UNIVERSIDAD AUTÓNOMA DE SINALOA
FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS
LICENCIATURA EN MATEMÁTICAS

EL ANILLO DE GRUPO Y LAS CONJETURAS DE KAPLANSKY

T E S I S

QUE COMO REQUISITO PARA OBTENER EL GRADO DE LICENCIADO EN MATEMÁTICAS

PRESENTA:
VÍCTOR ADRIÁN MEZA CAMPA

DIRECTOR DE TESIS:
JOSÉ MARÍA CANTARERO LÓPEZ

Culiacán, Sinaloa. Junio de 2024

A ese yo que creyó en lo que sería hoy

Agradecimientos

A mis padres (Flavio y Consuelo) y hermanas, (Jessi y Cristi) por siempre estar para mí a pesar de todo. En especial a mi madre que incondicionalmente siempre buscó que yo fuera una mejor persona y buscó la manera de que yo saliera adelante.

A mi novia, Kerly, por estar junto a mí desde que llegó a mi vida, hacerme feliz y darme todo el apoyo que me ha dado hasta ahora.

A todos esos profesores que en algún momento dejaron una marca en mí y me ayudaron a tomar las decisiones que me tienen hoy en este camino. En especial, a la profesora Elizabeth que me acercó por primera vez a una olimpiada de matemáticas; A la profesora América, que me motivó a participar por primera (y única) vez en la olimpiada de física; Al profesor Poncho, que por primera vez me enseñó el fascinante mundo de las matemáticas puras.

A todos esos amigos y compañeros que han estado a mi lado, acompañando y aconsejando en todo mi camino escolar.

A todas esas personas que formaron una parte importante en mi vida, pero que por una u otra razón ya no forman parte de ella. Hoy no están en mi vida, pero agradezco todos los momentos bonitos y el apoyo que me dieron.

A mi asesor de tesis, José Cantarero, que desde que lo conozco me ha guiado por el camino de la topología algebraica, me ha ayudado a aprender muchas cosas, siempre ha estado para mí y durante la realización de este trabajo siempre me dio muchos consejos, me ayudó sobre el camino que debía seguir y me mencionó las debidas correcciones a mis equivocaciones.

A los revisores de este trabajo, el Dr. Alfonso Rocha Arteaga, el M.C. Humberto Villegas Rodriguez y el Dr. Luis Jorge Sanchez Saldaña, por sus correspondientes observaciones, recomendaciones y correcciones a este trabajo.

Agradezco en especial a todas aquellas personas que durante el transcurso de mi vida creyeron en mí, creyeron que sería una gran persona y siempre me dieron su apoyo incondicional.

Esta tesis fue parcialmente apoyada por el proyecto de Ciencia de Frontera CF-2023-I-2649: Simetrías ocultas en álgebra y topología, otorgado por CONAHCYT en el año 2023.

Índice general

Introducción

Existen diversas maneras de estudiar la estructura de grupo y por supuesto es relevante relacionar la teoría de grupos con otras estructuras algebraicas. El anillo de grupo cumple un esfuerzo en este sentido, ya que relaciona un grupo y un anillo dado con otra estructura que resulta ser un anillo de nuevo, pero más que eso, también es un módulo y si se construye sobre un campo se tiene entonces los ya tan estudiados espacios vectoriales.

Tomando un grupo G y un anillo R, el anillo de grupo RG se construye como el $R-$módulo libre con base dada por los elementos de G. Por supuesto, esto intuye una operación de suma y una operación multiplicación de los elementos de R con RG, pero para completar la estructura de anillo RG hace falta una multiplicación, la que se realiza usando una convolución a través de la operación de grupo.

El anillo de grupo ha aparecido en diversas áreas matemáticas como la teoría de representaciones, el álgebra homológica, la topología algebraica o la teoría de homología. Por ejemplo, dar un $RG-$módulo es equivalente a dar una representación de G en la categoría de $R-$módulos. En particular, si X es un espacio con una acción de un grupo G, entonces sus grupos de homología $H_n(X;R)$ son de hecho $RG-$módulos. Si G es un grupo discreto, la homología y cohomología del espacio clasificante BG se pueden calcular usando funtores derivados para ciertos $RG-$módulos.

Debido a la importancia que han tenido los anillos de grupo se han realizado diversos trabajos tratando de entender su estructura, como los importantísimos trabajos de Connell y Passman en [6], [26], y algunos más que abordan problemas como el de encontrar unidades y cómo saber si $RG \cong RH$ implica $H \cong G$, el conocido como problema del isomorfismo, abordados por ejemplo en [13]. Tanto es así, que por ejemplo, Kaplansky, un relevante algebrista del siglo pasado presentó una selección de diversos problemas existentes y relevantes en la teoría de anillos ([16] y [15]), donde recurrentemente aparece el anillo de grupo.

