n)\alpha_m\beta_n^2 x^{m+2(n-1)} + \cdots .$$

Esto nos da inmediatamente la siguiente información:

Proposition 2.12. *Sea $k \geqslant 2$.*

a) *Para todo $l \geqslant k$ existe un elemento de la forma $x + x^{2l} + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.*

b) *Sean $l \geqslant k$, $\epsilon \in \{0,1\}$ y $\alpha \in \mathbb{Z}$ tal que $\alpha \equiv \epsilon \pmod 2$. Si existe un elemento de la forma $x + \alpha x^{2l+1} + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$, entonces existe un elemento de la forma $x + \epsilon x^{2l+1} + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.*

Demostración.

a) Basta notar que

$$[f_{l+1}, f_l] = x + x^{2l} + C(l+1,l)x^{3l-1} + \cdots$$

es un elemento de la forma $x + x^{2l} + \cdots$.

b) Por hipótesis tenemos que existe $n \in \mathbb{Z}$ tal que $\alpha = \epsilon + 2n$. Además, vemos que

$$[f_{l+2}, f_l] = x + 2x^{2l+1} + C(l+2,l)x^{3l} + \cdots .$$

De esta manera, tenemos que

$$(x + \alpha x^{2l+1} + \cdots) \circ [f_{l+2}, f_l]^{-n} = x + \epsilon x^{2l+1} + \cdots .$$

Siendo $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$ un grupo, esto implica lo deseado.

□

De la proposición anterior podemos notar que los elementos $[f_{l+1}, f_l]$ y $[f_{l+2}, f_l]$ jugarán un rol importante dentro de esta tesis, pues nos darán una forma sencilla de reducir elementos módulo conmutadores. Además, esto indica que si $c \geqslant k$ es tal que $\mathcal{J}_c(\mathbb{Z}) \subset [\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$, entonces $c \geqslant 2k$.
Es así como, dado $k \geqslant 2$, nuestro problema se reduce a determinar cuándo se cumple para $l \geqslant k$ que existe un producto de conmutadores de la forma $x + \alpha x^{2l+1} + \cdots$ con $\alpha \equiv 1 \pmod 2$. En lo que sigue de esta sección nos dedicaremos a fabricar dichos elementos con el siguiente resultado:

Proposition 2.13. *Sea $k \geqslant 2$. Sean $m, n \in \mathbb{Z}^+$ tales que $m-2>n$ y $n \geqslant k$. Entonces existe un elemento de la forma $x + C(m,n)x^{m+2(n-1)} + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.*

Demostración. Vemos que

$$[f_m, f_n] = x + (m-n)x^{m+n-1} + C(m,n)x^{m+2(n-1)} + \cdots .$$

Si $m+n-1 \equiv 0 \pmod 2$, entonces existe el siguiente elemento de $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$:

$$[f_{\frac{m+n-1}{2}+1}, f_{\frac{m+n-1}{2}}]^{-(m-n)} = x + (-(m-n))x^{m+n-1} + \alpha x^{3\frac{m+n-1}{2}-1} + \cdots .$$

Si asumimos que $3\frac{m+n-1}{2} - 1 \leqslant m + 2(n-1)$, entonces

$$\begin{aligned} &3m+3n-3 \leqslant 2m+4n-2 \\ \Leftrightarrow &m-1 \leqslant n \\ \Rightarrow &m-1 < m-2 \\ \Leftrightarrow &1 > 2 \end{aligned}$$

que es claramente una contradicción. De esta manera tenemos que $3\frac{m+n-1}{2} - 1 > m+2n-2$, y por tanto

$$[f_m, f_n] \circ [f_{\frac{m+n-1}{2}+1}, f_{\frac{m+n-1}{2}}]^{-(m-n)} = x + C(m,n)x^{m+2(n-1)} + \cdots .$$

Por otro lado, si $m+n-1 \equiv 1 \pmod 2$, entonces existe el siguiente elemento de $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$:

$$[f_{\frac{m+n-2}{2}+2}, f_{\frac{m+n-2}{2}}]^{-\frac{m-n}{2}} = x + (-(m-n))x^{m+n-1} + \beta x^{3\frac{m+n-2}{2}} + \cdots .$$

Si asumimos que $3\frac{m+n-2}{2} \leqslant m + 2(n-1)$, entonces

$$\begin{aligned} &3m+3n-6 \leqslant 2m+4n-4 \\ \Leftrightarrow &m-2 \leqslant n \\ \Rightarrow &m-2 < m-2 \end{aligned}$$

que es claramente una contradicción. De esta manera tenemos que $3\frac{m+n-2}{2} > m+2(n-1)$, y por tanto

$$[f_m, f_n] \circ [f_{\frac{m+n-2}{2}+2}, f_{\frac{m+n-2}{2}}]^{-\frac{m-n}{2}} = x + C(m,n)x^{m+2(n-1)} + \cdots .$$

$\square$

Sea $\ell(m,n) := m + 2(n-1)$. Dado $l \geqslant 2k$ impar, gracias al resultado anterior podremos intentar responder la pregunta de si existe un elemento de la forma $x + x^l + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$ buscando un par de enteros positivos (m,n) tal que $\ell(m,n) = l$ y $C(m,n) \equiv 1 \pmod 2$. Es por esta misma razón que estudiaremos la paridad de $C(m,n)$.

Recordando que $C(m,n) = \binom{m}{2} + (m-n)(m+n-1)$ podemos notar es que $C(m,n) \equiv \binom{m}{2} \pmod 2$. De donde bastará estudiar la paridad de este símbolo binomial. Lo que sigue no es particularmente difícil ni extenso.

Proposition 2.14. *Sea $m \geqslant 2$. Se tiene que $\binom{m}{2} \equiv 1 \pmod 2$ si y solo si $m \equiv 2 \pmod 4$ ó $m \equiv 3 \pmod 4$.*

Demostración. Por definición se tiene que

$$\begin{aligned}
&\binom{m}{2} \equiv 1 \pmod 2 \\
\Leftrightarrow &\frac{m(m-1)}{2} \equiv 1 \pmod 2 \\
\Leftrightarrow &\exists l \in \mathbb{Z} : \frac{m(m-1)}{2} = 1 + 2l \\
\Leftrightarrow &\exists l \in \mathbb{Z} : m(m-1) = 2 + 4l \\
\Leftrightarrow &m(m-1) \equiv 2 \pmod 4.
\end{aligned}$$

Ahora, evaluando en la última igualdad tenemos que las únicas clases que la cumplen son la del 2 módulo 4 y la del 3 módulo 4. Obtenemos que $m(m-1) \equiv 2 \pmod 4$ si y solo si $m \equiv 2 \pmod 4$ ó $m \equiv 3 \pmod 4$, lo cual completa la cadena de equivalencias que deseábamos. $\square$

Corollary 2.15. *Sean $m, n \in \mathbb{Z}^+$ tales que $m > n$. Se tiene que $C(m,n) \equiv 1 \pmod 2$ si y solo si $m \equiv 2 \pmod 4$ ó $m \equiv 3 \pmod 4$.*

De todo esto, la parte que más consecuencias tiene es que la paridad de $C(m,n)$ dependa de la clase módulo 4 de m.

Notemos que $\ell(m,n) \equiv m \pmod 2$. Es así que nos concentraremos en los casos en que $m \equiv 1 \pmod 2$. Gracias a la proposición anterior sabemos que si $m \equiv 1 \pmod 2$, entonces se cumple que $C(m,n) \equiv 1 \pmod 2$ si y solo si $m \equiv 3 \pmod 4$. De esta manera, dado $l \geqslant k$ impar, para fabricar un elemento de la forma $x + x^l + \cdots$ bastará encontrar un par de enteros positivos (m,n) tal que $l = \ell(m,n), m > n + 2, n \geqslant k$ y $m \equiv 3 \pmod 4$.

En garantizar que se cumplan la primera y última condición es donde habrá más sutilezas.
Para aliviar los enunciados les pondremos nombre a los pares de enteros que verifiquen algunas de estas hipótesis:

Definition 2.16. Diremos que $(m, n) \in \mathbb{Z}^2$ es útil si $m > n + 2$ y $m \equiv 1 \pmod 2$.

Definition 2.17. Dado $k \geqslant 2$. Diremos que $(m, n) \in \mathbb{Z}^2$ es $k-$útil si es útil y $n \geqslant k$.

Hacemos una distinción entre ambos pues, nuevamente, aliviará los enunciados.

Observación 2.18. *Sean $m, n \in \mathbb{Z}^+$, con $m > 2$. Notemos que $\ell(m-2, n+1) = \ell(m, n)$, y que*

$$C(m-2, n+1) \equiv \binom{m-2}{2} \not\equiv \binom{m}{2} \equiv C(m, n) \pmod 2.$$

De esta manera tenemos que si (m, n) es útil, entonces $C(m-2, n+1) \not\equiv C(m, n) \pmod 2$.
Es así que, dado $k \geqslant 2$, si para un $l \geqslant k$ impar garantizamos que existe un par $k-$útil (m, n) tal que $l = \ell(m, n)$ y $(m-2, n+1)$ es $k-$útil, entonces garantizamos que existe un elemento de la forma $x + x^l + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.
Es por esto que nos preocuparemos de escribir impares en términos de pares útiles.

Proposition 2.19. *Para todo entero impar l existe un par útil (m, n) tal que $l = \ell(m, n)$.*
En particular, se tiene que:

- *Si $l \equiv 0 \pmod 3$ y $l \equiv 1 \pmod 4$, entonces existe $n \in \mathbb{Z}$ tal que $n \equiv 2 \pmod 4$ y $l = \ell(n+5, n)$.*
- *Si $l \equiv 0 \pmod 3$ y $l \equiv 3 \pmod 4$, entonces existe $n \in \mathbb{Z}$ tal que $n \equiv 3 \pmod 4$ y $l = \ell(n+8, n)$.*
- *Si $l \equiv 1 \pmod 3$, entonces existe $n \in \mathbb{Z}$ tal que $n \equiv 1 \pmod 2$ y $l = \ell(n+6, n)$.*
- *Si $l \equiv 2 \pmod 3$, entonces existe $n \in \mathbb{Z}$ tal que $n \equiv 0 \pmod 2$ y $l = \ell(n+7, n)$.*

Demostración. Tal como sugiere el enunciado, separaremos en los distintos casos módulo 3.

- Si $l \equiv 0 \pmod 3$ y $l \equiv 1 \pmod 4$, entonces por el Teorema Chino de los Restos tenemos que $l \equiv 9 \pmod{12}$. Es decir, existe $s \in \mathbb{Z}$ tal que $l = 12s + 9$. De esta manera, si consideramos $n = 4s + 2$, entonces

  $$\ell(n + 5, n) = 3n + 3 = 12s + 9 = l.$$

  Claramente $n \equiv 2 \pmod 4$ y $(n + 5, n)$ es un par útil.

- Si $l \equiv 0 \pmod 3$ y $l \equiv 3 \pmod 4$, entonces por el Teorema Chino de los Restos tenemos que $l \equiv 3 \pmod{12}$. Es decir, existe $s \in \mathbb{Z}$ tal que $l = 12s+3$. De esta manera, si consideramos $n = 4(s-1)+3$, entonces

  $$\ell(n + 8, n) = 3n + 6 = 12s + 3 = l.$$

  Claramente $n \equiv 3 \pmod 4$ y $(n + 8, n)$ es un par útil.

- Si $l \equiv 1 \pmod 3$, entonces existe $s \in \mathbb{Z}$ tal que $l = 3s + 1$. Vemos que $l \equiv 1 \pmod 2$ implica que $s \equiv 0 \pmod 2$. De esta manera, si consideramos $n = s - 1$, entonces

  $$\ell(n + 6, n) = n + 6 + 2(n - 1) = 3n + 3 + 1 = 3(n + 1) + 1 = l.$$

  Claramente $n \equiv 1 \pmod 2$ y $(n + 6, n)$ es un par útil.

- Si $l \equiv 2 \pmod 3$, entonces existe $s \in \mathbb{Z}$ tal que $l = 3s + 2$. Vemos que $l \equiv 1 \pmod 2$ implica que $s \equiv 1 \pmod 2$. De esta manera, si consideramos $n = s - 1$, entonces

  $$\ell(n + 7, n) = n + 7 + 2(n - 1) = 3n + 3 + 2 = 3(n + 1) + 1 = l.$$

  Claramente $n \equiv 0 \pmod 2$ y $(n + 7, n)$ es un par útil.

$\square$

Ya estamos en posición de dar una primera cota:

Corollary 2.20. *Sea $k \geqslant 2$. Para todo impar $l \geqslant 3k+5$ existe un par $k-$útil (m, n) tal que $l = \ell(m, n)$ y $C(m, n) \equiv 1 \pmod 2$.*

Demostración. Separamos por casos.

- Si $l \equiv 0 \pmod 3$ y $l \equiv 1 \pmod 4$, entonces existe $n \in \mathbb{Z}$ tal que $n \equiv 2 \pmod 4$ y $l = \ell(n+5, n)$. Comenzamos observando que

$$\begin{aligned} \ell(n+5, n) \geqslant& 3k+5 \\ \Leftrightarrow 3(n+1) \geqslant& 3k+5 \\ \Leftrightarrow n+1 \geqslant& k+\frac{5}{3} \\ \Leftrightarrow n \geqslant& k+\frac{2}{3} \\ \Rightarrow n \geqslant& k. \end{aligned}$$

  De esta manera concluimos que $(n+5, n)$ es $k-$útil.
  Siendo $n+5 \equiv 3 \pmod 4$, tendremos que $C(n+5, n)$ es impar.

- Si $l \equiv 0 \pmod 3$ y $l \equiv 3 \pmod 4$, entonces existe $n \in \mathbb{Z}$ tal que $n \equiv 3 \pmod 4$ y $l = \ell(n+8, n)$. Comenzamos observando que

$$\begin{aligned} l \geqslant& 3k+5 \\ \Leftrightarrow \ell(n+8, n) \geqslant& 3k+5 \\ \Leftrightarrow 3n+6 \geqslant& 3k+5 \\ n \geqslant& k-\frac{1}{3} \end{aligned}$$

  Dado que $n \in \mathbb{Z}$, tenemos que la última desigualdad implica que $n \geqslant k$.
  De esta manera concluimos que $(n+8, n)$ es $k-$útil.
  Siendo $n+8 \equiv 3 \pmod 4$, tendremos que $C(n+8, n)$ es impar.

- Si $l \equiv 1 \pmod 3$, entonces existe $n \in \mathbb{Z}$ tal que $n \equiv 1 \pmod 2$ y $l = \ell(n+6, n)$. Vemos que

$$\begin{aligned} l &\geqslant 3k+5 \\ \Leftrightarrow \ell(n+6,n) &\geqslant 3k+5 \\ \Leftrightarrow 3(n+1)+1 &\geqslant 3k+5 \\ \Leftrightarrow n &\geqslant k+\frac{1}{3} \\ \Rightarrow n &\geqslant k. \end{aligned}$$

Concluimos que tanto $(n+6,n)$ como $(n+4,n+1)$ son $k-$útiles. Además, o $C(n+6,n)$ es impar, o $C(n+4,n+1)$ es impar.

- Si $l \equiv 2 \pmod 3$, entonces existe $n \in \mathbb{Z}$ tal que $n \equiv 0 \pmod 2$ y $l = \ell(n+7,n)$. Vemos que

$$\begin{aligned} l &\geqslant 3k+5 \\ \Leftrightarrow \ell(n+7,n) &\geqslant 3k+5 \\ \Leftrightarrow 3(n+1)+2 &\geqslant 3k+5 \\ \Leftrightarrow n &\geqslant k. \end{aligned}$$

Concluimos que tanto $(n+7,n)$ como $(n+5,n+1)$ son $k-$útiles. Además, o $C(n+7,n)$ es impar, o $C(n+5,n+1)$ es impar.

$\square$

De esta manera tenemos que, dado $k \geqslant 2$, para todo $l \geqslant 3k+5$ impar existe un elemento de la forma $x+x^l+\cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$. Y dado que para $l \geqslant 2k$ par ya existe un elemento de dicha forma en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$, podemos concluir que $\mathcal{J}_{3k+5}(\mathbb{Z}) \subset [\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$. Esta cota no es solo mejorable, si no que puede ser mejorada usando el mismo método. Veremos en seguida que esta mejora solo depende de la clase de k módulo 4.
Definimos el siguiente número:

$$c_k := \begin{cases} 3k+1 & si\ k \equiv 1 \pmod 2 \\ 3k+2 & si\ k \equiv 2 \pmod 4 \\ 3k+4 & si\ k \equiv 0 \pmod 4 \end{cases}$$

Notemos que $c_k \equiv 0 \pmod 2$ para todo $k \geqslant 2$. Este es un hecho del cual haremos uso a menudo.

Lemma 2.21. *Sea $k \geqslant 2$. Se cumple que $\mathcal{J}_{c_k}(\mathbb{Z}) \subset [\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$*

Demostración. Fijaremos $k \geqslant 2$. Ya sabemos que $\mathcal{J}_{3k+5}(\mathbb{Z}) \subset [\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$. Demostraremos que para todo $l \in \{c_k, \dots, 3k+4\}$, existen elementos de la forma $x + x^l + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$. Como sugiere la definición de c_k, trataremos esto por casos.

- Si $k \equiv 3 \pmod 4$, entonces hay que demostrar que para todo $l \in \{3k+1, 3k+2, 3k+3, 3k+4\}$ existe un elemento de la forma $x+x^l+\cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.
  Notemos que $3k+1$ y $3k+3$ son pares. Siendo ambos mayores que $2k$, sabemos que existen elementos de la forma $x + x^{3k+1} + \cdots$ y $x + x^{3k+3} + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.
  Por otro lado, vemos que $3k+2 = \ell(k+4, k)$ y $3k+4 = \ell(k+4, k+2)$. Siendo tanto $(k+4, k)$ como $(k+4, k+2)$ pares $k-$útiles, y
  $$C(k+4, k) \equiv 1 \equiv C(k+4, k+2) \pmod 2$$
  pues $k+4 \equiv 3 \pmod 4$, concluimos que existen los elementos de la forma $x + x^{3k+2} + \cdots$ y $x + x^{3k+4} + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.

- Si $k \equiv 2 \pmod 4$, entonces hay que demostrar que para todo $l \in \{3k+2, 3k+3, 3k+4\}$ existe un elemento de la forma $x + x^l + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.
  Notemos que $3k+2$ y $3k+4$ son pares. Siendo ambos mayores que $2k$, sabemos que existen elementos de la forma $x + x^{3k+2} + \cdots$ y $x + x^{3k+4} + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.
  Por otro lado, vemos que $3k+3 = \ell(k+5, k)$. Siendo $(k+5, k)$ un par $k-$útil y
  $$C(k+5, k) \equiv 1 \pmod 2$$
  pues $k+5 \equiv 3 \pmod 4$, concluimos que existe un elemento de la forma $x + x^{3k+3} + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.