Entre algunos de los relevantes problemas de la lista antes mencionada de Kaplansky, estaban tres que pasaron a llamarse justamente como las conjeturas de Kaplansky (Aunque algunos ya habían sido abordados en [13]), y que se enuncian a continuación.

Conjetura de la Unidad. *Si K es un campo y G es un grupo libre de torsión, entonces KG no tiene unidades que no sean de la forma kg, con $k \in K\backslash\{0\}$ y $g \in G$.*

Conjetura de Divisores de Cero. *Si K es un campo y G es un grupo libre de torsión, entonces KG no tiene divisores de cero.*

Conjetura de Elementos Idempotentes. *Si K es un campo y G es un grupo libre de torsión, entonces KG no tiene elementos idempotentes diferentes de 0 y 1.*

Las anteriores conjeturas son el principal punto de partida de este trabajo. Aquí se exponen importantes trabajos que se han realizado para intentar demostrar o dar contraejemplos para las conjeturas. Así como también, se presenta una familia de contrajemplos para la conjetura de la unidad basados en los artículos de Gardam y Murray ([10] y [23]).

A pesar de que la conjetura de la unidad fue desmentida, en realidad queda mucho trabajo por hacer para el problema de descifrar cómo funcionan las unidades en un anillo de grupo. Por ejemplo, existe una propiedad importante para estudiar la conjetura de la unidad, la propiedad de ser de producto único. Por definición, un grupo G es de producto único si para cada par de subconjuntos finitos A, B de G, existe $g \in AB$ que tiene representación única como producto de un elemento de A y uno de B. Es decir, que si $g = a_1b_1 = a_2b_2$ con $a_1, a_2 \in A$ y $b_1, b_2 \in B$, entonces $a_1 = a_2$ y $b_1 = b_2$.

De acuerdo al Corolario 3.2.8, si G es un grupo con producto único, entonces KG tiene solo unidades triviales (es decir, de la forma kg), para cualquier campo K. A día de hoy, la familia de grupos con producto único, es la familia más grande conocida que satisface la conjetura de la unidad de Kaplansky y es interesante ver, que de hecho uno de los primeros ejemplos de grupos sin producto único, como lo es el grupo de Promislow en [27], en realidad no satisface la conjetura de la unidad, al ser el contrajemplo dado por Gardam sobre el campo finito $\mathbb{F}_2$ de característica 2.

Otro ejemplo conocido simple de grupo que no satisface la propiedad de producto único fue dado por Soelberg en [35]. Tiempo después se demostró en [11] que de hecho, este grupo tampoco satisface la conjetura de la unidad de Kaplansky. En este trabajo se da una prueba de hechos relevantes que este grupo satisface en el Teorema 3.4.1.

Teorema 3.4.1. *Sea* $G = \langle x, y \mid (y^2x)^2 = x^2, (x^2y)^2 = y^{-2} \rangle \cong \langle x, y \mid xy^2x^{-1} = y^{-2}, yx^2y^3 = x^{-2} \rangle$.

a) G no satisface la propiedad de producto único.

b) $G \ncong P_k$ para cada $k \geq 1$.

c) G satisface la conjetura de divisor de cero de Kaplansky.

En el anterior teorema, los grupos P_k son la familia de grupos que no satisface la propiedad de producto único dados en [23] y que tienen la siguiente presentación.

$$P_k = \left\langle x, y \mid x^{-1}y^{2^k}x = y^{-2^k}, y^{-1}x^2y = x^{-2} \right\rangle.$$

A continuación, se resume detalladamente el contenido de este texto, desglosando por capítulos una visión de lo que se puede encontrar. Es importante mencionar que en este texto se supone que el lector conoce sobre teoría de grupos y teoría de anillos.

En el primer capítulo se exponen a manera de referencia resultados en teoría de grupos y teoría de anillos. También se desarrollan algunas nociones que normalmente no se ven en un primer curso sobre teoría de grupos que serán útiles más adelante, como lo son las presentaciones de grupo y el producto libre y amalgamado.

En el segundo capítulo se introduce el concepto de anillo de grupo, se dan diferentes perspectivas acerca de su definición y se dan algunas nociones acerca de su relevancia. También se demuestran diversas características acerca de la estructura que relacionan el mismo anillo de grupo con condiciones sobre las que es construido. Se brinda y demuestra un resultado relevante sobre condiciones que debe satisfacer un anillo de grupo para ser primo, resultado que es de gran importancia y que será útil para próximos capítulos. En la Sección 2.4 se da una útil aplicación del resultado anterior acerca de anillos de grupo noetherianos y artinianos.

En el tercer capítulo se enuncian las conjeturas de Kaplansky, así como se exponen algunos de los resultados más relevantes que han sido publicados sobre la resolución de las conjeturas. Se define la condición de grupo con producto único, que históricamente en el estudio de las conjeturas de Kaplansky ha aparecido con gran relevancia. Se da así también la relación que tienen los grupos con producto único sobre las conjeturas de Kaplansky, así como algunos ejemplos de grupos que satisfacen la propiedad de tener producto único. Se demuestran en este capítulo algunas condiciones que debe satisfacer un producto amalgamado de grupos para que al formarse el anillo de grupo de este grupo satisfaga la conjetura de divisor de cero usando la condición de Ore para anillos.

Por último, en el tercer capítulo se dan algunos ejemplos de grupos que no satisfacen la propiedad de producto único. Se desarrolla en especial un grupo estudiado por primera vez por Soelberg en [35], pero se le da una perspectiva diferente. En este trabajo se demuestra que, el grupo que Soelberg propone, que no satisface la propiedad de producto único, sí satisface la conjetura de divisor de cero de Kaplansky y además, que es un grupo diferente a diversos ejemplos conocidos, a pesar de construirse de manera muy similar.

En el cuarto capítulo se desarrollan los contrajemplos ya encontrados para la conjetura de la unidad de Kaplansky. En particular, se desarrollan los cálculos no realizados en [23], donde se da una familia de contraejemplos para anillos de grupo formados en campos finitos sobre el grupo de Promislow P_1. También en este capítulo se habla del trabajo realizado después de haber encontrado la conjetura, se intenta explicar por qué las unidades funcionan y sobre el como encontrar más contraejemplos.

En el quinto capítulo se discuten algunos trabajos adicionales realizados para intentar demostrar o refutar las conjeturas y además se desarrollan ciertas ideas que surgieron durante la realización de todo este trabajo a manera de motivar investigación futura para llegar a la verdad de las conjeturas. También se relacionan las conjeturas de Kaplansky con otros problemas abiertos.

Se incluye además un apéndice con algunos códigos computacionales que fueron útiles durante la realización del trabajo, así como un código en particular que demuestra un resultado pendiente de la Sección 3.4.

Así, en este trabajo se hace un esfuerzo por explicar con detalle y dar diversos ejemplos sobre la estructura de anillo de grupo, así como el estado actual en que se encuentran los importantes problemas para la teoría de anillos de grupo de las conjeturas de Kaplansky. Además, se desarrolla cada tema dando diferentes perspectivas y algunos puntos de vista diferentes. Se desarrollan demostraciones como el Teorema 3.4.1 y diversos cálculos como los de la Sección 4.1 que resultan inéditos.

1 Tópicos de Grupos y Anillos

En este texto, se supone que el lector ha tenido una introducción a la teoría de grupos y a la teoría de anillos, por ello esta sección sirve como puerta de entrada para conceptos que usualmente no se tratan en un primer curso de teoría de grupos o teoría de anillos. El contenido de esta sección está basado principalmente en [8], [12], [29], [31] y [34].

1.1 Grupos

A manera de completez, en esta sección se enuncian diferentes definiciones y notación que se usan a lo largo del texto. Las proposiciones enunciadas son resultados conocidos que usualmente se ven en un primer curso de teoría de grupos, por lo que se omiten las pruebas.

Primeramente, una **operación binaria** en X es una función $\cdot : X \times X \to X$, usualmente denotada $\cdot(x, y) = x \cdot y$ y cuando no haya ambigüedad, $x \cdot y = xy$.

Definición 1.1.1. *Un **grupo** es una dupla $(G, \cdot)$ donde G es un conjunto no vacío y $(\cdot)$ es una operación binaria en G tal que*

- $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, *para cada* $x, y, z \in G$.
- *Existe* $1 \in G$ *tal que* $1 \cdot g = g \cdot 1 = g$, *para cada* $g \in G$.
- *Para cada* $g \in G$, *existe* $g^{-1} \in G$ *tal que* $gg^{-1} = g^{-1}g = 1$.

Cuando no haya ambigüedad, el grupo se denota simplemente como G y la operación mediante $x \cdot y = xy$. Si además de las condiciones anteriores, el grupo G cumple que $gh = hg$ para cada $h, g \in G$, se dice entonces que G es **abeliano** y a menos que se diga lo contrario, la operación en G se denota como $+$, el neutro se denota como 0 y el inverso de g como $-g$. A su vez, si n es un entero positivo y $g \in G$,

$$\begin{aligned} g^0 &= 1, \\ g^n &= \underbrace{gg \cdots g}_{n \text{ veces}}, \\ g^{-n} &= \underbrace{g^{-1}g^{-1} \cdots g^{-1}}_{n \text{ veces}}. \end{aligned}$$

En esta sección, a menos que se diga lo contrario, G, H denotan grupos.