- Si $k \equiv 1 \pmod 4$, entonces hay que demostrar que para todo $l \in \{3k+1, 3k+2, 3k+3, 3k+4\}$ existe un elemento de la forma $x+x^l+\cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.
  Notemos que $3k+1$ y $3k+3$ son pares. Siendo ambos mayores que $2k$, sabemos que existen elementos de la forma $x+x^{3k+1}+\cdot$ y $x+x^{3k+3}+\cdot$

en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.
Notemos que $3k+4 = \ell(k+6,k)$. Siendo $(k+6,k)$ un par $k-$útil y

$$C(k+6,k) \equiv 1 \pmod 2$$

pues $k+6 \equiv 3 \pmod 4$, concluimos que existe un elemento de la forma $x + x^{3k+4} + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.
Por último, vemos que

$$[f_{k+3}, f_k] = x + 3x^{2k+2} + C(k+3,k)x^{3k+1} + \cdots,$$

y

$$[f_{k+2}, f_{k+1}] = x + x^{2k+2} + C(k+2,k)x^{3k+1} + \cdots.$$

De esta manera podemos obtener

$$[f_{k+2}, f_{k+1}]^3 \circ [f_{k+3}, f_k]^{-1} = x + (3C(k+2,k) + C(k+3,k))x^{3k+1} + \cdots.$$

Dado que $3C(k+2,k) + C(k+3,k) \equiv 1 \pmod 2$, concluimos que existe un elemento de la forma $x + x^{3k+1} + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.

- Si $k \equiv 0 \pmod 4$, entonces basta demostrar que existe un elemento de la forma $x + x^{3k+4} + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.
  Notemos que $3k+4$ es par. Además $3k+4$ es mayor que $2k$, por lo que podemos concluir que existe un elemento de la forma $x + x^{3k+4} + \cdots$ en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.

□

Con las herramientas a mano, la cota c_k es la mejor que podemos obtener para demostrar que un grupo $\mathcal{J}_l(\mathbb{Z})$ este contenido en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$. Sorprendentemente veremos al final de esta tesis que es efectivamente la mejor, en el sentido de que $\mathcal{J}_{c_k-1}(\mathbb{Z}) \nsubseteq [\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.
Este lema tiene dos consecuencias de las que nos aprovecharemos fuertemente. La primera será usar el siguiente teorema:

Theorem 2.22 (Teorema del Factor)**.** *Sea $\varphi : G \to H$ un morfismo de grupos y $N \trianglelefteq G$ tal que $N \subseteq ker(\varphi)$. Entonces existe un único morfismo $\tilde{\varphi} : G/N \to H$ tal que $\varphi = \tilde{\varphi} \circ p$. Esto es equivalente a decir que el siguiente diagrama conmuta:*

$$\begin{tikzcd} G \arrow[rr, "\varphi"] \arrow[dr, "p"'] & & H \\ & G/N \arrow[ur, "\tilde{\varphi}"'] & \end{tikzcd}$$

Observación 2.23. *Si consideramos $k \geqslant 2$ y $\pi : \mathcal{J}_k(\mathbb{Z}) \to H_1(\mathcal{J}_k(\mathbb{Z}))$ como la proyección canónica, tendremos que el siguiente diagrama conmuta:*

$$\begin{tikzcd} \mathcal{J}_k(\mathbb{Z}) \arrow[rr, "\pi"] \arrow[dr, "p"'] & & H_1(\mathcal{J}_k(\mathbb{Z})) \\ & \mathcal{J}_k^{c_k}(\mathbb{Z}) \arrow[ur, "\tilde{\pi}"'] & \end{tikzcd}$$

Dicho de una manera más informal: las imágenes de π pueden ser calculadas a través de $\tilde{\pi}$. Esto es de mucha ayuda pues como sabemos $\mathcal{J}_k^{c_k}(\mathbb{Z})$ es discreto, por lo que podremos trabajar solo con su estructura de grupo y olvidar en gran medida que se trata de un grupo topológico.
La segunda consecuencia importante es que, si bien es claro que $\mathcal{J}_{c_k}(\mathbb{Z}) \neq [\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$, este lema nos de un excelente criterio para verificar cuando se tiene que un elemento de $\mathcal{J}_k(\mathbb{Z})$ se encuentra en $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$. Combinado con la observación anterior, tendremos una buena herramienta para determinar cuando dos elementos pertenecen a la misma clase en $H_1(\mathcal{J}_k(\mathbb{Z}))$.

Capítulo 3

Resultados principales

Como ya se menciono en la introducción, el teorema principal de este trabajo es el siguiente:

Teorema 1.2 *Sea $k \geqslant 5$.*
Si $k \equiv 3 \pmod 4$, entonces

$$H_1(\mathcal{J}_k(\mathbb{Z})) \cong \mathbb{Z}^k \bigoplus (\mathbb{Z}/2\mathbb{Z})^{\frac{k+1}{2}}$$

Si $k \equiv 2 \pmod 4$, entonces

$$H_1(\mathcal{J}_k(\mathbb{Z})) \cong \mathbb{Z}^k \bigoplus (\mathbb{Z}/2\mathbb{Z})^{\frac{k+2}{2}}$$

Si $k \equiv 1 \pmod 4$, entonces

$$H_1(\mathcal{J}_k(\mathbb{Z})) \cong \mathbb{Z}^k \bigoplus \mathbb{Z}/4\mathbb{Z} \bigoplus (\mathbb{Z}/2\mathbb{Z})^{\frac{k-3}{2}}$$

Si $k \equiv 0 \pmod 4$, entonces

$$H_1(\mathcal{J}_k(\mathbb{Z})) \cong \mathbb{Z}^k \bigoplus \mathbb{Z}/4\mathbb{Z} \bigoplus (\mathbb{Z}/2\mathbb{Z})^{\frac{k-2}{2}}$$

Reiteramos que si bien el enunciado es para $k \geqslant 5$, fijaremos de todas formas $k \geqslant 2$, pues es solo al final por unos detalles técnicos que se impone esta restricción, y varios de los resultados que demostraremos seguirán siendo válidos en dicho contexto y podrán ser usados para lidiar con los casos restantes. También fijaremos $\pi : \mathcal{J}_k(\mathbb{Z}) \to H_1(\mathcal{J}_k(\mathbb{Z}))$ como la proyección canónica. Haremos la demostración por medio de una serie de resultados intermedios.

3.1 Identificación de la torsión

Como sugiere el enunciado de nuestro teorema principal, la parte más difícil proviene de la torsión. Es por esto que primero nos tomaremos el tiempo de verla desde una perspectiva más cómoda. A decir, demostraremos lo siguiente:

Proposition 3.1. *La torsión de* $H_1(\mathcal{J}_k(\mathbb{Z}))$ *es* $\pi(\mathcal{J}_{2k}(\mathbb{Z}))$.

Llamaremos $T(H_1(\mathcal{J}_k(\mathbb{Z})))$ *a la torsión de* $H_1(\mathcal{J}_k(\mathbb{Z}))$. *Para demostrar la proposición anterior, demostraremos que* $T(H_1(\mathcal{J}_k(\mathbb{Z})))$ *está contenido en* $\pi(\mathcal{J}_{2k}(\mathbb{Z}))$ *y viceversa.*
Gracias al hecho de que $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})] \subset \mathcal{J}_{2k}(\mathbb{Z})$, *verificar la primera contención es bastante sencillo.*

Proposition 3.2. *La torsión de* $H_1(\mathcal{J}_k(\mathbb{Z}))$ *esta contenida en* $\pi(\mathcal{J}_{2k}(\mathbb{Z}))$.

Demostración. Sea $\tilde{f} \in T(H_1(\mathcal{J}_k(\mathbb{Z})))$. Siendo π sobreyectiva, sabemos que existe $f \in \mathcal{J}_k(\mathbb{Z})$ tal que $\pi(f) = \tilde{f}$.
Por definición, se tiene que existe $n \in \mathbb{Z}^+$ tal que $\tilde{f}^n = 0$. Siendo $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})] = ker(\pi)$, esto es equivalente a decir que $f^n \in [\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.
Dado que $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})] \subset \mathcal{J}_{2k}(\mathbb{Z})$, esto implica que $nvl(f^n) \geqslant 2k$. Gracias al Corolario 2.3 tenemos que $nvl(f) = nvl(f^n)$.
De esta manera, vemos que $nvl(f) \geqslant 2k$. Es decir $f \in \mathcal{J}_{2k}(\mathbb{Z})$.
Por lo tanto $\pi(f) \in \pi(\mathcal{J}_{2k}(\mathbb{Z}))$. Concluimos que $\pi(\mathcal{J}_{2k}(\mathbb{Z})) \supseteq T(H_1(\mathcal{J}_k(\mathbb{Z})))$. □

Demostrar la contención de $\pi(\mathcal{J}_{2k}(\mathbb{Z}))$ *en* $T(H_1(\mathcal{J}(\mathbb{Z})))$ *será más difícil. Para esto, demostraremos* $\pi(\mathcal{J}_{2k}(\mathbb{Z}))$ *esta generado por elementos de orden finito.*

Recordemos que $f_i = x + x^i \in \mathcal{J}(\mathbb{Z})$ *para todo* $i \geqslant 2$ *y* $\mathcal{J}_{2k}(\mathbb{Z}) = \overline{\langle f_i | i \geqslant 2k \rangle}$.

Observación 3.3. *En virtud de la Observación 2.23, tenemos que*

$$\pi(\mathcal{J}_{2k}(\mathbb{Z})) = \tilde{\pi}(\mathcal{J}_{2k}^{c_k}(\mathbb{Z})).$$

Como sabemos

$$\mathcal{J}_{2k}^{c_k}(\mathbb{Z}) = \langle f_i + O(x^{c_k}) | 2k \leqslant i \leqslant c_k - 1 \rangle,$$

por lo que

$$\tilde{\pi}(\mathcal{J}_{2k}^{c_k}(\mathbb{Z})) = \langle \tilde{\pi}(f_i + O(x^{c_k})) | 2k \leqslant i \leqslant c_k - 1 \rangle.$$

Es decir

$$\pi(\mathcal{J}_{2k}(\mathbb{Z})) = \langle \pi(f_i) | 2k \leqslant i \leqslant c_k - 1 \rangle.$$

Tenemos los generadores, ahora queremos demostrar que son de orden finito. Para esto, demostraremos un pequeño lema técnico para acortar las siguientes demostraciones.

Lemma 3.4. *Si $l \geqslant 2k + 1$, entonces $\pi(f_l)^2 = \pi(x + 2x^l)$.*

Demostración. Sabemos que

$$f_l{}^2 = x + 2x^l + R,$$

donde $R \in x^{2l-1}\mathbb{Z}[[x]]$. Vemos que

$$2l - 1 \geqslant 2(2k + 1) - 1 = 4k + 1.$$

Si $k \geqslant 4$, entonces $4k + 1 > 3k + 4 \geqslant c_k$. Mientras que, si $k \in \{2, 3\}$, entonces se puede verificar directamente que $4k + 1 > c_k$.

De esta manera, vemos que

$$(f_l + O(x^{c_k}))^2 = x + 2x^l + O(x^{c_k}).$$

Esto implica que

$$\tilde{\pi}(f_l + O(x^{c_k}))^2 = \tilde{\pi}(x + 2x^l + O(x^{c_k})),$$

Y dada la observación 2.23, esto es equivalente a

$$\pi(f_l)^2 = \pi(x + 2x^l).$$

□

Introduciremos un poco más de notación: En un grupo G, denotaremos por $|g|$ al orden de un elemento $g \in G$. Nuestro objetivo es demostrar que $|\pi(f_l)| < \infty$ para todo $l \geqslant 2k$.

Recordemos también que, para $m > n$, se tiene

$$[f_m, f_n] = x + (m - n)x^{m+n-1} + C(m, n)x^{m+2(n-1)} + \cdots$$

donde $C(m, n) = \binom{m}{2} - (m - n)(m + n - 1)$.

Proposition 3.5. *Si $l \geqslant k+2$, entonces $\pi(f_{2l}) = 0$ y $|\pi(f_{2l+1})| \leqslant 2$.*

Demostración. Recordemos que para todo $l \geqslant k$ se tiene que

$$[f_{l+1}, f_l] = x + x^{2l} + C(l+1,l)x^{3l-1} + \cdots .$$

De esta manera tenemos que $f_{2l} \circ [f_{l+1}, f_l]^{-1} \in \mathcal{J}_{c_k}(\mathbb{Z})$ si y solo si $3l-1 \geqslant c_k$. Vemos que $l \geqslant k+2$ implica $3l-1 \geqslant 3k+5$. Siendo $3k+5 > c_k$, esto implica que $\pi(f_{2l}) = 0$.

Por otro lado, vemos que para todo $l \geqslant k$ se tiene que

$$(x + 2x^{2l+1}) \circ [f_{l+2}, f_l]^{-1} \in \mathcal{J}_{3l}(\mathbb{Z}).$$

Dado que $l \geqslant k+2$, tenemos que $3l > c_k$, por lo que $(x + 2x^{2l+1}) \circ [f_{l+2}, f_l]^{-1} \in \mathcal{J}_{c_k}(\mathbb{Z})$. De esta manera

$$\pi(f_{2l+1})^2 = \pi(x + 2x^l) = 0.$$

Concluimos que $|\pi(f_{2l+1})| \leqslant 2$. □

Esto no solo nos ayuda a determinar el orden de la gran mayoría de los generadores y reducir la cantidad de estos, si no que también nos esta indicado parte de la estructura de $\pi(\mathcal{J}_{2k}(\mathbb{Z}))$. Esto será crucial para la siguiente sección. De momento podemos decir lo siguiente:

Corollary 3.6. *Se cumple que*

$$\pi(\mathcal{J}_{2k}(\mathbb{Z})) = \langle \{\pi(f_{2k}), \pi(f_{2k+1}), \pi(f_{2k+2}), \pi(f_{2k+3})\} \cup \{\pi(f_{2i+1}) | k+2 \leqslant i \leqslant \tfrac{c_k}{2} - 1\} \rangle.$$

Notemos que

$$\begin{aligned} &\{\pi(f_{2k}), \pi(f_{2k+1}), \pi(f_{2k+2}), \pi(f_{2k+3})\} \cup \{\pi(f_{2i+1}) | k+2 \leqslant i \leqslant \tfrac{c_k}{2} - 1\} \\ =&\{\pi(f_{2k}), \pi(f_{2k+2})\} \cup \{\pi(f_{2i+1}) | k \leqslant i \leqslant \tfrac{c_k}{2} - 1\}. \end{aligned}$$

Hacemos esto pues podemos quitar dos generadores más.

Proposition 3.7. *El subgrupo $\pi(\mathcal{J}_{2k}(\mathbb{Z}))$ esta generado por $\{\pi(f_{2i+1}) | k \leqslant i \leqslant \frac{c_k}{2} - 1\}$.*

Demostración. Consideremos

$$[f_{k+1}, f_k] = x + x^{2k} + C(k+1,k)x^{3k-1} + \cdots .$$

Vemos que $f_{2k} \circ [f_{k+1}, f_k] \in \mathcal{J}_{3k-1}(\mathbb{Z})$. Esto implica que $\pi(f_{2k}) \in \langle \pi(f_{3k-1}), \ldots, \pi(f_{c_k-1}) \rangle$. Siendo $k \geqslant 2$, tendremos que $3k-1 \geqslant 2k+1$. De esta manera, $\pi(f_{2k}) \in \langle \pi(f_{2k+1}), \ldots, \pi(f_{c_k-1}) \rangle$, y por tanto

$$\langle \{\pi(f_{2k}), \pi(f_{2k+2})\} \cup \{\pi(f_{2i+1}) | k \leqslant i \leqslant \tfrac{c_k}{2} - 1\} \rangle = \langle \{\pi(f_{2k+2})\} \cup \{\pi(f_{2i+1}) | k \leqslant i \leqslant \tfrac{c_k}{2} - 1\} \rangle.$$

Análogamente, basta notar que

$$[f_{k+2}, f_{k+1}] = x + x^{2k+2} + C(k+2,k+1)x^{3k+2} + \cdots$$

y que $k \geqslant 2$ implica $3k+2 > 2k+3$ para repetir el argumento anterior. □

Ahora, para terminar nuestra demostración, solo falta probar que tanto $\pi(f_{2k+1})$ como $\pi(f_{2k+3})$ tienen orden finito. Como veremos enseguida, las demostraciones siguen el mismo ritmo que han llevado hasta ahora, pero será conveniente separar respecto a las posibles clases módulo 4 de k. Lo haremos de esta manera pues nos ahorrará unas cuantas sutilezas y los siguientes resultados volverán a ser útiles en la siguiente sección.

Proposition 3.8. *Si $k \not\equiv 0 \pmod 4$, entonces $|\pi(f_{2k+3})| \leqslant 2$.*

Demostración. Notemos que

$$[f_{k+3}, f_{k+1}] = x + 2x^{2k+3} + C(k+3,k+1)x^{3k+3} + \cdots .$$

Por otro lado, vemos que

$$(x + 2x^{2k+3}) \circ [f_{k+3}, f_{k+1}]^{-1} \in \mathcal{J}_{3k+3}(\mathbb{Z}).$$

Dado que $k \not\equiv 0 \pmod 4$, sabemos que $3k+3 \geqslant c_k$. Esto implica que $\mathcal{J}_{3k+3}(\mathbb{Z}) \subseteq \mathcal{J}_{c_k}(\mathbb{Z})$. Por lo tanto

$$(x + 2x^{2k+3}) \circ [f_{k+3}, f_{k+1}]^{-1} \in \mathcal{J}_{c_k}(\mathbb{Z}).$$

Concluimos que $\pi(f_{2k+3})^2 = \pi(x + 2x^{2k+3}) = 0$, por lo que $|\pi(f_{2k+3})| \leqslant 2$. □

Proposition 3.9. *Si $k \equiv 0 \pmod 4$, entonces $|\pi(f_{2k+3})|$ divide a 4.*

Demostración. Recordemos que

$$[f_{k+3}, f_{k+1}] = x + 2x^{2k+3} + C(k+3, k+1)x^{3k+3} + \cdots .$$

Vemos que

$$(x + 2x^{2k+3}) \circ [f_{k+3}, f_{k+1}]^{-1} \in \mathcal{J}_{3k+3}(\mathbb{Z}).$$

Dado que $k \equiv 0 \pmod 4$, sabemos que $\pi(\mathcal{J}_{3k+3}(\mathbb{Z})) = \langle \pi(f_{3k+3}) \rangle$. De esta manera, vemos que

$$\pi(f_{2k+3})^2 = \pi(x + 2x^{2k+3}) \in \langle \pi(f_{3k+3}) \rangle.$$

Es decir, existe $\alpha \in \mathbb{Z}$ tal que

$$\pi(f_{2k+3})^2 = \pi(f_{3k+3})^{\alpha}.$$

Siendo $3k + 3 \geqslant 2k + 4$, tenemos que

$$\pi(f_{2k+3})^4 = \pi(f_{3k+3})^{2\alpha} = 0.$$

Concluimos que $|\pi(f_{2k+3})|$ divide a 4. $\square$

Como ya mencionamos, el siguiente caso presentará algunas sutilezas. Estas no son particularmente difíciles, pero nos obligarán a tratar un par de casos aparte.

Proposition 3.10. *Si* $k \not\equiv 3 \pmod 4$*, entonces* $|\pi(f_{2k+1})|$ *divide a* 4*.*

Demostración. Recordemos que

$$[f_{k+2}, f_k] = x + 2x^{2k+1} + C(k+2, k)x^{3k} + \cdots .$$

Vemos que

$$(x + 2x^{2k+1}) \circ [f_{k+2}, f_k]^{-1} \in \mathcal{J}_{3k}(\mathbb{Z}).$$

Esto implica que $\pi(f_{2k+1})^2 = \pi(x + 2x^{2k+1}) \in \langle \pi(f_{3k}), \ldots, \pi(f_{c_k-1}) \rangle$. Es decir para todo $i \in \{3k, \ldots, c_k - 1\}$ existe $\alpha_i \in \{0, 1\}$ tal que

$$\pi(f_{2k+1})^2 = \prod_{i=3k}^{c_k-1} \pi(f_i)^{\alpha_i}.$$

En este punto hay que separar por casos, estos serán el caso de $k \equiv 0 \pmod 4$ o $k \equiv 1 \pmod 4$ y el caso de $k \equiv 2 \pmod 2$. Partiremos por el

primer caso:
Dado que $k \equiv 0 \pmod 4$ o $k \equiv 1 \pmod 4$, tenemos que $k \geqslant 4$, esto implica que $3k \geqslant 2k+4$. Siendo $H_1(\mathcal{J}_k(\mathbb{Z}))$ abeliano vemos que

$$\pi(f_{2k+1})^4 = \left(\prod_{i=3k}^{c_k-1} \pi(f_i)^{\alpha_i}\right)^2 = \prod_{i=3k}^{c_k-1} \pi(f_i)^{2\alpha_i} = 0.$$

Concluimos que en este caso $|\pi(f_{2k+1})|$ divide a 4.

Para el caso de $k \equiv 2 \pmod 4$, vemos que $3k \equiv 0 \pmod 2$. Esto implica que

$$\langle \pi(f_{3k}), \ldots, \pi(f_{c_k-1})\rangle = \langle \pi(f_{3k+1}), \ldots, \pi(f_{c_k-1})\rangle$$

Dado que $k \geqslant 2$ implica que $3k+1 \geqslant 2k+3$, podemos usar un argumento análogo al caso anterior para concluir que $|\pi(f_{2k+1})|$ divide a 4.

$\square$

Proposition 3.11. *Si* $k \equiv 3 \pmod 4$, *entonces* $|\pi(f_{2k+1})| \leqslant 2$.

Demostración. Recordemos que en este caso $c_k = 3k+1$ y $C(k+2,k) \equiv 0 \pmod 2$. Tenemos que

$$[f_{k+2}, f_k] = x + 2x^{2k+1} + C(k+2,k)x^{3k} + \cdots.$$

Además, tenemos que

$$[f_{\frac{3k-1}{2}+2}, f_{\frac{3k-1}{2}}] = x + 2x^{3k} + \alpha x^{3\frac{3k-1}{2}} + \cdots.$$

De esta manera, consideremos

$$g = [f_{k+2}, f_k]^{-1} \circ [f_{\frac{3k-1}{2}+2}, f_{\frac{3k-1}{2}}]^{\frac{C(k+2,k)}{2}+1} = x - 2x^{2k+1} + 2x^{3k} + \cdots.$$

Notemos que $g \in [\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})]$.
Por otro lado, vemos que

$$(f_{2k+1})^2 = x + 2x^{2k+1} + R_{2k+1},$$

donde $R_{2k+1} \in x^{4k+1}\mathbb{Z}[[x]]$. Es claro que $4k+1 \geqslant 3k+1$. De esta manera, tenemos que

$$f^2 \circ g = x + 2x^{3k} + \cdots.$$

Esto implica que $\pi(f_{2k+1})^2 = \pi(f_{3k})^2$.
Como ya sabemos, para este caso se cumple que $|\pi(f_{2i+1})| \leqslant 2$ para todo $i \in \{k+1, \frac{c_k}{2} - 1\}$. Siendo $k \equiv 3 \pmod 4$, tendremos que $k \geqslant 3$, por lo que $3k \geqslant 2k+3$. De estas dos últimas observaciones concluimos que $\pi(f_{3k})^2 = 0$, y por tanto que $\pi(f_{2k+1})^2 = 0$. Es decir $|\pi(f_{2k+1})| \leqslant 2$. $\square$

Finalmente podemos demostrar lo siguiente:

Proposition 3.12. *La torsión de $H_1(\mathcal{J}_k(\mathbb{Z}))$ contiene a $\pi(\mathcal{J}_{2k}(\mathbb{Z}))$.*

Demostración. Vemos que $\pi(\mathcal{J}_{2k}(\mathbb{Z}))$ esta finitamente generado por elementos de orden finito. Siendo $H_1(\mathcal{J}_k(\mathbb{Z}))$ un grupo abeliano, esto implica que todo elemento de $\pi(\mathcal{J}_{2k}(\mathbb{Z}))$ tiene orden finito, de donde se tiene que $\pi(\mathcal{J}_{2k}(\mathbb{Z})) \subset T(H_1(\mathcal{J}_k(\mathbb{Z})))$. $\square$

Con esto podemos concluir que se cumple la Proposición 3.1.

3.2 Cálculo de la torsión

Dado los resultados de la sección anterior, nos referiremos a $T(H_1(\mathcal{J}_k(\mathbb{Z})))$ y $\pi(\mathcal{J}_{2k}(\mathbb{Z}))$ de manera intercambiable.
Ya sabemos que $\pi(\mathcal{J}_{2k}(\mathbb{Z}))$ es un grupo abeliano finito y tenemos un conjunto generador de este. Lo que no sabemos es si dentro de este conjunto generador hay relaciones. Esto es un problema pues queremos determinar a este subgrupo como una suma directa de grupos cíclicos, y a priori podría hasta ser el grupo trivial. Veremos que este no es el caso, y que el conjunto de generadores está bastante cerca de darnos las respuestas que buscamos. Pero para llegar a dicho punto, tendremos que calcular conmutadores de forma explícita. Al principio de esta tesis esto podía sonar imposible, pero gracias al lema 2.21, y en particular al diagrama de la observación 2.23:

$$\begin{tikzcd}
\mathcal{J}_k(\mathbb{Z}) \arrow[rr, "\pi"] \arrow[dr, "p"'] & & H_1(\mathcal{J}_k(\mathbb{Z})) \\
& \mathcal{J}_k^{c_k}(\mathbb{Z}) \arrow[ur, "\tilde{\pi}"'] &
\end{tikzcd}$$

podremos contentarnos con intentar calcular conmutadores en $\mathcal{J}_k^{c_k}(\mathbb{Z})$. Para calcular dichos elementos tendremos que calcular el producto e inverso. El primero resulta ser razonablemente sencillo, pero el segundo presenta

ciertas dificultades que podemos ahorrarnos gracias al trabajo hecho en la sección anterior.
Previo a este punto se ha hecho alusión a que, dado un elemento de la forma $x + \sum_{i=2k}^{c_k-1} \alpha_i x^i + O(x^{c_k})$*, para calcular su clase en* $H_1(\mathcal{J}_k(\mathbb{Z}))$ *podemos olvidarnos de los coeficientes que corresponden a una potencia par de* x *y tomar la clase módulo* 2 *de los coeficientes que corresponden a potencias impares de* x*. Si bien esto puede parecer algo muy informal, puede ser formalizado tomando un cociente de* $\mathcal{J}_k^{c_k}(\mathbb{Z})$*. Más aún, podremos factorizar* $\tilde{\pi}$ *por este cociente. Esto es significativo pues calcular conmutadores en tal cociente será mucho mas cómodo que hacerlo en* $\mathcal{J}_k^{c_k}(\mathbb{Z})$*. Con el propósito de tomar este atajo, definiremos el siguiente número:*

$$d_k := \begin{cases} 2k+1 & si\ k \equiv 3 \pmod 4 \\ 2k+2 & si\ k \equiv 2 \pmod 4 \ ó\ k \equiv 1 \pmod 4 \\ 2k+4 & si\ k \equiv 0 \pmod 4 \end{cases}$$

Notemos que si $k \not\equiv 1 \pmod 4$*, entonces* $d_k = c_k - k$*. Podríamos definirlo de esa forma, pero es mejor escribirlo de forma explícita para lo que sigue. Definimos el siguiente subconjunto:*

$$H_k := \left\{ x + \sum_{i=d_k}^{c_k-1} \alpha_i x^i + O(x^{c_k}) \in \mathcal{J}_k^{c_k}(\mathbb{Z}) \middle| \alpha_i \equiv 0 \pmod 2, \forall i \in (2\mathbb{Z}+1) \cap \mathbb{Z}_{\geqslant d_k} \right\}.$$

Naturalmente, demostraremos que este es un subgrupo normal de $\mathcal{J}_k^{c_k}$ *y su cociente es donde podremos hacernos la vida más sencilla.*

Proposition 3.13. $H_k < \mathcal{J}_k^{c_k}(\mathbb{Z})$.

Demostración. Sean $\tilde{f}, \tilde{g} \in H_k$.
Por definición, sabemos que $\tilde{f} = x + \sum_{i=d_k}^{c_k-1} \alpha_i x^i + O(x^{c_k})$ y $\tilde{g} = x + \sum_{i=d_k}^{c_k-1} \beta_i x^i + O(x^{c_k})$, con $\alpha_i \equiv 0 \equiv \beta_i$ para todo i impar.
Sean $f, g \in \mathcal{J}_k(\mathbb{Z})$ tales que $f + O(x^{c_k}) = \tilde{f}$ y $g + O(x^{c_k}) = \tilde{g}$. Vemos que

$$f \circ g = f + g + R,$$

donde $R \in x^{2d_k-1}\mathbb{Z}[[x]]$. Notemos que $d_k \geqslant 2k+1$. Esto implica que

$$2d_k - 1 \geqslant 2(2k+1) - 1 = 4k+1 > c_k.$$

De esta manera, tenemos que

$$\tilde{f}\circ\tilde{g} = x + \sum_{i=2k}^{c_k-1}(\alpha_i+\beta_i)x^i + O(x^{c_k}).$$

Donde es claro que $\tilde{f}\circ\tilde{g}\in H_k$. Concluimos que $H_kH_k\subset H_k$.

Para verificar la clausura bajo inverso basta recordar que tomar inverso en $\mathcal{J}_k(\mathbb{Z})$ preserva niveles, tomar el producto antes descrito y notar que si $\alpha_i+\beta_i=0$, entonces en particular $\alpha_i\equiv\beta_i \pmod 2$.
La contención de la identidad es trivial. $\square$

Proposition 3.14. $H_k\triangleleft\mathcal{J}_k^{c_k}(\mathbb{Z})$.

Demostración. Sean $\tilde{f}\in\mathcal{J}_k^{c_k}(\mathbb{Z})$ y $\tilde{g}\in H_k$. Sean $f,g\in\mathcal{J}_k(\mathbb{Z})$ tales que $f+O(x^{c_k})=\tilde{f}$ y $g+O(x^{c_k})=\tilde{g}$. Vemos que

$$f\circ g\circ f^{-1} = [f,g]\circ g.$$

Por definición tenemos que $nvl(g)\geqslant d_k$. Además, sabemos que

$$nvl([f,g])\geqslant nvl(f)+nvl(g)-1.$$

Por un lado, si $nvl(f)\geqslant k+1$ o $nvl(g)\geqslant d_k+1$, entonces

$$nvl([f,g])\geqslant k+d_k=c_k.$$

Es decir, tendremos que $[\tilde{f},\tilde{g}]=x+O(x^{c_k})$. De esta manera $\tilde{f}\circ\tilde{g}\circ\tilde{f}^{-1}=\tilde{g}\in H_k$.
Si $k\equiv 1 \pmod 4$, entonces podemos aplicar el argumento anterior.
Por otro lado, si $k\not\equiv 1 \pmod 4, nvl(f)=k$ y $nvl(g)=d_k$, tenemos que $[\tilde{f},\tilde{g}]=x+(k-d_k)x^{c_k-1}+O(x^{c_k})$. De donde es claro que

$$\tilde{f}\circ\tilde{g}\circ\tilde{f}^{-1}=(x+(k-d_k)x^{c_k-1}+O(x^{c_k}))\circ g = g-(d_k-k)x^{c_k-1}+O(x^{c_k}).$$

Vemos que $d_k-k=c_k-2k$, por lo que $d_k-k\equiv c_k \pmod 2$. De esta manera, si $c_k-1\equiv 1 \pmod 2$, entonces $d_k-k\equiv 0 \pmod 2$. Esto implica que $\tilde{f}\circ\tilde{g}\circ\tilde{f}^{-1}\in H_k$.

Concluimos que $\tilde{f}H_k\tilde{f}^{-1}\subset H_k$. Dada la arbitrariedad de $\tilde{f}\in\mathcal{J}_k^{c_k}(\mathbb{Z})$, concluimos que H_k es normal. $\square$

Definiremos $\Gamma_k := \mathcal{J}_k^{c_k}(\mathbb{Z})/H_k$. Este es el grupo en donde podremos calcular con tranquilidad los cocientes como veremos en seguida.

Proposition 3.15. *$H_k \subset ker(\tilde{\pi})$.*

Demostración. Notemos que

$$H_k = \langle \{f_i + O(x^{c_k}) | d_k \leqslant i \leqslant c_k - 2, \text{ e } i \text{ par}\} \cup \{(f_i + O(x^{c_k}))^2 | d_k \leqslant i \leqslant c_k - 1, \text{ e } i \text{ impar}\}\rangle.$$

Más aún, vemos que

$$\begin{aligned} &\{f_i + O(x^{c_k}) | d_k \leqslant i \leqslant c_k - 2, \text{ e } i \text{ par}\} \\ =&\{f_i + O(x^{c_k}) | d_k \leqslant i \leqslant 2k + 2, \text{ e } i \text{ par}\} \cup \{f_{2i} + O(x^{c_k}) | k + 2 \leqslant i \leqslant \tfrac{c_k}{2} - 1\}. \end{aligned}$$

y

$$\begin{aligned} &\{(f_i + O(x^{c_k}))^2 | d_k \leqslant i \leqslant c_k - 1, \text{ e } i \text{ impar}\} \\ =&\{(f_i + O(x^{c_k}))^2 | d_k \leqslant i \leqslant 2k + 3, \text{ e } i \text{ impar}\} \cup \{(f_{2i+1} + O(x^{c_k}))^2 | k + 2 \leqslant i \leqslant \tfrac{c_k}{2} - 1\}. \end{aligned}$$

Dado que $\tilde{\pi} \circ p = \pi$, tendremos que $\pi(f_i) = \tilde{\pi}(f_i + O(x^{c_k}))$ para todo $i \geqslant k$. Por la proposición 3.5, esto implica que

$$\{f_{2i} + O(x^{c_k}) | k + 2 \leqslant i \leqslant \tfrac{c_k}{2} - 1\} \subset ker(\tilde{\pi}).$$

y

$$\{(f_{2i+1} + O(x^{c_k}))^2 | k + 2 \leqslant i \leqslant \tfrac{c_k}{2} - 1\} \subset ker(\tilde{\pi}).$$

Con esto, bastará demostrar que $\tilde{\pi}(f_i + O(x^{c_k})) = 0$ para todo $i \in \{d_k, \ldots, 2k + 2\}$ tal que i es par y $\tilde{\pi}(f_i + O(x^{c_k}))^2 = 0$ para todo $i \in \{d_k, \ldots, 2k + 3\}$ tal que i es impar. Para hacer esto habrá que considerar la clase de k módulo 4.

- Si $k \equiv 3 \pmod 4$, entonces $d_k = 2k + 1$ y ya sabemos que

  $$\tilde{\pi}(f_{2k+1} + O(x^{c_k}))^2 = 0 = \tilde{\pi}(f_{2k+3} + O(x^{c_k}))^2,$$

  por lo que bastará demostrar que $\tilde{\pi}(f_{2k+2}) = 0$. Para esto consideremos

  $$[f_{k+2}, f_{k+1}] = x + x^{2k+2} + C(k + 2, k + 1)x^{3k+3} + \cdots .$$

  Vemos que $f_{2k+2} \circ [f_{k+2}, f_{k+1}]^{-1} \in \mathcal{J}_{3k+3}(\mathbb{Z}) \subset \mathcal{J}_{c_k}(\mathbb{Z})$. Esto implica que

  $$\tilde{\pi}(f_{2k+2} + O(x^{c_k})) = \pi(f_{2k+2}) = 0.$$

- Si $k \equiv 2 \pmod 2$, entonces $d_k = 2k+2$ y ya sabemos que $\tilde{\pi}(f_{2k+3} + O(x^{c_k}))^2 = 0$. La demostración de que $\tilde{\pi}(f_{2k+2}) = 0$ es análoga a la anterior.

- Si $k \equiv 1 \pmod 4$, entonces $d_k = 2k+2$. Ya sabemos que $\tilde{\pi}(f_{2k+3} + O(x^{c_k}))^2 = 0$. Por otro lado, podemos aplicar el mismo argumento del caso de $k \equiv 3 \pmod 4$ para demostrar que $\pi(f_{2k+2}) = 0$.

- Si $k \equiv 0 \pmod 4$, entonces $d_k = 2k+4$ y no hay nada que demostrar.

Dado que sus generadores están en $ker(\tilde{\pi})$, concluimos que $H_k \subset ker(\tilde{\pi})$.

$\square$

Ahora basta aplicar el teorema del factor para ver que existe un único morfismo $\rho : \Gamma_k \to H_1(\mathcal{J}_k(\mathbb{Z}))$ tal que el siguiente diagrama conmuta:

$$\begin{tikzcd}
\mathcal{J}_k^{c_k}(\mathbb{Z}) \arrow[rr, "\tilde{\pi}"] \arrow[dr, "p'"'] & & H_1(\mathcal{J}_k(\mathbb{Z})) \\
& \Gamma_k \arrow[ur, "\rho"'] &
\end{tikzcd}$$

Más aún, podemos juntar este diagrama con el de la observación 2.23, para obtener el siguiente diagrama conmutativo:

$$\begin{tikzcd}
\mathcal{J}_k(\mathbb{Z}) \arrow[rr, "\pi"] \arrow[dr, "p' \circ p"'] & & H_1(\mathcal{J}_k(\mathbb{Z})) \\
& \Gamma_k \arrow[ur, "\rho"'] &
\end{tikzcd}$$

Esto, al igual que en secciones anteriores, nos permitirá calcular las clases en $H_1(\mathcal{J}_k(\mathbb{Z}))$ por medio de las imágenes de ρ. La ventaja que obtenemos en esta ocasión es que podremos describir de manera explícita al núcleo de ρ.