Proposición 1.1.2. *Si $g \in G$ y n, m son enteros,*

$$\begin{aligned} g^n g^m &= g^{n+m} \\ (g^n)^m &= g^{nm} \end{aligned}$$

Para cada $g \in G$, si existe $n \in \mathbb{N}$ (donde $\mathbb{N} = \{1, 2, \dots\}$) tal que $g^n = 1$, denotamos $o(g) = \min\{n \in \mathbb{N} \mid g^n = 1\}$. Si $g \in G \backslash \{1\}$ es tal que existe $n \in \mathbb{N}$ con $g^n = 1$, se dice que g es un **elemento de torsión**. Si G tiene algún elemento de torsión, se dice que G **tiene torsión**. En otro caso, se dice que G es **libre de torsión**.

Proposición 1.1.3. *Si $x, y, z \in G$ son tales que $xy = xz$ ó $yx = zx$, entonces $y = z$.*

Si H es un subconjunto de G tal que la operación $\cdot$ restringida a $H \times H$ tiene rango contenido en H y H es un grupo bajo esta restricción, se dice entonces que H es un **subgrupo** de G y se denota $H \leq G$. Si A, B son subconjuntos de G, denotamos

$$AB = \{ab \mid a \in A, b \in B\}.$$

Si $A = \{g\}$ ó $B = \{g\}$, se denota simplemente gB o Ag, respectivamente. Se nombra a gB la **clase lateral izquierda** de g con respecto a B y a Ag la **clase lateral derecha** de g con respecto a A. Un subgrupo N de G se dice **normal** si $Ng = gN$, para cada $g \in G$ y se denota $N \trianglelefteq G$.

Proposición 1.1.4. *Sea H un subconjunto no vacío de G. Se cumple $H \leq G$ si y sólo si $gh^{-1} \in H$ para cada $g, h \in H$. Si $N \leq G$, se tiene $N \trianglelefteq G$ si y sólo si $g^{-1}Ng \subseteq N$ para cada $g \in G$.*

Proposición 1.1.5. *Si $H, K \leq G$, entonces $H \cap K \leq G$.*

Si $H \leq G$, se denota G/H al conjunto de las clases laterales izquierdas de G en H y $H\backslash G$ el conjunto de clases laterales derechas de G en H. En el caso de que $H \trianglelefteq G$, se cumple $G/H = H\backslash G$, por lo que sin amgigüedad se puede denotar

$$G/H = \frac{G}{H} = H\backslash G.$$

Proposición 1.1.6. *Si $N \trianglelefteq G$, entonces G/N es un grupo con la operación $NgNh = Ngh$. Se le nombra el grupo cociente de G en N.*

Se define también $[G : H] = |G/H|$. Cuando esta cardinalidad no es finita, se suele escribir simplemente $[G : H] = \infty$.

Proposición 1.1.7. *Si G es un grupo y $H \leq G$, se cumple $[G : H]|H| = |G|$.*

Si $\phi \colon G \to H$ es tal que $\phi(gh) = \phi(g)\phi(h)$, se dice que ϕ es un **homomorfismo**. Si además ϕ es biyectiva, se dice que ϕ es un **isomorfismo de grupos** y en tal caso, se dice que G y H son **isomorfos** y se denota $G \cong H$. También tenemos dos subgrupos asociados a ϕ, su **núcleo** y su ¸**imagen**.

$$\ker \phi = \{g \in G \mid \phi(g) = 1\},$$
$$\operatorname{im} \phi = \{\phi(g) \mid g \in G\}.$$

Si $x, g \in G$, se denota $x^g = g^{-1}xg$ y se le nombra **conjugado** de x y denotamos por $C_G(x) = \{g \in G \mid g^{-1}xg = x\}$ al **centralizador** de x.

Definición 1.1.8. *Sea G un grupo. Un subgrupo H de G se dice **característico** si para cualquier isomorfismo $\phi : G \to G$ se tiene $\phi(H) = H$.*

Proposición 1.1.9. *Sea G un grupo. El grupo $G' = \langle \{ghg^{-1}h^{-1} \mid g, h \in G\} \rangle$ (conocido como subgrupo conmutador o grupo derivado) es un subgrupo característico de G. Más aún, si G y H son isomorfos, entonces $G/G' \cong H/H'$.*

Definición 1.1.10. *Sean H, G grupos. Si existe un subgrupo $K \leq G$ tal que $\phi : H \to K$ es un isomorfismo, se dice entonces que ϕ es un **encaje** de K en G. A su vez, se dice que K está **encajado** en G.*

Los siguientes tres teoremas se conocen como el primer, segundo y tercer teorema de isomorfismo respectivamente.