De ahora en adelante tendremos que fijar $k \geqslant 5$. La razón de esto es que, por obstrucciones técnicas no podemos dar una fórmula general para el producto en $\mathcal{J}_k^{c_k}(\mathbb{Z})$ para $k \in \{2, 3, 4, 5\}$. Dicha descripción general, junto con una descripción general del producto, inverso, y cierta versión del conmutador en Γ_k, se encuentran desarrolladas al final del apéndice, pues su demostración involucra cálculos y verificaciones que, a pesar de ser simples, *son engorrosos y no ofrecen mayores intuiciones sobre ninguno de los grupos que nos interesan, al menos ninguna más de la que la misma formula que se obtiene al final puede otorgar. El siguiente resultado es una descripción del conmutador en Γ_k por medio de las descripciones generales que se encuentran en el apéndice.*

Proposition 3.16. *Sean $f, g \in \Gamma_k$, con $f = p'(x + \sum_{i=k}^{c_k-1} \alpha_i x^i + O(x^{c_k}))$ y $g = p'(x + \sum_{i=k}^{c_k-1} \beta_i x^i + O(x^{c_k}))$.*

- *Si $k \equiv 3 \pmod 4$, entonces*

$$[f,g] = p'(x+(\alpha_{k+1}\beta_k-\alpha_k\beta_{k+1})x^{2k}+(\alpha_{k+1}\beta_k-\alpha_k\beta_{k+1})x^{3k}+O(x^{3k+1})).$$

- *Si $k \equiv 2 \pmod 4$, entonces*

$$\begin{aligned}[f,g] = p'(x &+ (\alpha_{k+1}\beta_k - \alpha_k\beta_{k+1})x^{2k} + 2(\alpha_{k+2}\beta_k - \alpha_k\beta_{k+2})x^{2k+1} \\ &+ (\alpha_{k+1}\beta_k - \alpha_k\beta_{k+1})x^{3k-1} + O(x^{3k+2})).\end{aligned}$$

- *Si $k \equiv 1 \pmod 4$, entonces*

$$\begin{aligned}[f,g] = p'(x &+ (\alpha_{k+1}\beta_k - \alpha_k\beta_{k+1})x^{2k} + 2(\alpha_{k+2}\beta_k - \alpha_k\beta_{k+2})x^{2k+1} \\ &+(3(\alpha_{k+3}\beta_k - \alpha_k\beta_{k+3}) + (\alpha_{k+2}\beta_{k+1} - \alpha_{k+1}\beta_{k+2}))x^{2k+2} \\ &+(\alpha_{k+2}\beta_k - \alpha_k\beta_{k+2})x^{3k} + O(x^{3k+1})).\end{aligned}$$

- *Si $k \equiv 0 \pmod 4$, entonces*

$$\begin{aligned}[f,g] = p'(x &+ (\alpha_{k+1}\beta_k - \alpha_k\beta_{k+1})x^{2k} + 2(\alpha_{k+2}\beta_k - \alpha_k\beta_{k+2})x^{2k+1} \\ &+(3(\alpha_{k+3}\beta_k - \alpha_k\beta_{k+3}) + (\alpha_{k+2}\beta_{k+1} - \alpha_{k+1}\beta_{k+2}))x^{2k+2} \\ &+(4(\alpha_{k+4}\beta_k - \alpha_k\beta_{k+4}) + 2(\alpha_{k+3}\beta_{k+1} - \alpha_{k+1}\beta_{k+3}))x^{2k+3} \\ &+(\alpha_{k+3}\beta_k - \beta_{k+3}\alpha_k)x^{3k+1} + (\alpha_{k+3}\beta_{k+1} - \beta_{k+3}\alpha_{k+1})x^{3k+3} + O(x^{3k+4})).\end{aligned}$$

Esta nueva fórmula nos permite calcular el subgrupo derivado de Γ_k:

Corollary 3.17. *Sea $k \geqslant 5$.*

a) *Si $k \equiv 3 \pmod 4$, entonces $[\Gamma_k, \Gamma_k] = \langle p'(x + x^{2k} + x^{3k} + O(x^{3k+1}))\rangle$.*

b) *Si $k \equiv 2 \pmod 4$, entonces*

$$[\Gamma_k, \Gamma_k] = \langle p'(x + x^{2k} + x^{3k-1} + O(x^{3k+2})), p'(x + 2x^{2k+1} + O(x^{3k+2}))\rangle.$$

c) *Si* $k \equiv 1 \pmod 4$*, entonces*

$$[\Gamma_k, \Gamma_k] = \langle p'(x + x^{2k} + O(x^{3k+1})), p'(x + 2x^{2k+1} + x^{3k} + O(x^{3k+1}))\rangle.$$

d) *Si* $k \equiv 0 \pmod 4$*, entonces*

$$\begin{aligned}[\Gamma_k, \Gamma_k] =&\langle p'(x + x^{2k} + O(x^{3k+4})), p'(x + 2x^{2k+1} + O(x^{3k+4})),\\ &p'(x + x^{2k+2} + O(x^{3k+4})), p'(x + x^{3k+1} + O(x^{3k+4})),\\ &p'(x + 4x^{2k+3} + O(x^{3k+4})), p'(x + 2x^{2k+3} + x^{3k+3} + O(x^{3k+4}))\rangle\end{aligned}$$

Demostración.

a) Vemos que

$$[p'(f_{k+1}+O(x^{3k+1})), p'(f_k+O(x^{3k+1}))] = p'(x+x^{2k}+x^{3k}+O(x^{3k+1})).$$

De esta manera, $\langle p'(x + x^{2k} + x^{3k} + O(x^{3k+1})\rangle \subseteq [\Gamma_k, \Gamma_k]$. Por otro lado, retomando la notación del corolario anterior, tenemos que

$$[f, g] = p'(x + x^{2k} + x^{3k} + O(x^{3k+1}))^{(-1)\alpha_k\beta_{k+1}+\alpha_{k+1}\beta_k}.$$

Es decir $[f, g] \in \langle p'(x+x^{2k}+x^{3k}+O(x^{3k+1})\rangle$ para todo $f, g \in \Gamma_k$. Esto implica que $[\Gamma_k, \Gamma_k]$ está contenido en $\langle p'(x + x^{2k} + x^{3k} + O(x^{3k+1})\rangle$, y por tanto, que son iguales.

b) Vemos que

$$[p'(f_{k+1}+O(x^{3k+2})), p'(f_k+O(x^{3k+2}))] = p'(x+x^{2k}+x^{3k-1}+O(x^{3k+2}))$$

y

$$[p'(f_{k+2} + O(x^{3k+2})), p'(f_k + O(x^{3k+2}))] = p'(x + 2x^{2k+1} + O(x^{3k+2})).$$

De esta manera, $\langle p'(x+x^{2k}+x^{3k}+O(x^{3k+2}), p'(x+2x^{2k+1}+O(x^{3k+2}))\rangle \subseteq [\Gamma_k, \Gamma_k]$. Por otro lado, retomando la notación del corolario anterior, tenemos que

$$\begin{aligned}[f, g] =&p'(x + x^{2k} + x^{3k-1} + O(x^{3k+2}))^{(-1)\alpha_k\beta_{k+1}+\alpha_{k+1}\beta_k}\\ &\circ p'(x + 2x^{2k+1} + O(x^{3k+2}))^{(-1)\alpha_k\beta_{k+2}+\alpha_{k+2}\beta_k}\end{aligned}$$

Es decir, $[f,g] \in \langle p'(x+x^{2k}+x^{3k}+O(x^{3k+2}), p'(x+2x^{2k+1}+O(x^{3k+2}))\rangle$ para todo $f,g \in \Gamma_k$. Esto implica que

$$[\Gamma_k, \Gamma_k] \subseteq \langle p'(x + x^{2k} + x^{3k} + O(x^{3k+2}), p'(x + 2x^{2k+1} + O(x^{3k+2}))\rangle$$

.

Concluimos la igualdad.

$c)$ Basta notar que

$$[p'(f_{k+1} + O(x^{3k+1})), p'(f_k + O(x^{3k+1}))] = p'(x + x^{2k} + O(x^{3k+1}))$$

y

$$[p'(f_{k+2}+O(x^{3k+1})), p'(f_k+O(x^{3k+1}))] = p'(x+2x^{2k+1}+x^{3k}+O(x^{3k+1})).$$

Desde este punto se sigue de manera análoga a los casos anteriores.

$d)$ Basta notar que

$$[p'(f_{k+1} + O(x^{3k+4})), p'(f_k + O(x^{3k+4}))] = p'(x + x^{2k} + O(x^{3k+4})),$$

$$[p'(f_{k+2} + O(x^{3k+4})), p'(f_k + O(x^{3k+4}))] = p'(x + 2x^{2k+1} + O(x^{3k+4})),$$

$$[p'(f_{k+2} + O(x^{3k+4})), p'(f_{k+1} + O(x^{3k+4}))] = p'(x + x^{2k+2} + O(x^{3k+4})),$$

$$[p'(f_{k+3} + O(x^{3k+4})), p'(f_k + O(x^{3k+4}))] \circ [p'(f_{k+2} + O(x^{3k+4})), p'(f_{k+1} + O(x^{3k+4}))]^{-3} = p'(x + x^{3k+4} + O(x^{3k+4})),$$

$$[p'(f_{k+4} + O(x^{3k+4})), p'(f_k + O(x^{3k+4}))] = p'(x + 4x^{2k+3} + O(x^{3k+4}))$$

y

$$[p'(f_{k+3}+O(x^{3k+4})), p'(f_{k+1}+O(x^{3k+4}))] = p'(x+2x^{2k+3}+x^{3k+3}+O(x^{3k+4})).$$

Desde este punto se sigue de manera análoga a los casos anteriores.

□

Con esto finalmente podemos determinar las relaciones de los generadores de $\pi(\mathcal{J}_{2k}(\mathbb{Z}))$.

Proposition 3.18. *Sea $k \geqslant 5$.*

a) *Si $k \equiv 3 \pmod 4$, entonces, para $i \in \{k, \ldots, \frac{3k-1}{2}\}$ se tiene que*

$$\pi(f_{2i+1}) \notin \left\langle \{\pi(f_{2j+1})\}_{j=k}^{\frac{3k-1}{2}} \setminus \{\pi(f_{2i+1})\} \right\rangle.$$

b) *Si $k \equiv 2 \pmod 4$, entonces $|\pi(f_{2k+1})| = 2$ y para $i \in \{k, \ldots, \frac{3k}{2}\}$ se tiene que*

$$\pi(f_{2i+1}) \notin \left\langle \{\pi(f_{2j+1})\}_{j=k}^{\frac{3k}{2}} \setminus \{\pi(f_{2i+1})\} \right\rangle.$$

c) *Si $k \equiv 1 \pmod 4$, entonces $\pi(f_{2k+1})^2 = \pi(f_{3k})$ y para $i \in \{k, \ldots, \frac{3k-3}{2}\}$ se tiene que*

$$\pi(f_{2i+1}) \notin \left\langle \{\pi(f_{2j+1})\}_{j=k}^{\frac{3k-3}{2}} \setminus \{\pi(f_{2i+1})\} \right\rangle.$$

d) *Si $k \equiv 0 \pmod 4$, entonces $\pi(f_{2k+3})^2 = \pi(f_{3k+3}), |\pi(f_{2k+1})| = 2, \pi(f_{3k+1}) = 0$ y para $i \in \{k, \ldots, \frac{3k-2}{2}\}$ se tiene que*

$$\pi(f_{2i+1}) \notin \left\langle \{\pi(f_{2j+1})\}_{j=k}^{\frac{3k-2}{2}} \setminus \{\pi(f_{2i+1})\} \right\rangle.$$

Demostración. Recordemos que, para $f \in \mathcal{J}_k(\mathbb{Z})$, se tiene que $\pi(f) = \rho \circ p'(f + O(x^{c_k}))$.

a) Sea $i \in \{k, \ldots, \frac{3k-1}{2}\}$. Por definición tenemos que

$$\pi(f_{2i+1}) \in \left\langle \{\pi(f_{2j+1})\}_{j=k}^{\frac{3k-1}{2}} \setminus \{\pi(f_{2i+1})\} \right\rangle.$$

si y solo si existe para todo $j \in \{k, \ldots, \frac{3k-1}{2}\} \setminus \{i\}$ existe $\epsilon_j \in \{0, 1\}$ tal que

$$\pi(f_{2i+1}) = \prod_{\substack{k\leqslant j\leqslant \frac{3k-1}{2}\\ j\neq i}} \pi(f_{2j+1})^{\epsilon_j} = \pi\left(x + \sum_{\substack{k\leqslant j\leqslant \frac{3k-1}{2}\\ j\neq i}} \epsilon_j x^{2j+1}\right).$$

Esta igualdad se cumple si y solo si existe $g \in [\Gamma_k, \Gamma_k]$ tal que

$$p'(f_{2i+1} + O(x^{3k+1}))g = p'\left(x + \sum_{\substack{k\leqslant j\leqslant \frac{3k-1}{2}\\ j\neq i}} \epsilon_j x^{2j+1} + O(x^{3k+1})\right).$$

Por el corolario anterior tenemos que existe $\alpha \in \mathbb{Z}$ tal que $g = p'(x + x^{2k} + x^{3k} + O(x^{3k+1}))^{\alpha}$, es decir, $g = p'(x + \alpha x^{2k} + \alpha x^{3k} + O(x^{3k+1}))$. De esta manera, la última igualdad se cumple si y solo si existe $\alpha \in \mathbb{Z}$ tal que

$$p'(x+\alpha x^{2k}+x^{2i+1}+\alpha x^{3k}+O(x^{3k+1})) = p'\left(x + \sum_{\substack{k\leqslant j\leqslant \frac{3k-1}{2}\\ j\neq i}} \epsilon_j x^{2j+1} + O(x^{3k+1})\right).$$

Dado que las preimagenes en $\mathcal{J}_k^{c_k}(\mathbb{Z})$ de estos elementos solo pueden diferir desde el $(2k+1)-$ésimo coeficiente, tenemos que la igualdad anterior se cumple si y solo si existe $h = \sum_{l=2k+1}^{3k} \beta_l x^l$ tal que $l \equiv 1 \pmod 2$ implica que $\beta_l \equiv 0 \pmod 2$ y

$$x+\alpha x^{2k}+x^{2i+1}+\alpha x^{3k}+h+O(x^{3k+1}) = x+\sum_{\substack{k\leqslant j\leqslant \frac{3k-1}{2}\\ j\neq i}} \epsilon_j x^{2j+1}+O(x^{3k+1}).$$

Esto ocurre si y solo si $\alpha = 0$, de donde

$$x + x^{2i+1} + h + O(x^{3k+1}) = x + \sum_{\substack{k\leqslant j\leqslant \frac{3k-1}{2}\\ j\neq i}} \epsilon_j x^{2j+1} + O(x^{3k+1}).$$

Vemos que el $(2i+1)-$ésimo coeficiente del lado izquierdo de la igualdad es impar. Por otro lado el $(2i+1)-$ésimo coeficiente del lado derecho es nulo, por lo que es par. Esto es una contradicción.

b) Notemos que $\pi(f_{2k+1})^2 = \pi(x+2x^{2k+1}) = \rho\circ p'(x+2x^{2k+1}+O(x^{3k+2})) = 0$. El resto de la demostración es análoga al caso anterior.

c) Notemos que

$$\pi(f_{2k+1})^2 = \pi(x + 2x^{2k+1}) = \rho \circ p'(x + 2x^{2k+1} + O(x^{3k+1})).$$

Por otro lado, vemos que

$$p'(x+2x^{2k+1}+O(x^{3k+1})) = p'(x+x^{3k}+O(x^{3k+1}))p'(x+2x^{2k+1}+x^{3k}+O(x^{3k+1})).$$

De esta manera

$$\pi(f_{2k+1})^2 = \rho\circ p'(x+2x^{2k+1}+O(x^{3k+1})) = \rho\circ p'(x+x^{3k}+O(x^{3k+1})) = \pi(f_{3k}).$$

El resto de la demostración es análoga a los casos anteriores.

d) Notemos que

$$\pi(f_{3k+1}) = \rho \circ p'(x + x^{3k+1} + O(x^{3k+3})) = 0.$$

El resto de la demostración es análoga a los casos anteriores.

□

Notar que este último resultado implica en particular que, salvo los elementos explícitamente mencionados, ninguno está en la clase de 0.

Finalmente podemos calcular la torsión de $H_1(\mathcal{J}_k(\mathbb{Z}))$. Con todos los resultados desarrollados, esto se vuelve una serie de observaciones.

Theorem 3.19. *Sea $k \geqslant 5$.*

a) *Si* $k \equiv 3 \pmod 4$, *entonces* $T(H_1(\mathcal{J}_k(\mathbb{Z}))) \cong (\mathbb{Z}/2\mathbb{Z})^{\frac{k+1}{2}}$.

b) *Si* $k \equiv 2 \pmod 4$, *entonces* $T(H_1(\mathcal{J}_k(\mathbb{Z}))) \cong (\mathbb{Z}/2\mathbb{Z})^{\frac{k+2}{2}}$.

c) *Si* $k \equiv 1 \pmod 4$, *entonces* $T(H_1(\mathcal{J}_k(\mathbb{Z}))) \cong \mathbb{Z}/4\mathbb{Z} \bigoplus (\mathbb{Z}/2\mathbb{Z})^{\frac{k-3}{2}}$.

d) *Si* $k \equiv 0 \pmod 4$, *entonces* $T(H_1(\mathcal{J}_k(\mathbb{Z}))) \cong \mathbb{Z}/4\mathbb{Z} \bigoplus (\mathbb{Z}/2\mathbb{Z})^{\frac{k-2}{2}}$.