Teorema 1.1.11. *Sea $\phi\colon G \to H$ un homomorfismo. Entonces $\ker\phi \trianglelefteq G$ y existe un isomorfismo $G/\ker\phi \cong$ im ϕ.*

Teorema 1.1.12. *Sean $H \leq G$ y $N \trianglelefteq G$. Entonces $N \cap H \trianglelefteq H$ y $H/(N \cap H) \cong NH/N$.*

Teorema 1.1.13. *Sean $K \leq H \leq G$, con $K, H \trianglelefteq G$. Entonces H/K es normal en G/K y*

$$(G/K)/(H/K) \cong G/H.$$

Si G, H son grupos, el **grupo producto** de G y H es el conjunto de pares ordenados de G y H, es decir,

$$G \times H = \{(g, h) \mid g \in G, h \in H\},$$

donde la operación está dada por $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$. Si G y H son abelianos, se suele decir al producto de G y H, la **suma directa** de G y H. Esta se denota por $G \oplus H$.

1.2 Presentaciones de Grupo

Sea X un conjunto. A cada elemento $x \in X$ se le asigna un elemento abstracto x^{-1} y se define $X^{-1} = \{x^{-1} \mid x \in X\}$. Una **palabra** en X es una sucesión finita de elementos en $X \cup X^{-1}$ de la forma

$$x_1x_2\cdots x_n, \quad \text{donde } x_1, x_2, \ldots, x_n \in X \cup X^{-1}.$$

La palabra vacía (una sucesión finita de longitud cero) se denota por 1. Para cada $x \in X$, se toma $(x^{-1})^{-1} = x$. Para una palabra $x_1x_2\cdots x_n$, se toma el inverso $(x_1x_2\cdots x_n)^{-1} = x_n^{-1}\cdots x_1^{-1}$. Una **palabra reducida** en X es una palabra

$$x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n},$$

donde $x_1, \ldots, x_n \in X$, $a_i \in \{1, -1\}$ y si $i = j+1$, no puede suceder a la vez $a_i \neq a_j$ y $x_i = x_j$. Al conjunto de palabras reducidas en X se le denota F_X. Toda palabra de X puede ser llevada a una forma reducida quitando las palabras triviales. Por ejemplo, si consideramos $xyy^{-1}z$, la forma reducida de la palabra es xz. Se define además una operación concatenación $(\cdot)$ de forma que si $x_1x_2\cdots x_n, y_1y_2\cdots y_m \in F_X$ y $x_n \neq y_1^{-1}$,

$$(x_1x_2\cdots x_n)\cdot(y_1\cdots y_n) = x_1x_2\cdots x_ny_1\cdots y_m.$$

En caso de que $x_n = y_1^{-1}$, se toma el producto recursivamente de la siguiente manera,

$$(x_1x_2\cdots x_n)\cdot(y_1\cdots y_n) = (x_1x_2\cdots x_{n-1})\cdot(y_2\cdots y_m),$$

y sucesivamente se hace esta reducción hasta tener una palabra reducida. Con la operación anterior, F_X es un grupo, llamado el **grupo libre generado por** X. Si X es finito, se suele denotar al grupo libre generado por X como $F_{|X|}$.

Ejemplo 1.2.1. *Si $X = \{x\}$, entonces $F_X = F_1$ es el grupo libre generado por una letra, que es isomorfo a $\mathbb{Z}$. Denotamos para un número entero positivo n,*

$$x^n = \underbrace{x \cdot x \cdot \cdots \cdot x}_{n \text{ veces}},$$

y de manera análoga para enteros negativos. Entonces todo elemento de F_1 es de la forma x^n donde n es entero y por propiedades de F_X, se cumple $x^n x^m = x^{n+m}$, por lo que la función $\phi\colon F_1 \to \mathbb{Z}$ definida mediante $\phi(x^n) = n$ es un isomorfismo de grupos. De hecho, F_1 es el único grupo libre abeliano.

Si G es un grupo y $X \subseteq G$, se dice que X es un **conjunto generador** de G si el subgrupo de G más pequeño que contiene a X es G. Esto se denota $\langle X \rangle = G$. No es complicado ver que, de hecho, para cualquier $X \subseteq G$, el subgrupo $\langle X \rangle$ consta de las posibles multiplicaciones finitas de elementos de X y sus inversos. Algo así como las palabras que se pueden formar con los elementos de X y sus inversos, solo que en esta ocasión, comparar las palabras reducidas no basta para decir que dos elementos son iguales. En el sentido anterior, si Y es un conjunto no vacío y lo vemos dentro de F_Y como palabras con una letra, se tiene $\langle Y \rangle = F_Y$.