Demostración. Recordemos que $T(H_1(\mathcal{J}_k(\mathbb{Z}))) = \pi(\mathcal{J}_{2k}(\mathbb{Z}))$.

a) Sabemos que $\pi(\mathcal{J}_{2k}(\mathbb{Z})) = \langle \pi(f_{2i+1}) | k \leqslant i \leqslant \frac{3k-1}{2} \rangle$. Definimos

$$\begin{aligned} \omega_k : \langle a_1, \dots a_{\frac{k+1}{2}} | {a_i}^2, [a_i, a_j] \rangle &\to \pi(\mathcal{J}_{2k}(\mathbb{Z})) \\ a_i &\mapsto \pi(f_{2(i+k-1)+1}). \end{aligned}$$

Por el corolario anterior sabemos que $|\pi(f_{2i+1})| = 2$ para todo $i \in \{k, \dots, \frac{3k-1}{2}\}$, y dado que $\pi(\mathcal{J}_{2k}(\mathbb{Z}))$ es abeliano, tenemos que la asignación está bien definida y es un morfismo. Este morfismo es claramente sobreyectivo. Por otro lado, si $g \in ker(\omega)$ es distinto de la identidad, tendremos que para todo $i \in \{1, \dots, \frac{k+1}{2}\}$ existe $\epsilon_i \in \{0, 1\}$ tal que

$$g = \prod_{i=1}^{\frac{k+1}{2}} a_i^{\epsilon_i}$$

y existe $j \in \{1, \dots \frac{k+1}{2}\}$ tal que $\epsilon_j = 1$. Esto implica que

$$0 = \pi(f_{2j+1}) \prod_{\substack{1 \leqslant i \leq \frac{k+1}{2} \\ i \neq j}} \pi(f_{2j+1})^{\epsilon_i}.$$

Esto es una contradicción con el corolario anterior. Concluimos que $ker(\omega) = 0$, y por lo tanto que

$$\pi(\mathcal{J}_{2k}(\mathbb{Z})) \cong \langle a_1, \dots a_{\frac{k+1}{2}} | {a_i}^2, [a_i, a_j] \rangle \cong (\mathbb{Z}/2\mathbb{Z})^{\frac{k+1}{2}}.$$

b) Sabemos que $\pi(\mathcal{J}_{2k}(\mathbb{Z})) = \langle \pi(f_{2i+1}) | k \leqslant i \leqslant \frac{3k}{2} \rangle$. Definimos

$$\begin{aligned} \omega_k : \langle a_1 \to a_{\frac{k+2}{2}} | {a_i}^2, [a_i, a_j] \rangle &\to \pi(\mathcal{J}_{2k}(\mathbb{Z})) \\ a_i &\mapsto \pi(f_{2(i+k-1)+1}). \end{aligned}$$

El resto de la demostración es análoga al caso anterior.

c) Sabemos que $\pi(\mathcal{J}_{2k}(\mathbb{Z})) = \langle \pi(f_{2i+1}) | k \leqslant i \leqslant \frac{3k-3}{2} \rangle$. Definimos

$$\begin{aligned} \omega_k : \langle b, a_1, \ldots, a_{\frac{k-3}{2}} | b^4, {a_i}^2, [a_i, a_j], [b, a_i] \rangle &\to \pi(\mathcal{J}_{2k}(\mathbb{Z})) \\ b &\mapsto \pi(f_{2k+1}) \\ a_i &\mapsto \pi(f_{2(i+k)+1}). \end{aligned}$$

El resto de la demostración es análoga al caso anterior.

d) Sabemos que $\pi(\mathcal{J}_{2k}(\mathbb{Z})) = \langle \pi(f_{2i+1}) | k \leqslant i \leqslant \frac{3k-2}{2} \rangle$. Definimos

$$\begin{aligned} \omega_k : \langle b, a_1, \ldots, a_{\frac{k-2}{2}} | b^4, {a_i}^2, [a_i, a_j], [b, a_i] \rangle &\to \pi(\mathcal{J}_{2k}(\mathbb{Z})) \\ a_1 &\mapsto \pi(f_{2k+1}) \\ b &\mapsto \pi(f_{2k+3}) \\ a_i &\mapsto \pi(f_{2(i+k)+1}) \text{ para } i \geqslant 2. \end{aligned}$$

El resto de la demostración es análoga al caso anterior.

$\square$

3.3 Libertad

Solo nos queda calcular la parte libre de $H_1(\mathcal{J}_k(\mathbb{Z}))$. Por suerte, esto no requiere de un estudio tan extenso de la estructura de $H_1(\mathcal{J}_k(\mathbb{Z}))$ como fue el caso de la torsión, si no de solo un par de observaciones y definir correctamente un morfismo. Más aún, podemos volver a fijar $k \geqslant 2$, pues no habrá ninguna restricción técnica para esto.

Sabemos que $[\mathcal{J}_k(\mathbb{Z}), \mathcal{J}_k(\mathbb{Z})] \subset \mathcal{J}_{2k}(\mathbb{Z})$. Por el teorema del factor, esto implica que el siguiente diagrama es conmutativo:

$$\begin{tikzcd} \mathcal{J}_k(\mathbb{Z}) \arrow[rr, "p"] \arrow[dr, "\pi"'] & & \mathcal{J}_k^{2k}(\mathbb{Z}) \\ & H_1(\mathcal{J}_k(\mathbb{Z})) \arrow[ur, "\varphi"'] & \end{tikzcd}$$

El morfismo φ es sobreyectivo pues p lo es, y claramente su núcleo es $\pi(\mathcal{J}_{2k}(\mathbb{Z}))$. También sabemos que $\pi(\mathcal{J}_{2k}(\mathbb{Z})) = T(H_1(\mathbb{Z}))$. Así, por el primer teorema de isomorfía se tiene que

$$H_1(\mathcal{J}_k(\mathbb{Z}))/T(H_1(\mathcal{J}_k(\mathbb{Z}))) \cong \mathcal{J}_k^{2k}(\mathbb{Z}).$$

Es decir, la parte libre $H_1(\mathcal{J}_k(\mathbb{Z}))$ es isomorfa a dicho cociente, por lo que bastará identificarlo con algún grupo conocido para terminar. Como ya mencionamos antes, esto es suficientemente sencillo.

Proposition 3.20. *El cociente $\mathcal{J}_k^{2k}(\mathbb{Z})$ es isomorfo a $\mathbb{Z}^k$.*

Demostración. Construiremos un isomorfismo entre ambos grupos.
Sean $f, g \in \mathcal{J}_k^{2k}(\mathbb{Z})$, con $f = x + \sum_{i=k}^{2k-1} \alpha_i x^i + O(x^{2k-1})$ y $g = x + \sum_{i=k}^{2k-1} \beta_i x^i + O(x^{2k})$. Gracias a la primera formula de 2.1 vemos que

$$f \circ g = x + \sum_{i=k}^{2k-2} (\alpha_i + \beta_i)x^i + (\alpha_{2k-1} + \beta_{2k-1} + k\alpha_k\beta_k)x^{2k-1} + O(x^{2k}).$$

Esto describe el producto en $\mathcal{J}_k^{2k}(\mathbb{Z})$.

Por otro lado, definimos $\psi : \mathcal{J}_k^{2k}(\mathbb{Z}) \to \mathbb{Z}^{k-1} \bigoplus \mathbb{Z}$ como

$$\psi\left(x + \sum_{i=k}^{2k-1} \alpha_i x^i + O(x^{2k})\right) = (\alpha_i)_{i=k}^{2k-2} \oplus (k{\alpha_k}^2 - 2\alpha_{2k-1}).$$

Vemos que es un morfismo de grupos pues en las primeras coordenadas es solo la proyección, mientras que en la ultima se tiene

$$k(\alpha_k + \beta_k)^2 - 2(\alpha_{2k-1} + \beta_{2k-1} + k\alpha_k\beta_k) = k{\alpha_k}^2 - 2\alpha_{2k-1} + k{\beta_k}^2 - 2\beta_{2k-1}.$$

Notemos que $\psi(x + \sum_{i=k}^{2k-1} \alpha_i x^i) = 0$ si y solo si $\alpha_{2k-1} = \frac{k}{2}{\alpha_k}^2$ y $\alpha_i = 0$ para todo $i \in \{k, \ldots, 2k-2\}$. La segunda condición implica que, en particular $\alpha_k = 0$, así que, si se cumplen ambas condiciones, entonces $\alpha_{2k-1} = 0$. Es decir, estas dos condiciones implican que $\alpha_i = 0$ para todo $i \in \{k, \ldots, 2k-1\}$. De esta manera se tiene que $ker(\psi) = \{x + O(x^{2k})\}$.
Sea $x = (n_1, \ldots, n_k) \in \mathbb{Z}^k$. Vemos que $n_k = k{n_1}^2 - \tilde{n}$. Más aun, existen $n \in \mathbb{Z}$ y $\epsilon \in \{0, -1\}$ tales que $\tilde{n} = 2n + \epsilon$. De esta manera tendremos $x = (n_1, \ldots n_{k-1}, k{\alpha_k}^2 - 2n) + (0, \ldots, 0, -\epsilon)$. Esto implica que

$$\mathbb{Z}^k/\psi(\mathcal{J}_k^{2k}(\mathbb{Z})) \cong \mathbb{Z}/2\mathbb{Z}.$$

Es decir $\psi(\mathcal{J}_k^{2k}(\mathbb{Z}))$ es de índice finito en $\mathbb{Z}^k$, por lo que son isomorfos. Concluimos que $\mathcal{J}_k^{2k}(\mathbb{Z}) \cong \psi(\mathcal{J}_k^{2k}(\mathbb{Z})) \cong \mathbb{Z}^k$. $\square$

Cabe mencionar que el morfismo

$$x + \sum_{i \geqslant k} \alpha_i x^i \mapsto k{\alpha_k}^2 - 2\alpha_{2k-1}$$

es conocido como Resad$_k$. Más sobre este morfismo puede ser encontrado en el trabajo de H. Eynard-Bontemps y A. Navas en [6].

Finalmente, solo basta juntar esta proposición con el teorema 3.19 para demostrar el teorema 1.2.

Capítulo 4

Apéndice

4.1 Operaciones de series formales

Se dará la demostración de dos resultados importantes para establecer el grupo de Jennings.

Proposition 4.1. *La operación*

$$\begin{aligned} \circ : xR[[x]] \times xR[[x]] &\to xR[[x]] \\ \left(\sum_{i \geqslant 1} \alpha_i x^i, \sum_{i \geqslant 1} \beta_i x^i \right) &\mapsto \sum_{i \geqslant 1} \alpha_i \left(\sum_{j \geqslant 1} \beta_j x^j \right)^i \end{aligned}$$

está bien definida.

Demostración. Sean $f, g \in xR[[x]]$. Basta hacer el cómputo directo:

$$\begin{aligned}
f \circ g =& \alpha_1 g + \sum_{i \geqslant 2} \alpha_i g^i \\
=& \alpha_1 g + \sum_{i \geqslant 2} \alpha_i (\sum_{j \geqslant 1} \beta_j x^j)^i \\
=& \alpha_1 g + \sum_{i \geqslant 2} \alpha_i (\beta_1 x + \sum_{j \geqslant 2} \beta_j x^j)^i \\
=& \alpha_1 g + \sum_{i \geqslant 2} \alpha_i \sum_{l=0}^{i} \binom{i}{l} (\beta_1 x)^{i-l} \left(\sum_{j \geqslant 2} \beta_j x^j \right)^l \\
=& \alpha_1 g + \sum_{i \geqslant 2} \alpha_i \left((\beta_1 x)^i + \sum_{l=1}^{i} \binom{i}{l} (\beta_1 x)^{i-l} \left(\sum_{j \geqslant 2} \beta_j x^j \right)^l \right) \\
=& \alpha_1 g + \sum_{i \geqslant 2} \alpha_i (\beta_1)^i x^i + \sum_{i \geqslant 2} \alpha_i \left(\sum_{l=1}^{i} \binom{i}{l} (\beta_1 x)^{i-l} \left(\sum_{j \geqslant 2} \beta_j x^j \right)^l \right)
\end{aligned}$$

Notemos que $\alpha_1 g$ y $\sum_{i \geqslant 2} \alpha_i (\beta_1)^i x^i$ son elementos de $xR[[x]]$. Por otro lado, reordenando obtendremos que para todo $i \geqslant 3$ existe un polinomio $\phi_i \in R[x_1, \ldots, x_{2(i-1)}]$ tal que

$$\sum_{i \geqslant 2} \alpha_i \left(\sum_{l=1}^{i} \binom{i}{l} (\beta_1 x)^{i-l} \left(\sum_{i \geqslant 2} \beta_i x^j \right)^l \right) = \sum_{i \geqslant 3} \phi_i(\alpha_1, \ldots, \alpha_{i-1}, \beta_1, \ldots, \beta_{i-1}) x^i$$

de donde tenemos que $f \circ g$ se expresa como la suma de tres elementos de $xR[[x]]$, por lo que $f \circ g \in xR[[x]]$. $\square$

Corollary 4.2. *Sean $f, g \in xR[[x]]$, con $f = \sum_{i \geqslant 1} \alpha_i x^i$ y $g = \sum_{i \geqslant 1} \beta_i x^i$. Si γ_i es el $i-$ésimo coeficiente de $f \circ g$. Entonces*

$$\gamma_i = \begin{cases} \alpha_1 \beta_1 & si\ i = 1 \\ \alpha_2 {\beta_1}^2 + \beta_2 \alpha_1 & si\ i = 2 \\ \alpha_i (\beta_1)^i + \beta_i \alpha_1 + \phi_i(\alpha_1, \ldots, \alpha_{i-1}, \beta_1, \ldots, \beta_{i-1}) & si\ i \geqslant 3 \end{cases}$$

Proposition 4.3. *Sea $f \in xR[[x]]$, con $f = \sum_{i \geqslant 1} \alpha_i x^i$. Entonces existe $g \in R[[x]]$ tal que $f \circ g = x = g \circ f$ si y solo si $\alpha_1 \in R^*$.*

Demostración. Por un lado, si existe $g = \sum_{i\geqslant 1} \beta_i x^i$ tal que $f \circ g = x$, entonces por el corolario anterior tenemos que $\alpha_1\beta_1 = 1$. Esto implica que $\alpha_1 \in R^*$.

Por otro lado, si $\alpha_1 \in R^*$, entonces podemos definir

$$\beta_i = \begin{cases} \alpha_1^{-1} & \text{si } i = 1 \\ -\alpha_2(\alpha_1)^{-3} & \text{si } i = 2 \\ -(\alpha_1)^{-1}(\alpha_i(\alpha_1)^{-i} + \phi_i(\alpha_1, \ldots, \alpha_{i-1}, \beta_1, \ldots, \beta_{i-1})) & \text{si } i \geqslant 3 \end{cases}$$

y considerar $g := \sum_{i\geqslant 1} \beta_i x^i$. Una evaluación directa verifica que $f \circ g = x = g \circ f$.

□

Proposition 4.4. *$\mathcal{J}(R) \lhd \widetilde{\mathcal{J}(R)}$ y $\widetilde{\mathcal{J}(R)}/\mathcal{J}(R) \cong R^*$.*

Demostración. Consideremos

$$\begin{aligned} \varphi : \widetilde{\mathcal{J}(R)} &\to R^* \\ \sum_{i\geqslant 1} \alpha_i x^i &\mapsto \alpha_1 \end{aligned}$$

Vemos que esta función está bien definida y es un morfismo de grupos. Más aún, notemos que $ker(\varphi) = \mathcal{J}(R)$, por lo que este es un subgrupo normal de $\widetilde{\mathcal{J}(R)}$. Finalmente, es claro que φ es sobreyectiva, así que por el primer teorema de isomorfia concluimos que $\widetilde{\mathcal{J}(R)}/\mathcal{J}(R) \cong R^*$. □

4.2 Grupos con topología

Los objetos centrales de esta tesis son grupos topológicos, por lo que es sensato dar las definiciones y resultados correspondientes para discutir y desarrollar el estudio de estos.

Definition 4.5. Un grupo topológico G es un conjunto con estructuras de grupo y espacio topológico tales que las funciones

$$\begin{aligned} m : G \times G &\to G \\ (f, g) &\mapsto f \circ g \end{aligned} \qquad\qquad \begin{aligned} inv : G &\to G \\ g &\mapsto g^{-1} \end{aligned}$$

son continuas.

Todo grupo que no sea declarado como grupo topológico será asumido como grupo topológico discreto.

Observación 4.6. *Sean G un grupo topológico y $g \in G$. Las funciones*

$$\begin{aligned} L_g : G &\to G & \qquad R_g : G &\to G & \qquad K_g : G &\to G \\ x &\mapsto gx & x &\mapsto xg & x &\mapsto gxg^{-1} \end{aligned}$$

son homeomorfismos.

Siendo nuestro objetivo abelianizar grupos topológicos, tendremos que definir en que consiste cocientar en este contexto.

Proposition 4.7. *Sea G un grupo topológico y $N \trianglelefteq G$. El grupo G/N con la topología cociente que induce la proyección canónica es un grupo topológico.*

Intentar abelianizar solo cocientando por el subgrupo $\langle [g,h] | g,h \in G \rangle$ puede traernos problemas a la hora de intentar replicar las propiedades que debería cumplir. Es por esto que se define lo siguiente:

Definition 4.8. Sea G un grupo topológico. Definimos $[G,G]$ como la clausura de $\langle [g,h] | g,h \in G \rangle$.

A priori no tenemos ningún derecho a cocientar por este subconjunto, pues ni siquiera es claro que es un subgrupo de G. Aclararemos la situación enseguida.

Proposition 4.9. *Sea G un grupo topológico. Si $H \leq G$, entonces $\overline{H} \leq G$.*

Demostración. Primero, por definición tenemos la contención $e_G \in H \subset \overline{H}$. Por otro lado, por definición tenemos la cadena de contenciones

$$H^{-1}H \subset H \subset \overline{H}.$$

Esto implica que $\overline{H^{-1}H} \subset H \subset \overline{H}$. Notemos que

$$\overline{H^{-1}H} = \overline{m(H^{-1} \times H)} \supseteq m(\overline{H^{-1} \times H}) = m(\overline{H^{-1}} \times \overline{H}) = \overline{H^{-1}}\,\overline{H}.$$

Finalmente, vemos que $inv^2 = id_G$, por lo que inv es un homeomorfismo. Esto implica que $\overline{H^{-1}} = \overline{H}^{-1}$. Concluimos que

$$\overline{H}^{-1}\overline{H} \subseteq \overline{H^{-1}H} \subseteq \overline{H}.$$

Y por lo tanto $\overline{H} \leq G$. $\square$

Proposition 4.10. *Sea G un grupo topológico. Si $N \trianglelefteq G$, entonces $\overline{N} \trianglelefteq G$.*

Demostración. Notemos que para todo $g \in G$ se tiene que

$$\begin{aligned} K_g : G &\to G \\ h &\mapsto ghg^{-1} \end{aligned}$$

es continua. Por definición $K_g(N) \subseteq N$ para todo $g \in G$. Así que $g\overline{N}g^{-1} = K_g(\overline{N}) \subseteq \overline{K_g(N)} \subseteq \overline{N}$ para todo $g \in G$. Es decir $\overline{N} \trianglelefteq G$. $\square$

Con esto ya es claro que $[G, G] \trianglelefteq G$.