Proposición 1.2.2. *Sea X un conjunto no vacío. Para cada función $f\colon X \to G$, con G un grupo, existe un único homomorfismo $\phi\colon F_X \to G$ tal que $\phi(x) = f(x)$ para cada $x \in X$.*

Demostración. Como cada elemento $g \in F_X$ es de la forma

$$g = x_1 x_2 \cdots x_n,$$

donde $x_1, x_2, \ldots, x_n \in X \cup X^{-1} \cup \{1\}$, entonces se define $\phi\colon F_X \to G$ como $\phi(x) = f(x)$ y $\phi(x^{-1}) = f(x)^{-1}$ para cada $x \in X$, y $\phi(1) = 1$. De esta forma, se define para $g \in F_X$ arbitrario como,

$$\phi(g) = \phi(x_1)\phi(x_2)\cdots\phi(x_n). \tag{1.1}$$

Para ver que está bien definida, basta ver que al reducir trivialidades de la forma xx^{-1} ó $x^{-1}x$, el valor de la función es igual, en este caso, si $x_{i+1} = x_i^{-1}$ y g_r es la palabra que quita esta trivialidad en g,

$$\begin{aligned}
\phi(g) &= \phi(x_1)\phi(x_2)\cdots\phi(x_i)\phi(x_{i+1})\cdots\phi(x_n) \\
&= f(x_1)f(x_2)\cdots f(x_i)f(x_i)^{-1}\cdots f(x_n) \\
&= f(x_1)f(x_2)\cdots f(x_{i-1})f(x_{i+2})\cdots f(x_n) \\
&= \phi(g_r),
\end{aligned}$$

por lo que ϕ está bien definida. Ahora, como todo homomorfismo de F_X a G necesita satisfacer (1.1), el homomorfismo ϕ debe ser único. Resta probar que, en efecto, ϕ es un homomorfismo. Si $g = x_1 x_2 \cdots x_n$ y $h = y_1 y_2 \cdots y_n$,

$$\phi(gh) = \phi(x_1 x_2 \cdots x_n y_1 y_2 \cdots y_n) = \phi(x_1)\phi(x_2)\cdots\phi(x_n)\phi(y_1)\phi(y_2)\cdots\phi(y_n) = \phi(g)\phi(h),$$

completando el resultado. □

Proposición 1.2.3. *Todo grupo G es isomorfo a un cociente de un grupo libre.*

Demostración. Para cada $g \in G$, sea x_g una letra distinta, de tal manera que $X = \{x_g \mid g \in G\}$ sea isomorfo a G como conjunto mediante $x_g \mapsto g$. Por la Proposición 1.2.2, existe un único homomorfismo $\phi\colon F_X \to G$ que extiende esa función. Ya que ϕ es sobreyectiva, por el primer teorema de isomorfismo, $F_X / \ker\phi \cong G$. □

El resultado anterior dice que debe haber una manera de representar cada grupo G a partir de un grupo libre del que G es isomorfo a un cociente. En este sentido, es como aparecen las presentaciones de grupo, una manera práctica y útil de escribir cada grupo.

Sea X un conjunto y R un subconjunto de F_X. Si llamamos $\langle R \rangle_N$ al subgrupo normal más pequeño de F_X que contiene a R, se denota

$$\langle X \mid R \rangle = \frac{F_X}{\langle R \rangle_N}.$$

A $\langle X \mid R \rangle$ se le llama **presentación de grupo con generadores en X y relaciones R.**

Proposición 1.2.4. *Todo grupo admite una presentación de grupo.*

Demostración. Sean G, F_X, ϕ como en la Proposición 1.2.3. Entonces, como $\ker \phi \trianglelefteq F_X$, por el primer teorema de isomorfismo,

$$G \cong \frac{F_X}{\ker \phi} = \langle X \mid \ker \phi \rangle ,$$

obteniendo una presentación de G. □

En ocasiones, si X y R son conjuntos a lo más numerables, se suelen escribir los elementos de X y R en la presentación. Por ejemplo, si $X = \{x_1, x_2, x_3\}$ y $R = \{x_2x_3, x_1x_2\}$, entonces

$$\langle X \mid R \rangle = \langle x_1, x_2, x_3 \mid x_2x_3, x_1x_2 \rangle .$$

También, en algunas ocasiones suele ser más práctico escribir en las relaciones expresiones de la forma $x_1 = x_2x_3$, lo que simplemente quiere decir, $x_1(x_2x_3)^{-1} \in R$. Si existe un conjunto finito X tal que $G = \langle X \mid R \rangle$, se dice que G es **finitamente generado**, y si existen Y, Q finitos tal que $G = \langle Y \mid Q \rangle$, se dice que G es **finitamente presentado**.