Observación 4.11. *Sea G un grupo topológico. El grupo $H_1(G) := G/[G, G]$ es abeliano.*

Finalmente, daremos un criterio para determinar cuando un grupo cociente es discreto, pues trabajar con grupos discretos nos ayudará a simplificar buena parte de nuestro trabajo.

Proposition 4.12. *Sea G un grupo topológico y $N \trianglelefteq G$. Entonces son equivalentes:*

a) *G/N es discreto.*

b) *$\{e_{G/N}\}$ es abierto en G/N.*

c) *N es abierto en G.*

Demostración. Demostraremos que *a*) implica *b*), que *b*) implica *a*) y que *b*) es equivalente a *c*).

Primero, si G/N es discreto, entonces $\{x\}$ es abierto para todo $x \in G/N$, por lo que, en particular $\{e_{G/N}\}$ es abierto.
Sea $g \in G/N$, notemos que $\{g\} = L_g(\{e_{G/N}\})$. Siendo L_g un homeomorfismo, si $\{e_{G/N}\}$ es abierto, entonces $\{g\}$ es abierto. Siendo $g \in G/N$ arbitrario, concluimos que si $\{e_{G/N}\}$ es abierto, entonces $\{g\}$ es abierto para todo $g \in G/N$, es decir, G/N es discreto.
Sea $A \subset G$, vemos que

$$p^{-1}(p(A)) = AN = \bigcup_{a \in A} L_a(N).$$

En particular

$$p^{-1}(\{e_{G/N}\}) = p^{-1}(p(N)) = N,$$

pues $N = e_G N$. Además, por definición sabemos que $U \subset G/N$ es abierto si y solo si $p^{-1}(U)$ es abierto en G. De esta manera tendremos que $N = p^{-1}(\{e_{G/N}\})$ es abierto si y solo si $\{e_{G/N}\}$ es abierto en G/N. $\square$

4.3 El producto en un cociente

En esta sección se da una descripción del producto en el grupo $\mathcal{J}_k^{c_k}(\mathbb{Z})$, para $k \geqslant 5$, junto con una descripción del producto, inverso y conmutador en Γ_k. Dichas descripciones se encuentra al final de la sección.

Sean $f, g \in \mathcal{J}_k^{c_k}(\mathbb{Z})$, con $f = x+\sum_{i=k}^{c_k-1} \alpha_i x^i + O(x^{c_k})$ y $g = x+\sum_{i=k}^{c_k-1} \beta_i x^i + O(x^{c_k})$. Como sabemos $f \circ g = x+\sum_{i=k}^{c_k-1} \beta_i x^i+\sum_{i=k}^{c_k-1} \alpha_i (x+\sum_{j=k}^{c_k-1} \beta_j x^j)^i + O(x^{c_k})$. Para poder escribir $f \circ g$ de una manera ordenada, utilizaremos el teorema multinomial. Para enunciarlo cómodamente tendremos que dar las siguientes definiciones.

Definition 4.13. Sea $v \in (\mathbb{Z}_{\geqslant 0})^m$. Sea $i \in \{1, \dots, m\}$. Escribiremos v_i para referirnos a la $i-$ésima coordenada de v.

Definition 4.14. Sea $v \in (\mathbb{Z}_{\geqslant 0})^m$. Definimos $|v| := \sum_{i=1}^m v_i$.

Definition 4.15. Sea $n \in \mathbb{Z}_{\geqslant 0}$. Sea $v \in (\mathbb{Z}_{\geqslant 0})^m$ tal que $|v| = n$. Se define el número

$$\binom{n}{v} := \frac{n!}{\prod_{i=1}^n v_i!}.$$

Theorem 4.16 (Teorema Multinomial.)**.** *Sea R un anillo conmutativo con unidad. Sean $m, n \in \mathbb{Z}_{\geqslant 0}$ y $\{\alpha_i\}_{i=1}^m \subset R$. Entonces*

$$\left(\sum_{i=1}^m \alpha_i\right)^n = \sum_{\substack{v \in (\mathbb{Z}_{\geqslant 0})^m \\ |v|=n}} \binom{n}{v} \prod_{i=1}^m (\alpha_i)^{v_i}.$$

Para adaptarlo a una versión más adecuada para nuestro caso, notemos que un elemento de $\mathcal{J}_k^{c_k}(\mathbb{Z})$ tiene $c_k - k + 1$ sumandos. Denotaremos $m_k := c_k - k + 1$. Fijaremos $w^k \in (\mathbb{Z}_{\geqslant 0})^{m_k}$ como $(w^k)_1 = 1$ y $(w^k)_i = k + (i-2)$ para $i \in \{2, \dots, m_k\}$. Sean $v, w \in (\mathbb{Z}_{\geqslant 0})^m$, definimos $v \cdot w = \sum_{i=1}^m v_i w_i$. Dado que las operaciones para calcular el producto de $\mathcal{J}_k(\mathbb{Z})/\mathcal{J}_{c_k}(\mathbb{Z})$ son las de $\mathbb{Z}[[x]]/x^{c_k}\mathbb{Z}[[x]]$, tendremos que si en el producto de los sumandos aparece una potencia de x mayor que c_k. entonces ese termino desaparece. Con esto en mente definimos $S_{n,k} := \{v \in (\mathbb{Z}_{\geqslant 0})^{m_k} | v \cdot w^k < c_k \text{ y } |v| = n\}$. Podemos reescribir $f \circ g$ de la siguiente manera:

Corollary 4.17. *Sean $f, g \in \mathcal{J}_k(\mathbb{Z})/\mathcal{J}_{c_k}(\mathbb{Z})$, con $f = x + \sum_{i=k}^{c_k-1} \alpha_i x^i + O(x^{c_k})$ y $g = x + \sum_{i=k}^{c_k-1} \beta_i x^i + O(x^{c_k})$. Entonces*

$$f \circ g = x + \sum_{i=k}^{c_k-1} \beta_i x^i + \sum_{l=k}^{c_k-1} \alpha_l \sum_{v \in S_{l,k}} \binom{l}{v} \left(\prod_{i=k}^{c_k-1} (\beta_i)^{v_{i-k+2}} \right) x^{v \cdot w^k} + O(x^{c_k}).$$

Analizaremos el conjunto $S_{l,k}$ para $l \geqslant k$, pues su comportamiento nos indicara que monomios pueden aparecer en los coeficientes del producto $f \circ g$.

Demostración. Tenemos que

$$f \circ g = x + \sum_{i=k}^{c_k-1} \beta_i x^i + \sum_{i=k}^{c_k-1} \alpha_i \left(x + \sum_{j=k}^{c_k-1} \beta_j x^j \right)^i + O(x^{c_k}).$$

Por el teorema multinomial sabemos que, dado $l \geqslant k$, se tiene

$$\begin{aligned}
\left(x + \sum_{j=k}^{c_k-1} \beta_j x^j \right)^l &= \sum_{\substack{v \in (\mathbb{Z}_{0\geqslant})^{m_k} \\ |v|=l}} \binom{l}{v} x^{v_1} \prod_{j=k}^{c_k-1} (\beta_j x^j)^{v_{j-k+2}} \\
&= \sum_{\substack{v \in (\mathbb{Z}_{0\geqslant})^{m_k} \\ |v|=l}} \binom{l}{v} \prod_{j=k}^{c_k-1} (\beta_j)^{v_{j-k+2}} x^{v_1} \prod_{j=k}^{c_k-1} (x^j)^{v_{j-k+2}} \\
&= \sum_{\substack{v \in (\mathbb{Z}_{0\geqslant})^{m_k} \\ |v|=l}} \binom{l}{v} \prod_{j=k}^{c_k-1} (\beta_j)^{v_{j-k+2}} x^{v_1} \prod_{i=2}^{m_k} (x^{k+(i-2)})^{v_i} \\
&= \sum_{\substack{v \in (\mathbb{Z}_{0\geqslant})^{m_k} \\ |v|=l}} \binom{l}{v} \prod_{j=k}^{c_k-1} (\beta_j)^{v_{j-k+2}} x^{v_1} \prod_{i=2}^{m_k} (x^{(w^k)_i})^{v_i} \\
&= \sum_{\substack{v \in (\mathbb{Z}_{0\geqslant})^{m_k} \\ |v|=l}} \binom{l}{v} \prod_{j=k}^{c_k-1} (\beta_j)^{v_{j-k+2}} x^{v_1} \prod_{i=2}^{m_k} x^{(w^k)_i v_i} \\
&= \sum_{\substack{v \in (\mathbb{Z}_{0\geqslant})^{m_k} \\ |v|=l}} \binom{l}{v} \prod_{j=k}^{c_k-1} (\beta_j)^{v_{j-k+2}} \prod_{i=1}^{m_k} x^{(w^k)_i v_i}
\end{aligned}$$

$$= \sum_{\substack{v\in(\mathbb{Z}_{0\geqslant})^{m_k}\\ |v|=l}} \binom{l}{v} \prod_{j=k}^{c_k-1} (\beta_j)^{v_{j-k+2}} x^{\sum_{i=1}^{m_k}(w^k)_i v_i} = \sum_{\substack{v\in(\mathbb{Z}_{0\geqslant})^{m_k}\\ |v|=l}} \binom{l}{v} \prod_{j=k}^{c_k-1} (\beta_j)^{v_{j-k+2}} x^{w^k\cdot v}.$$

Si $v \in (\mathbb{Z}_{\geqslant 0})^{m_k}$ es tal que $|v| = l$ y $v \cdot w^k \geqslant c_k$, entonces

$$\binom{l}{v} \prod_{j=k}^{c_k-1} (\beta_j)^{v_{j-k+2}} x^{w^k\cdot v} \equiv 0 \pmod{x^{c_k}}.$$

De esta manera, si $v \in (\mathbb{Z}_{\geqslant 0})^{m_k}$ es tal que $|v| = l$ y

$$\binom{l}{v} \prod_{j=k}^{c_k-1} (\beta_j)^{v_{j-k+2}} x^{w^k\cdot v} \not\equiv 0 \pmod{x^{c_k}}.$$

Entonces $v \cdot w^k < c_k$. Es decir, $v \in S_{l,k}$. Concluimos que

$$\sum_{\substack{v\in(\mathbb{Z}_{\geqslant 0})^{m_k}\\ |v|=l}} \binom{l}{v} \prod_{j=k}^{c_k-1} (\beta_j)^{v_{j-k+2}} x^{w^k\cdot v} = \sum_{v\in S_{l,k}} \binom{l}{v} \prod_{j=k}^{c_k-1} (\beta_j)^{v_{j-k+2}} x^{w^k\cdot v}.$$

□

Lemma 4.18. *Sean $k \geqslant 2$ y $l \geqslant k$. Si $v \in S_{l,k}$, entonces $\#\{i \in \{2,\ldots,m_k\} | v_i \neq 0\} \leqslant 2$.*

Demostración. Sea $v \in S_{l,k}$. Asumiremos que existen $i_1, i_2, i_3 \in \{2,\ldots,m_k\}$ tales que $v_{i_1}, v_{i_2}, v_{i_3}$ son no nulas. Sin perdida de generalidad asumiremos que $i_1 < i_2 < i_3$. Si alguna de estas coordenadas es mayor o igual a 2, entonces

$$\begin{aligned} v \cdot w^k \geqslant & v_{i_1}(k + (i_1 - 2)) + v_{i_2}(k + (i_2 - 2)) + v_{i_3}(k + (i_3 - 2)) \\ \geqslant & v_{i_1}k + v_{i_2}(k + 1) + v_{i_3}(k + 2) \\ \geqslant & 2k + k + 1 + k + 2 = 4k + 3 \\ \geqslant & c_k \end{aligned}$$

lo que contradice que $v \in S_{l,k}$. Concluimos que $v_{i_1} = v_{i_2} = v_{i_3} = 1$.
Si asumimos que existe $i_4 \in \{2,\ldots,m_k\}\setminus\{i_1,i_2,i_3\}$ tal que $v_{i_4} \neq 0$, entonces

por la contradicción anterior tenemos que $v_{i_4} = 1$. Sin perdida de generalidad podemos asumir que $i_3 < i_4$. Vemos que

$$\begin{aligned} v \cdot w^k \geqslant & v_{i_1}(k + (i_1 - 2)) + v_{i_2}(k + (i_2 - 2)) + v_{i_3}(k + (i_3 - 2)) + v_{i_4}(k + (i_4 - 2)) \\ = & k + (i_1 - 2) + k + (i_2 - 2) + k + (i_3 - 2) + k + (i_4 - 2) \\ \geqslant & k + k + 1 + k + 2 + k + 3 \\ = & 4k + 6 \\ \geqslant & c_k. \end{aligned}$$

Esto es una contradicción. Concluimos que $\{i \in \{2, \dots, m_k\} | v_i \neq 0\} = \{i_1, i_2, i_3\}$.
Vemos que $|v| = l$ implica que $v_1 = l - 3$, con lo que finalmente tenemos que

$$\begin{aligned} v \cdot w^k = & v_1 + v_{i_1}(k + i_1 - 2) + v_{i_2}(k + i_2 - 2) + v_{i_3}(k + i_3 - 2) \\ = & l - 3 + k + i_1 - 2 + k + i_2 - 2 + k + i_3 - 2 \\ \geqslant & k - 3 + k + k + 1 + k + 2 = 4k \\ \geqslant & c_k. \end{aligned}$$

Esto es una contradicción. Finalmente, concluimos que $\#\{i \in \{2, \dots, m_k\} | v_i \neq 0\} \leqslant 2$. $\square$

Nos concentraremos en el caso de $k \geqslant 5$, pues como veremos nos permitirá dar una descripción general de $S_{l,k}$.

Lemma 4.19. *Sean $k \geqslant 5, l \geqslant k$ y $v \in S_{l,k}$.*

a) *Si $\{i \in \{2, \dots, m_k\} | v_i \neq 0\} = \{i_1, i_2\}$, entonces $v_{i_1} = 1 = v_{i_2}$.*

b) *Si $\{i \in \{2, \dots, m_k\} | v_i \neq 0\} = \{i\}$, entonces $v_i \leqslant 2$.*

Demostración.

a) Sin perdida de generalidad asumiremos que $i_1 < i_2$. Asumiremos que $v_{i_1} \geqslant 2$. Si $v_{i_2} = 2$, entonces $v_1 = l - 2 - v_{i_1}$ y

$$\begin{aligned} v \cdot w^k = & v_1 + v_{i_1}(k + (i_1 - 2)) + v_{i_2}(k + (i_2 - 2)) \\ = & l - 2 - v_{i_1} + v_{i_1}(k + (i_1 - 2)) + 2(k + (i_2 - 2)) \\ = & l - 2 + v_{i_1}(k + (i_1 - 2) - 1) + 2(k + (i_2 - 2)) \\ \geqslant & k - 2 + 2(k - 1) + 2(k + 1) \\ = & 5k - 2 \\ \geqslant & c_k. \end{aligned}$$

Esto es una contradicción. De esta manera $v_{i_2} = 1$ y $v_1 = l - 1 - v_{i_1}$. Esto implica que

$$\begin{aligned} v \cdot w^k =& v_1 + v_{i_1}(k + (i_1 - 2)) + v_{i_2}(k + (i_2 - 2)) \\ =& l - 1 - v_{i_1} + v_{i_1}(k + (i_1 - 2)) + k + (i_2 - 2) \\ =& l - 1 + v_{i_1}(k + (i_1 - 2) - 1) + k + (i_2 - 2) \\ \geqslant& k - 1 + 2(k - 1) + k + 1 \\ =& 4k - 2 \\ \geqslant& c_k. \end{aligned}$$

Esto es una contradicción. Concluimos que $v_{i_1} = 1$. Si asumimos que $v_{i_2} \geqslant 2$ llegaremos a una contradicción de manera análoga. Concluimos que $v_{i_1} = 1 = v_{i_2}$.

b) Asumiremos que $v_i \geqslant 4$. Tenemos que

$$v \cdot w^k \geqslant 4k \geqslant c_k.$$

Esto es una contradicción. Concluimos que $v_i \leqslant 3$.
Ahora asumiremos que $v_i = 3$. Vemos que $|v| = l$ implica $v_1 = l - 3$. Tenemos que

$$\begin{aligned} v \cdot w^k =& v_1 + v_i(k + (i - 2)) \\ =& l - 3 + 3(k + (i - 2)) \\ \geqslant& k - 3 + 3k \\ =& 4k - 3 \\ \geqslant& c_k. \end{aligned}$$

Esto es una contradicción. Concluimos que $v_i \leqslant 2$.

□

Observación 4.20. *Sea $l \geqslant k$. Si $v \in S_{l,k}$, entonces $v_1 \neq 0$.*

Definition 4.21. Sea $l \geqslant k$. Sea $v \in S_{l,k}$. Diremos que v es de:

- Tipo A si tiene dos coordenadas no nulas y $v_1 = l - 1$.
- Tipo B si tiene dos coordenadas no nulas y $v_1 = l - 2$.
- Tipo C si tiene tres coordenadas no nulas, en cuyo caso $v_1 = l - 2$.

De esta manera, podemos describir $S_{l,k}$ como la unión de $\{(l,0,\dots,0)\}$ y los vectores de tipos A, B y C en este mismo. Esto nos permite determinar los monomios que aparecerán en $f \circ g$.