Ejemplo 1.2.5. *Si C_n es el grupo cíclico de orden n, se tiene que $C_n \cong \langle x \mid x^n = 1 \rangle$.*

Ejemplo 1.2.6. $\mathbb{Z} \oplus \mathbb{Z} \cong \langle x, y \mid xy = yx \rangle$.

Ejemplo 1.2.7. *El teorema fundamental de la aritmética dice que todo entero puede ser factorizado de manera única como producto de primos. Como el conjunto de números primos es infinito numerable y los primos conmutan entre sí al multiplicarse,*

$$\mathbb{Q}^+ \cong \langle x_1, x_2, \ldots \mid x_ix_j = x_jx_i, \forall i, j \in \mathbb{N} \rangle .$$

Aquí $\mathbb{Q}^+$ es el conjunto de los racionales positivos con la operación dada por el producto.

Ejemplo 1.2.8. *El grupo dihedral de orden $2n$.*

$$D_{2n} \cong \left\langle x, y \mid x^n = 1, y^2 = 1, (yx)^2 = 1 \right\rangle .$$

1.3 El Producto Amalgamado

En el estudio de la topología algebraica, el producto amalgamado apareció como un producto de grupos útil para calcular el grupo fundamental de la unión de espacios bajo ciertas condiciones. Debido al enfoque de este texto, no se abundará mucho en la motivación topológica del producto amalgamado. En cambio, se plantea un enfoque práctico.

Sean G y H grupos. Una **palabra alternante** de G y H es una secuencia de elementos alternantes entre G y H, es decir, una palabra alternante w tiene la forma

$$w = g_1 h_1 g_2 h_2 \cdots g_n h_n,$$

donde $g_2, \ldots, g_n \in G \backslash \{1\}$, $h_1, \ldots, h_{n-1} \in H \backslash \{1\}$, $g_1 \in G$, $h_n \in H$. La palabra vacía simplemente se denota 1. Al conjunto de estas palabras alternantes se le llama el **producto libre** de G y H y se denota $G * H$. De hecho, $G * H$ es un grupo, donde 1 es el elemento neutro y la operación de grupo de w_1, w_2 es la concatenación si la última letra de w_1 diferente de 1 pertenece a un grupo distinto al de la primera letra de w_2. Es decir, si $w_1 = x_1 x_2 \cdots x_n$, $w_2 = y_1 y_2 \cdots y_m$,

$$w_1 w_2 = x_1 x_2 \cdots x_n y_1 y_2 \cdots y_m.$$

Pero si dos elementos adyacentes pertenecen al mismo grupo, estos dos elementos se cambian por su producto, y si este producto es 1, simplemente se eliminan las letras. Se itera este proceso hasta que quede una palabra alternante.

Ejemplo 1.3.1. *Si* $G = \langle x \mid x^2 = 1 \rangle$ *y* $H = \langle y \mid y^2 = 1 \rangle$*, cualquier elemento* $k \in G * H - \{1\}$ *es de la forma*

$$\begin{aligned} k &= xy \cdots xy, \text{ ó} \\ k &= yx \cdots xy, \text{ ó} \\ k &= xy \cdots yx, \text{ ó} \\ k &= yx \cdots yx. \end{aligned}$$

De esta forma, se observa que a pesar de la pequeña cantidad de elementos de G *y* H*, el grupo* $G * H$ *tiene infinitos elementos.*

Supongamos ahora que un grupo K está encajado tanto en el grupo G como en el grupo H, siendo K_G, K_H las imágenes de los respectivos encajes. Sea $\phi \colon K_G \to K_H$ un isomorfismo. Entonces el **producto amalgamado** de G y H con respecto a K a través de la función ϕ, escrito como $G *_K H$, es

$$G *_K H = \frac{G * H}{N},$$

donde N es el subgrupo normal más pequeño (la clausura normal) en $G * H$ que contiene a $\{g\phi(g^{-1}) \mid g \in K_G\}$.

Definición 1.3.2. *Sea* $H \leq G$*. Un* ***transversal derecho*** T *para* G *en* H *es una clase de representantes de clases laterales derechas de* H *en* G*, donde a la clase lateral* H *se le asigna* 1.