Lemma 4.22. *Sean $f, g \in \mathcal{J}_k(\mathbb{Z})/\mathcal{J}_{c_k}(\mathbb{Z})$, con $f = x + \sum_{i=k}^{c_k-1} \alpha_i x^i + O(x^{c_k})$ y $g = x + \sum_{i=k}^{c_k-1} \beta_i x^i + O(x^{c_k})$. Sean $k \geqslant 5, l \geqslant k$ y $v \in S_{l,k}$. Tendremos que:*

a) Si v es de tipo A, donde $i \geqslant k$ es tal que $v_{i-k+2} = 1$, entonces

$$\alpha_l \binom{l}{v} \left(\prod_{e=k}^{c_k-1} (\beta_e)^{v_{e-k+2}} \right) x^{v \cdot w^k} = l \alpha_l \beta_i x^{l-1+i}$$

y $v \cdot w^k \geqslant 2k-1$.

b) Si v es de tipo B, donde $i \geqslant k$ es tal que $v_{i-k+2} = 2$, entonces

$$\alpha_l \binom{l}{v} \left(\prod_{e=k}^{c_k-1} (\beta_e)^{v_{e-k+2}} \right) x^{v \cdot w^k} = \binom{l}{2} \alpha_l {\beta_i}^2 x^{l-2+2i}$$

y $v \cdot w^k \geqslant 3k-2$.

c) Si v es de tipo C, donde $j > i \geqslant k$ son tales que $v_{i-k+2} = 1 = v_{j-k+2}$, entonces

$$\alpha_l \binom{l}{v} \left(\prod_{e=k}^{c_k-1} (\beta_e)^{v_{e-k+2}} \right) x^{v \cdot w^k} = l(l-1) \alpha_l \beta_i \beta_j x^{l-2+i+j}$$

y $v \cdot w^k \geqslant 3k-1$.

d) Si $v = (l,0,\dots,0)$, entonces

$$\alpha_l \binom{l}{v} \left(\prod_{e=k}^{c_k-1} (\beta_e)^{v_{e-k+2}} \right) x^{v \cdot w^k} = \alpha_l x^l.$$

Demostración.

a) Notemos que v es de la forma $(l-1, 0 \dots, 0, 1, 0 \dots, 0)$. Esto implica que

$$\binom{l}{v} = \frac{l!}{(l-1)!0! \cdots 1! \cdots 0!} = l$$

y

$$\prod_{e=k}^{c_k-1} (\beta_e)^{v_{e-k+2}} = \beta_i.$$

Más aún, tenemos que $v \cdot w^k = l - 1 + i$, con lo que se obtiene la igualdad. Además, vemos que

$$l - 1 + i \geqslant k - 1 + i \geqslant k - 1 + k = 2k - 1.$$

b) Notemos que v es de la forma $(l-2, 0\dots, 0, 2, 0\dots, 0)$. Esto implica que

$$\binom{l}{v} = \frac{l!}{(l-2)!0! \cdots 2! \cdots 0!} = \binom{l}{2}$$

y

$$\prod_{e=k}^{c_k-1} (\beta_e)^{v_{e-k+2}} = {\beta_i}^2.$$

Más aún, tenemos que $v \cdot w^k = l - 2 + 2i$, con lo que se obtiene la igualdad. Además, vemos que

$$l - 2 + 2i \geqslant k - 2 + 2i \geqslant k - 2 + 2k = 3k - 2.$$

c) Notemos que v es de la forma $(l-2, 0\dots, 0, 1, 0\dots, 0, 1, 0, \dots, 0)$. Esto implica que

$$\binom{l}{v} = \frac{l!}{(l-2)!0! \cdots 1! \cdots 0!1! \dots 0!} = l(l-1)$$

y

$$\prod_{e=k}^{c_k-1} (\beta_e)^{v_{e-k+2}} = \beta_i \beta_j.$$

Más aún, tenemos que $v \cdot w^k = l - 2 + i + j$, con lo que se obtiene la igualdad. Siendo $j > i \geqslant k$, tenemos que $j \geqslant k + 1$. Vemos que

$$l - 2 + i + j \geqslant k - 2 + i + j \geqslant k - 2 + k + k + 1 = 3k - 1.$$

d) Tenemos que

$$\binom{l}{v} = \frac{l!}{l!0! \cdots 0! \cdots 0!} = 1$$

y

$$\prod_{e=k}^{c_k-1}(\beta_e)^{v_{e+k-2}} = 1.$$

Más aún, vemos que $v \cdot w^k = l$, con lo que se obtiene la igualdad.

□

Con esto ya podemos dar una descripción más ordenada de $f \circ g$.

Theorem 4.23. *Sean $f, g \in \mathcal{J}_k(\mathbb{Z})/\mathcal{J}_{c_k}(\mathbb{Z})$, con $f = x+\sum_{i=k}^{c_k-1}\alpha_i x^i+O(x^{c_k})$ y $g = x + \sum_{i=k}^{c_k-1}\beta_i x^i + O(x^{c_k})$. Sea γ_l el $l-$esimo coeficiente de $f \circ g$.*

- *Si $k \leqslant l \leqslant 2k-2$, entonces $\gamma_l = \alpha_l + \beta_l$.*
- *Si $2k-1 \leqslant l \leqslant 3k-3$, entonces $\gamma_l = \alpha_l + \beta_l + \sum_{i=k}^{l-k+1} i\alpha_i\beta_{l-i+1}$.*
- $\gamma_{3k-2} = \alpha_{3k-2} + \beta_{3k-2} + \sum_{i=k}^{2k-1} i\alpha_i\beta_{3k-1-i} + \binom{k}{2}\alpha_k{\beta_k}^2$.
- $\gamma_{3k-1} = \alpha_{3k-1}+\beta_{3k-1}+\sum_{i=k}^{2k} i\alpha_i\beta_{3k-i}+\binom{k+1}{2}\alpha_{k+1}{\beta_k}^2+k(k-1)\alpha_k\beta_k\beta_{k+1}$.
- $$\begin{aligned}\gamma_{3k} =&\alpha_{3k} + \beta_{3k} + \sum_{i=k}^{2k+1} i\alpha_i\beta_{3k+1-i} + \binom{k}{2}\alpha_k\beta_{k+1}^2 + \binom{k+2}{2}\alpha_{k+2}{\beta_k}^2\\ &+ k(k-1)\alpha_k\beta_k\beta_{k+2} + (k+1)k\alpha_{k+1}\beta_k\beta_{k+1}.\end{aligned}$$
- *Si $k \equiv 0 \pmod 2$, entonces*
$$\begin{aligned}\gamma_{3k+1} =&\alpha_{3k+1} + \beta_{3k+1} + \sum_{i=k}^{2k+2} i\alpha_i\beta_{3k+2-i} + \binom{k+1}{2}\alpha_{k+1}(\beta_{k+1})^2 + \binom{k+3}{2}\alpha_{k+3}{\beta_k}^2\\ &+ \sum_{\substack{k\leqslant l,i,j<c_k\\ i<j\\ l-2+i+j=3k+1}} l(l-1)\alpha_l\beta_i\beta_j.\end{aligned}$$
- *Si $k \equiv 0 \pmod 4$, entonces*
$$\begin{aligned}\gamma_{3k+2} =&\alpha_{3k+2} + \beta_{3k+2} + \sum_{i=k}^{2k+3} i\alpha_i\beta_{3k+3-i} + \binom{k}{2}\alpha_k(\beta_{k+2})^2 + \binom{k+2}{2}\alpha_{k+2}(\beta_{k+1})^2\\ &+ \binom{k+4}{2}\alpha_{k+4}{\beta_k}^2 + \sum_{\substack{k\leqslant l,i,j<c_k\\ i<j\\ l-2+i+j=3k+2}} l(l-1)\alpha_l\beta_i\beta_j.\end{aligned}$$

y

$$\gamma_{3k+3} = \alpha_{3k+3} + \beta_{3k+3} + \sum_{i=k}^{2k+4} i\alpha_i\beta_{3k+4-i} + \binom{k+1}{2}\alpha_{k+1}(\beta_{k+2})^2 + \binom{k+3}{2}\alpha_{k+3}(\beta_{k+1})^2$$
$$+ \binom{k+5}{2}\alpha_{k+5}{\beta_k}^2 + \sum_{\substack{k\leqslant l,i,j<c_k \\ i<j \\ l-2+i+j=3k+3}} l(l-1)\alpha_l\beta_i\beta_j.$$

Demostración. Por el corolario 4.17, sabemos que

$$f\circ g = x + \sum_{i=k}^{c_k-1}\beta_i x^i + \sum_{l=k}^{c_k-1}\alpha_l \sum_{v\in S_{l,k}}\binom{l}{v}\left(\prod_{i=2}^{m_k}(\beta_{k+(i-2)})^{v_i}\right)x^{v\cdot w^k} + O(x^{c_k}).$$

Fijaremos $l \geqslant k$ e identificaremos los vectores $v \in S_{i,k}$, con $k \leqslant i < c_k$, tales que $v \cdot w^k = l$.
Si $l \leqslant 2k-2$, entonces por el lema anterior sabemos que no existen vectores de tipo A,B o C tales que $v\cdot w^k = l$. Esto nos deja solo con vectores de la forma $(i, 0, \ldots, 0)$. Es claro que el único vector v con dicha forma tal que $v\cdot w^k = l$ es $(l, 0 \ldots, 0)$. De esta manera, los únicos sumandos de $f\circ g$ que son divisibles por x^l como factor y no por x^{l+1} son $\alpha_l x^l$ y $\beta_l x^l$. Basta factorizar estos sumandos por x^l para obtener el coeficiente γ_l, y por lo anterior, tendremos la igualdad deseada.

Si $2k-1 \leqslant l \leqslant 3k-3$, entonces por el lema anterior sabemos que no existen vectores de tipo B o C tales que $v\cdot w^k = l$. Esto nos deja solo con vectores de la forma $(i, 0, \ldots, 0)$ y de tipo A. Es claro que el único vector v de la forma $(i, 0, \ldots, 0)$ tal que $v\cdot w^k = l$ es $(l, 0 \ldots, 0)$. Así mismo, sea $v \in S_{i,k}$ un vector de tipo A tal que $v\cdot w^k = l$. Sea $j \geqslant k$ tal que $v_{j-k+2} = 1$. Tendremos que $l = i-1+j$, lo que implica que $j = l-i+1$. Por el lema anterior tendremos que

$$\alpha_i\binom{i}{v}\left(\prod_{e=k}^{c_k-1}(\beta_e)^{v_{e-k+2}}\right)x^{v\cdot w^k} = i\alpha_i\beta_{l-i+1}x^l.$$

De esta manera, y manteniendo la notación anterior, tendremos que $j = l-i+1$ y $k \leqslant j$ implican que el máximo valor de i es $l-k+1$. De esta manera, los únicos sumandos de $f\circ g$ que son divisibles por x^l pero no por x^{l+1} son $\alpha_l x^l, \beta_l x^l$ y $\sum_{i=k}^{l-k+1} i\alpha_i\beta_{l-i+1}$. Nuevamente, basta factorizar por x^l dichos sumandos para obtener γ_l.

Para determinar los coeficientes restantes, contaremos los posibles vectores de tipos B para $k \equiv 0 \pmod 4$, pues en cualquier otro caso solo serán un subconjunto de estos.

- Si $v \in S_{k,k}$, entonces
$$v \in \{(k-2,2,0,\ldots,0),(k-2,0,2,0,\ldots,0),(k-2,0,0,2,0,\ldots,0)\}.$$
- Si $v \in S_{k+1,k}$, entonces
$$v \in \{(k-1,2,0,\ldots,0),(k-1,0,2,0,\ldots,0),(k-1,0,0,2,0,\ldots,0)\}.$$
- Si $v \in S_{k+2,k}$, entonces $v \in \{(k,2,0,\ldots,0),(k,0,2,0,\ldots,0)\}$.
- Si $v \in S_{k+3,k}$, entonces $v \in \{(k+1,2,0,\ldots,0),(k+1,0,2,0,\ldots,0)\}$.
- Si $v \in S_{k+4,k}$, entonces $v = (k+2,2,0,\ldots,0)$.
- Si $v \in S_{k+5,k}$, entonces $v = (k+2,2,0,\ldots,0)$.

Gracias al lema anterior, los correspondientes monomios son

$$\binom{k}{2}\alpha_k{\beta_k}^2x^{3k-2},\ \binom{k}{2}\alpha_k(\beta_{k+1})^2x^{3k},\ \binom{k}{2}\alpha_k(\beta_{k+2})^2x^{3k+2},\ \binom{k+1}{2}\alpha_{k+1}{\beta_k}^2x^{3k-1}$$
$$\binom{k+1}{2}\alpha_{k+1}(\beta_{k+1})^2x^{3k+1},\ \binom{k+1}{2}\alpha_{k+1}(\beta_{k+2})^2x^{3k+3},\ \binom{k+2}{2}\alpha_{k+2}{\beta_k}^2x^{3k}$$
$$\binom{k+2}{2}\alpha_{k+2}(\beta_{k+1})^2x^{3k+2},\ \binom{k+3}{2}\alpha_{k+3}(\beta_k)^2x^{3k+1},\ \binom{k+3}{2}\alpha_{k+3}(\beta_{k+1})^2x^{3k+3}$$
$$\binom{k+4}{2}\alpha_{k+4}{\beta_k}^2x^{3k+2},\ \binom{k+5}{2}\alpha_{k+5}{\beta_k}^2x^{3k+3}.$$

Bastara agrupar los que se puedan factorizar por la misma potencia de x. Finalmente, si $v \in S_{l,k}$ es de tipo C, con $j > i \geqslant k$ tales que $v_{i-k+2} = 1 = v_{j-k+2}$, entonces $v \cdot w^k = l - 2 + i + j$, con lo que bastará igualar $v \cdot w^k$ al índice deseado para obtener los términos restantes. Para los casos de $k \not\equiv 0 \pmod 4$ basta con borrar los coeficientes correspondientes. Los restantes no dependen de los que borramos, así que el calculo es el mismo para los sobrevivientes. $\square$

Corollary 4.24. *Sean $f, g \in \Gamma_k$, con $f = p'(x + \sum_{i=k}^{c_k-1} \alpha_i x^i + O(x^{c_k}))$ y $g = p'(x + \sum_{i=k}^{c_k-1} \beta_i x^i + O(x^{c_k}))$. Sea γ_l el $l-$esimo coeficiente de $f \circ g$.*

- *Si* $k \leqslant l \leqslant 2k-2$, *entonces* $\gamma_l = \alpha_l + \beta_l$.
- *Si* $2k-1 \leqslant l \leqslant d_k - 1$, *entonces* $\gamma_l = \alpha_l + \beta_l + \sum_{i=k}^{l-k+1} i\alpha_i\beta_{l-i+1}$.
- *Si* $d_k \leqslant l \leqslant 3k-3$, *entonces*

$$\gamma_l = \begin{cases} \alpha_l + \beta_l + \sum_{i=k}^{l-k+1} i\alpha_i\beta_{l-i+1} \pmod 2 & , \textit{ si } l \equiv 1 \pmod 2 \\ 0 & , \textit{ si } l \equiv 0 \pmod 2 \end{cases}$$

.

- *Si* $k \equiv 0 \pmod 2$, *entonces* $\gamma_{3k-2} = 0$.
  Si $k \equiv 1 \pmod 2$, *entonces*

$$\gamma_{3k-2} \equiv \alpha_{3k-2} + \beta_{3k-2} + \sum_{i=k}^{2k-1} i\alpha_i\beta_{3k-1-i} + \binom{k}{2}\alpha_k\beta_k \pmod 2.$$

- *Si* $k \equiv 0 \pmod 2$, *entonces*

$$\gamma_{3k-1} \equiv \alpha_{3k-1} + \beta_{3k-1} + \sum_{i=k}^{2k} i\alpha_i\beta_{3k-i} + \binom{k+1}{2}\alpha_{k+1}\beta_k \pmod 2.$$

  Si $k \equiv 1 \pmod 2$, *entonces* $\gamma_{3k-1} = 0$.

- *Si* $k \equiv 0 \pmod 2$, *entonces* $\gamma_{3k} = 0$.
  Si $k \equiv 1 \pmod 2$, *entonces*

$$\gamma_{3k} \equiv \alpha_{3k} + \beta_{3k} + \sum_{i=k}^{2k+1} i\alpha_i\beta_{3k+1-i} + \binom{k}{2}\alpha_k\beta_{k+1} + \binom{k+2}{2}\alpha_{k+2}\beta_k \pmod 2.$$

- *Si* $k \equiv 0 \pmod 2$, *entonces*

$$\gamma_{3k+1} \equiv \alpha_{3k+1} + \beta_{3k+1} + \sum_{i=k}^{2k+2} i\alpha_i\beta_{3k+2-i} + \binom{k+1}{2}\alpha_{k+1}\beta_{k+1} + \binom{k+3}{2}\alpha_{k+3}\beta_k \pmod 2.$$

- *Si* $k \equiv 0 \pmod 4$, *entonces* $\gamma_{3k+2} = 0$, *y*

$$\gamma_{3k+3} \equiv \alpha_{3k+3} + \beta_{3k+3} + \sum_{i=k}^{2k+4} i\alpha_i\beta_{3k+4-i} + \alpha_{k+3}\beta_{k+1} \pmod 2.$$

Con esto podremos dar una formula para el inverso en Γ_k, y a través de ambas formulas podremos dar una para el conmutador.

Corollary 4.25. *Sea $f \in \Gamma_k$, con $f = p'(x + \sum_{i=k}^{c_k-1} \alpha_i x^i + O(x^{c_k}))$. Sea β_l el $l-$esimo coeficiente de f^{-1}.*

- *Si $k \leqslant l \leqslant 2k-2$, entonces $\beta_l = -\alpha_l$.*
- *Si $2k-1 \leqslant l \leqslant d_k - 1$, entonces $\beta_l = -\alpha_l + \sum_{i=k}^{l-k+1} i\alpha_i\alpha_{l-i+1}$.*
- *Si $d_k - 1 \leqslant l \leqslant 3k-3$, entonces*

$$\beta_l = \begin{cases} -\alpha_l + \sum_{i=k}^{l-k+1} i\alpha_i\alpha_{l-i+1} \pmod 2 & , \text{ si } l \equiv 1 \pmod 2 \\ 0 & , \text{ si } l \equiv 0 \pmod 2 \end{cases}.$$

- *Si $k \equiv 0 \pmod 2$, entonces $\beta_{3k-2} = 0$.*
  Si $k \equiv 1 \pmod 2$, entonces

$$\beta_{3k-2} \equiv \alpha_{3k-2} + \sum_{i=k}^{2k-1} i\alpha_i\alpha_{3k-1-i} + \alpha_k + \binom{k}{2}\alpha_k \pmod 2.$$

- *Si $k \equiv 0 \pmod 2$, entonces*

$$\beta_{3k-1} \equiv \alpha_{3k-1} + \sum_{i=k}^{2k} i\alpha_i\alpha_{3k-i} + \binom{k+1}{2}\alpha_{k+1}\alpha_k \pmod 2.$$

  Si $k \equiv 1 \pmod 2$, entonces $\beta_{3k-1} = 0$.

- *Si $k \equiv 0 \pmod 2$, entonces $\beta_{3k} = 0$.*
  Si $k \equiv 1 \pmod 2$, entonces

$$\beta_{3k} \equiv \alpha_{3k} + \sum_{i=k}^{2k+1} i\alpha_i\alpha_{3k+1-i} + \alpha_{k+2}\alpha_k + \binom{k}{2}\alpha_k\alpha_{k+1} + \binom{k+2}{2}\alpha_{k+2}\alpha_k \pmod 2.$$

- *Si $k \equiv 0 \pmod 2$, entonces*

$$\beta_{3k+1} \equiv \alpha_{3k+1} + \sum_{i=k}^{2k+2} i\alpha_i\alpha_{3k+2-i} + (k+1)\alpha_{k+1} + \binom{k+1}{2}\alpha_{k+1} + \binom{k+3}{2}\alpha_{k+3}\alpha_k \pmod 2.$$

- *Si* $k \equiv 0 \pmod 4$, *entonces* $\gamma_{3k+2} = 0$, *y*

$$\beta_{3k+3} \equiv \alpha_{3k+3} + \sum_{i=k}^{2k+4} i\alpha_i\alpha_{3k+4-i} \pmod 2.$$

Demostración. Sabemos que $f \circ f^{-1} = x$. Por el corolario anterior tendremos que:

- Si $k \leqslant l \leqslant 2k-2$, entonces $0 = \alpha_l + \beta_l$, de donde $\beta_l = -\alpha_l$.

- Si $2k-1 \leqslant l \leqslant d_k - 1$, entonces $0 = \alpha_l + \beta_l + \sum_{i=k}^{l-k+1} i\alpha_i\beta_{l-i+1}$. Vemos que $l \leqslant 3k-3$ implica que $l - i + 1 \leqslant 2k-2$ para todo $i \in \{k, \ldots, l-k+1\}$. De esta manera, tenemos que

$$\sum_{i=k}^{l-k+1} i\alpha_i\beta_{l-i+1} = \sum_{i=k}^{l-k+1} i\alpha_i(-\alpha_{l-i+1}),$$

  de donde $\beta_l = -\alpha_l + \sum_{i=k}^{l-k+1} i\alpha_i\alpha_{l-i+1}$.

- Si $d_k - 1 \leqslant l \leqslant 3k-3$, entonces de manera análoga al punto anterior tenemos que

$$\beta_l = \begin{cases} -\alpha_l + \sum_{i=k}^{l-k+1} i\alpha_i\alpha_{l-i+1} \pmod 2 & , \text{ si } l \equiv 1 \pmod 2 \\ 0 & , \text{ si } l \equiv 0 \pmod 2 \end{cases}.$$

- Si $k \equiv 0 \pmod 2$, entonces $\beta_{3k-2} = 0$ por hipótesis.
  Si $k \equiv 1 \pmod 2$, entonces

$$0 \equiv \alpha_{3k-2} + \beta_{3k+2} + \sum_{i=k}^{2k-1} i\alpha_i\beta_{3k-1-i} + \binom{k}{2}\alpha_k\beta_k \pmod 2.$$

  Vemos que $\sum_{i=k}^{2k-1} i\alpha_i\beta_{3k-1-i} = \sum_{i=k+1}^{2k-1} i\alpha_i\beta_{3k-1-i} + k\alpha_k\beta_{2k-1}$. Notemos que $3k-1-i \leqslant 2k-2$, para todo $i \in \{k+1, \ldots, 2k-1\}$. De esta manera tenemos que $\sum_{i=k+1}^{2k-1} i\alpha_i\beta_{3k-1-i} = -\sum_{i=k+1}^{2k-1} i\alpha_i\alpha_{3k-1-i}$. Por otro lado, tenemos que

$$k\alpha_k\beta_{2k-1} = k\alpha_k(-\alpha_{2k-1} + k{\alpha_k}^2) = -k\alpha_k\alpha_{2k-1} + k^2{\alpha_k}^3.$$

  De esta manera, tenemos que

$$\sum_{i=k}^{2k-1} i\alpha_i\beta_{3k-1-i} \equiv \sum_{i=k+1}^{2k-1} i\alpha_i\alpha_{3k-1-i}+k\alpha_k\alpha_{2k-1}+k\alpha_k \equiv \sum_{i=k}^{2k-1} i\alpha_i\alpha_{3k-1-i}+k\alpha_k \pmod 2.$$

Finalmente, recordando que $\beta_k = -\alpha_k$, concluimos que

$$\beta_{3k-2} \equiv \alpha_{3k-2} + \sum_{i=k}^{2k-1} i\alpha_i\alpha_{3k-1-i} + k\alpha_k + \binom{k}{2}\alpha_k \pmod 2.$$

- Si $k \equiv 0 \pmod 2$, entonces

$$0 \equiv \alpha_{3k-1} + \beta_{3k-1} + \sum_{i=k}^{2k} i\alpha_i\beta_{3k-i} + \binom{k+1}{2}\alpha_{k+1}\beta_k \pmod 2.$$

Vemos que $\sum_{i=k}^{2k} i\alpha_i\beta_{3k-i} = \sum_{i=k+2}^{2k} i\alpha_i\beta_{3k-i} + (k+1)\alpha_{k+1}\beta_{2k-1} + k\alpha_k\beta_{2k}$. Notemos que $3k-i \leqslant 2k-2$ para todo $i \in \{k+2, \dots, 2k\}$. De esta manera tenemos que $\sum_{i=k+2}^{2k} i\alpha_i\beta_{3k-i} = -\sum_{i=k+2}^{2k} i\alpha_i\alpha_{3k-i}$. Por otro lado, vemos que $k \equiv 0 \pmod 2$ implica que

$$k\alpha_k\beta_{2k} \equiv 0 \equiv k\alpha_k\alpha_{2k} \pmod 2.$$

Además, sabemos que $\beta_{2k-1} = -\alpha_{2k-1} + k{\alpha_k}^2$. Tenemos que

$$\sum_{i=k}^{2k} i\alpha_i\beta_{3k-i} \equiv \sum_{i=k+2}^{2k} i\alpha_i\alpha_{3k-i}+k\alpha_k\alpha_{2k}+(k+1)\alpha_{k+1}\alpha_{2k-1} \equiv \sum_{i=k}^{2k} i\alpha_i\alpha_{3k-i} \pmod 2$$

Finalmente, recordando que $\beta_k = -\alpha_k$, concluimos que

$$\beta_{3k-1} \equiv \alpha_{3k-1} + \sum_{i=k}^{2k} i\alpha_i\alpha_{3k-i} + \binom{k+1}{2}\alpha_{k+1}\alpha_k \pmod 2.$$

Si $k \equiv 1 \pmod 2$, entonces $\beta_{3k-1} = 0$ por hipótesis.

- Si $k \equiv 0 \pmod 2$, entonces $\beta_{3k} = 0$ por hipótesis.
  Si $k \equiv 1 \pmod 2$, entonces

$$0 \equiv \alpha_{3k}+\beta_{3k}+\sum_{i=k}^{2k+1} i\alpha_i\beta_{3k+1-i}+\binom{k}{2}\alpha_k\beta_{k+1}+\binom{k+2}{2}\alpha_{k+2}\beta_k \pmod 2.$$

  Vemos que

$$\sum_{i=k}^{2k+1} i\alpha_i\beta_{3k+1-i} = \sum_{i=k+3}^{2k+1} i\alpha_i\beta_{3k+1-i}+(k+2)\alpha_{k+2}\beta_{2k-1}+(k+1)\alpha_{k+1}\beta_{2k}+k\alpha_k\beta_{2k+1}.$$

  Notemos que $3k+1-i \leqslant 2k-2$ para todo $i \in \{k+3, \ldots, 2k+1\}$. De esta manera tenemos que $\sum_{i=k+3}^{2k+1} i\alpha_i\beta_{3k+1-i} = -\sum_{i=k+3}^{2k+1} i\alpha_i\alpha_{3k+1-i}$.
  Por otro lado, vemos que $k \equiv 1 \pmod 2$ implica que

$$(k+1)\alpha_{k+1}\beta_{2k} \equiv 0 \equiv (k+1)\alpha_{k+1}\alpha_{2k} \pmod 2.$$

  Además, tenemos que $\beta_{2k-1} = -\alpha_{2k-1} + k\alpha_k^2$ y

$$\beta_{2k+1} = -\alpha_{2k+1} + k\alpha_k\alpha_{k+2} + (k+1)\alpha_{k+1}^2 + (k+2)\alpha_{k+2}\alpha_k.$$

  Tenemos que

$$\begin{aligned}\sum_{i=k}^{2k+1} i\alpha_i\beta_{3k+1-i} &\equiv \sum_{i=k+3}^{2k+1} i\alpha_i\alpha_{3k+1-i} + (k+2)\alpha_{k+2}(\alpha_{2k-1} + k\alpha_k^2) \\ &\quad + (k+1)\alpha_{k+1}\alpha_{2k} + k\alpha_k\alpha_{2k+1} \pmod 2 \\ &\equiv \sum_{i=k}^{2k+1} i\alpha_i\alpha_{3k+1-i} + (k+2)k\alpha_{k+2}\alpha_k \pmod 2\end{aligned}$$

  Finalmente, recordando que $\beta_k = -\alpha_k$ y $\beta_{k+1} = -\alpha_{k+1}$, concluimos que

$$\beta_{3k} \equiv \alpha_{3k}+\sum_{i=k}^{2k+1} i\alpha_i\alpha_{3k+1-i}+\alpha_{k+2}\alpha_k+\binom{k}{2}\alpha_k\alpha_{k+1}+\binom{k+2}{2}\alpha_{k+2}\alpha_k \pmod 2.$$

- Si $k \equiv 0 \pmod 2$, entonces

$$0 \equiv \alpha_{3k+1}+\beta_{3k+1}+\sum_{i=k}^{2k+2} i\alpha_i\beta_{3k+2-i}+\binom{k+1}{2}\alpha_{k+1}\beta_{k+1}+\binom{k+3}{2}\alpha_{k+3}\beta_k \pmod 2.$$

Vemos que

$$\begin{aligned}\sum_{i=k}^{2k+2} i\alpha_i\beta_{3k+2-i} &= \sum_{i=k+4}^{2k+2} i\alpha_i\beta_{3k+2-i} + (k+3)\alpha_{k+3}\beta_{2k-1} \\ &\quad + (k+2)\alpha_{k+2}\beta_{2k} + (k+1)\alpha_{k+1}\beta_{2k+1} + k\alpha_k\beta_{2k+2}.\end{aligned}$$

Notemos que $3k+2-i \leqslant 2k-2$ para todo $i \in \{k+4,\ldots,2k+2\}$. De esta manera tenemos que $\sum_{i=k+4}^{2k+2} i\alpha_i\beta_{3k+2-i} = -\sum_{i=k+4}^{2k+2} i\alpha_i\alpha_{3k+2-i}$. Por otro lado, vemos que $k \equiv 0 \pmod 2$ implica que

$$(k+2)\alpha_{k+2}\beta_{2k} \equiv 0 \equiv (k+2)\alpha_{k+2}\alpha_{2k} \pmod 2$$

y

$$k\alpha_k\beta_{2k+2} \equiv 0 \equiv k\alpha_k\alpha_{2k+2} \pmod 2.$$

Además, tenemos que $\beta_{2k-1} = -\alpha_{2k-1} + k\alpha_k^2$ y

$$\beta_{2k+1} = -\alpha_{2k+1} + k\alpha_k\alpha_{k+2} + (k+1)\alpha_{k+1}^2 + (k+2)\alpha_{k+2}\alpha_k.$$

Tenemos que

$$\begin{aligned}\sum_{i=k}^{2k+2} i\alpha_i\beta_{3k+2-i} &\equiv \sum_{i=k+4}^{2k+2} i\alpha_i\alpha_{3k+2-i} + (k+3)\alpha_{k+3}\alpha_{2k-1} + (k+2)\alpha_{k+2}\alpha_{2k} \\ &\quad + (k+1)\alpha_{k+1}(\alpha_{2k+1} + (k+1)\alpha_{k+1}^2) + k\alpha_k\alpha_{2k+2} \pmod 2 \\ &\equiv \sum_{i=k}^{2k+2} i\alpha_i\alpha_{3k+2-i} + (k+1)\alpha_{k+1} \pmod 2.\end{aligned}$$

Finalmente, recordando que $\beta_k = -\alpha_k$ y $\beta_{k+1} = -\alpha_{k+1}$, concluimos que

$$\beta_{3k+1} \equiv \alpha_{3k+1} + \sum_{i=k}^{2k+2} i\alpha_i\alpha_{3k+2-i} + \alpha_{k+1} + \binom{k+1}{2}\alpha_{k+1} + \binom{k+3}{2}\alpha_{k+3}\alpha_k \pmod{2}.$$

- Si $k \equiv 0 \pmod{4}$, entonces $\beta_{3k+2} = 0$ por hipótesis. Por otro lado

$$0 \equiv \alpha_{3k+3} + \beta_{3k+3} + \sum_{i=k}^{2k+4} i\alpha_i\beta_{3k+4-i} + \alpha_{k+3}\beta_{k+1} \pmod{2}.$$

Vemos que

$$\sum_{i=k}^{2k+4} i\alpha_i\beta_{3k+4-i} = \sum_{i=k+6}^{2k+4} i\alpha_i\beta_{3k+4-i} + (k+5)\alpha_{k+5}\beta_{2k-1} + (k+4)\alpha_{k+4}\beta_{2k}$$
$$+(k+3)\alpha_{k+3}\beta_{2k+1} + (k+2)\alpha_{k+2}\beta_{2k+2} + (k+1)\alpha_{k+1}\beta_{2k+3} + k\alpha_k\beta_{2k+4}.$$

Notemos que $3k+4-i \leqslant 2k-2$ para todo $i \in \{k+6, \ldots, 2k+4\}$. De esta manera tenemos que $\sum_{i=k+6}^{2k+4} i\alpha_i\beta_{3k+4-i} = -\sum_{i=k+6}^{2k+4} i\alpha_i\alpha_{3k+4-i}$. Por otro lado, vemos que $k \equiv 0 \pmod{2}$ implica que

$$(k+4)\alpha_{k+4}\beta_{2k} \equiv 0 \equiv (k+4)\alpha_{k+4}\alpha_{2k} \pmod{2},$$

$$(k+2)\alpha_{k+2}\beta_{2k+2} \equiv 0 \equiv (k+2)\alpha_{k+2}\alpha_{2k+2} \pmod{2}$$

y

$$k\alpha_k\beta_{2k+4} \equiv 0 \equiv k\alpha_k\alpha_{2k+4} \pmod{2}$$

Además, tenemos que $\beta_{2k-1} = -\alpha_{2k-1} + k{\alpha_k}^2$,

$$\beta_{2k+1} = -\alpha_{2k+1} + k\alpha_k\alpha_{k+2} + (k+1)\alpha_{k+1}^2 + (k+2)\alpha_{k+2}\alpha_k,$$

y

$$\beta_{2k+3} = -\alpha_{2k+3} + k\alpha_k\alpha_{k+4} + (k+1)\alpha_{k+1}\alpha_{k+3} + (k+2)\alpha_{k+2}^2 + (k+3)\alpha_{k+3}\alpha_{k+1} + (k+4)\alpha_{k+4}\alpha_k.$$

Tenemos que

$$\begin{aligned}\sum_{i=k}^{2k+4} i\alpha_i\beta_{3k+4-i} \equiv & \sum_{i=k+6}^{2k+4} i\alpha_i\alpha_{3k+4-i} + (k+5)\alpha_{k+5}\alpha_{2k-1} + (k+4)\alpha_{k+4}\alpha_{2k} \\ & + (k+3)\alpha_{k+3}(\alpha_{2k+1} + (k+1)\alpha_{k+1}^2) + (k+2)\alpha_{k+2}\alpha_{2k+2} \\ & + (k+1)\alpha_{k+1}\alpha_{2k+3} + k\alpha_k\alpha_{2k+4} \pmod 2 \\ \equiv & \sum_{i=k}^{2k+4} i\alpha_i\alpha_{3k+4-i} + (k+3)(k+1)\alpha_{k+3}\alpha_{k+1} \pmod 2\end{aligned}$$

Finalmente, recordando que $\beta_{k+1} = -\alpha_{k+1}$, concluimos que

$$\beta_{3k+3} \equiv \alpha_{3k+3} + \sum_{i=k}^{2k+4} i\alpha_i\alpha_{3k+4-i} \pmod 2.$$

$\square$

Corollary 4.26. *Sean $f, g \in \Gamma_k$, con $f = p'(x + \sum_{i=k}^{c_k-1} \alpha_i x^i + O(x^{c_k}))$ y $g = p'(x + \sum_{i=k}^{c_k-1} \beta_i x^i + O(x^{c_k}))$. Sea δ_l el $l-$esimo coeficiente de $[f, g]$.*

- *Si $k \leqslant l \leqslant 2k-1$, entonces $\delta_l = 0$.*
- *Si $2k \leqslant l \leqslant d_k - 1$, entonces*

$$\delta_l = \sum_{i=k}^{l-k+1} (2i - l - 1)\alpha_i\beta_{l-i+1}.$$

- *Si $d_k \leqslant l \leqslant 3k-3$, entonces $\delta_l \equiv 0 \pmod 2$.*
- *Si $k \equiv 0 \pmod 2$, entonces $\delta_{3k-2} = 0$.*
  Si $k \equiv 1 \pmod 2$, entonces $\delta_{3k-2} \equiv 0 \pmod 2$.
- *Si $k \equiv 0 \pmod 2$, entonces*

$$\delta_{3k-1} \equiv \binom{k+1}{2}(\alpha_{k+1}\beta_k + \beta_{k+1}\alpha_k) \pmod 2.$$

Si $k \equiv 1 \pmod 2$, entonces $\delta_{3k-1} = 0$.

- *Si* $k \equiv 0 \pmod 2$, *entonces* $\delta_{3k} = 0$.
  Si $k \equiv 1 \pmod 2$, *entonces*
  $$\delta_{3k} \equiv \binom{k}{2}(\alpha_k\beta_{k+1}+\beta_k\alpha_{k+1})+\binom{k+2}{2}(\alpha_{k+2}\beta_k+\beta_{k+2}\alpha_k) \pmod 2.$$

- *Si* $k \equiv 0 \pmod 2$, *entonces*
  $$\delta_{3k+1} \equiv \binom{k+3}{2}(\alpha_{k+3}\beta_k+\beta_{k+3}\alpha_k) \pmod 2.$$

- *Si* $k \equiv 0 \pmod 4$, *entonces* $\delta_{3k+2} = 0$.

- *Si* $k \equiv 0 \pmod 4$, *entonces*
  $$\delta_{3k+3} \equiv \alpha_{k+3}\beta_{k+1}+\beta_{k+3}\alpha_{k+1} \pmod 2.$$

Demostración. Notemos que $[f,g] = (f \circ g) \circ (g \circ f)^{-1}$. Podemos utilizar los últimos dos corolarios para calcular $(g \circ f)^{-1}$. Estos cálculos, al igual que el computo de $(f \circ g) \circ (g \circ f)^{-1}$, son análogos a los de la demostración anterior. $\square$

Bibliografía

[1] *I. K. Babenko and S. A. Bogatyĭ. On the substitution group of formal integer series.* Izv. Ross. Akad. Nauk Ser. Mat.*, 72(2):39–64, 2008.*

[2] *Salomon Bochner and William Ted Martin.* Several Complex Variables*, volume vol. 10 of* Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 1948.*

[3] *Morikuni Gotô. On the group of formal analytic transformations.* Kodai Math. Sem. Rep.*, 2:45–46, 1950. {Volume numbers not printed on issues until Vol.* **7** *(1955)}.*

[4] *S. A. Jennings. Substitution groups of formal power series.* Canad. J. Math.*, 6:325–340, 1954.*

[5] *Rachel Camina. Subgroups of the Nottingham group.* J. Algebra*, 196(1):101–113, 1997.*

[6] *Hélène Eynard-Bontemps and Andrés Navas. On residues and conjugacies for germs of 1-d parabolic diffeomorphisms in finite regularity, 2023.*