Sean T_G, T_H transversales derechos de G, H en K respectivamente y $x \in G *_K H$. Una **forma normal** para x en $G *_K H$ es una palabra w en $G * H$ de la forma

$$w = k g_1 h_1 g_2 h_2 \cdots g_n h_n,$$

para algún $n \in \mathbb{N}$, donde $k \in K$ visto como subgrupo de G, $g_1 \in T_G$, $h_n \in T_H$, $g_2, \dots g_n \in T_G \backslash \{1\}$ y $h_1, \dots, h_{n-1} \in T_H \backslash \{1\}$ y w es tal que $x = Nw$, donde N es como en la definición de producto amalgamado.

La importancia de una forma normal radica en el siguiente importante teorema, conocido como teorema de la forma normal

Teorema 1.3.3. *Sean G, H grupos y K un grupo encajado en G y H. Todo elemento $x \in G *_K H$ tiene una única forma normal.*

Demostración. Sea $x \in G *_K H$ y sean K_G, K_H isomorfos tal que el producto amalgamado es través del isomorfismo $\phi \colon K_G \to K_H$. Sean T_G, T_H transversales derechos de K_G, K_H de G, H respectivamente. Ya que $G *_K H = (G * H)/N$, para algún $N \trianglelefteq G * H$, el elemento x tiene un representante $g_1 h_1 \cdots g_n h_n \in G * H$, donde $g_k \in G$, $h_k \in H$ y sólo g_1, h_n pueden ser 1. Ahora bien, para h_n, existen $h'_n \in T_H$ y $k_n^H \in K_H$ tales que $h_n = k_n^H h'_n$, por lo que

$$g_1 h_1 \cdots g_n h_n = g_1 h_1 \cdots g_n k_n^H h'_n. \tag{1.2}$$

Los elementos k_n^H y $\phi^{-1}(k_n^H) \in G$ generan la misma clase lateral en $G *_K H$, por lo que se puede reescribir el representante como

$$g_1 h_1 \cdots g_n h_n = g_1 h_1 \cdots g_n \phi^{-1}(k_n^H) h'_n,$$

donde $g_n \phi^{-1}(k_n^H) \in G$. Por lo que existen $g'_n \in T_G$ y $k_n^G \in K_G$ tales que $g_n \phi^{-1}(k_n^H) = k_n^G g'_n$, es decir,

$$g_1 h_1 \cdots g_n h_n = g_1 h_1 \cdots h_{n-1} k_n^G g'_n h'_n.$$

De nuevo se puede cambiar k_n^G por $\phi(k_n^G) \in K_H$, de forma que $h_{n-1}\phi(k_n^G) \in H$, por lo que existen $k_{n-1}^H \in K_H$ y $h'_{n-1} \in T_H$ tales que $h_{n-1}\phi(k_n^G) = k_{n-1}^H h'_{n-1}$. Es decir, el representante se puede reescribir como

$$g_1 h_1 \cdots g_n h_n = g_1 h_1 \cdots k_{n-1}^H h'_{n-1} g'_n h'_n,$$

Iterando sucesivamente este proceso, el representante se puede escribir como

$$k_1^G g'_1 h'_1 \cdots g'_n h'_n,$$

la forma normal buscada para x. En caso de que en algún paso el anterior procedimiento, se tuviera por ejemplo $g_j \in K_G$, se tendría entonces en la nueva forma $h'_{j-1} 1 h'_j$. Entonces, se realiza el mismo procedimiento para $h'_{j-1} h'_j \in H$. Así, cada elemento en $G *_K H$ tiene una forma normal.

Ahora, para la unicidad, supongamos que $k g_1 h_1 \cdots g_n h_n$ y $k' g'_1 h'_1 \cdots g'_m h'_m$ son palabras en $G * H$ en su forma normal que generan la misma clase lateral en $G *_K H$. Entonces, existe $r \in N$, la clausura normal en $G * H$ de $\{g\phi(g^{-1}) \mid g \in K_G\}$, tal que

$$r k g_1 h_1 \cdots g_n h_n = k' g'_1 h'_1 \cdots g'_m h'_m,$$

en $G * H$. Pero como $h_n, h'_m \in H$ y $g_n, g'_m \in G$, lo anterior solo ocurre si $n = m$ y los elementos en las correspondientes posiciones coinciden. Es decir, $h_n = h'_m$ y $g_n = g'_m$ y así sucesivamente hasta $h_2 = h'_2$, lo que deja

$$r k g_1 = k' g'_1.$$

Pero se tiene

$$N = \{w_1^{-1}(k_1 \phi(k_1^{-1}))^{\varepsilon_1} w_1 \cdots w_s^{-1}(k_s \phi(k_s^{-1}))^{\varepsilon_s} w_s \mid s \in \mathbb{N}, k_1, \dots, k_s \in K_G, w_1 \cdots w_s \in G * H, \varepsilon_j = \pm 1\},$$

luego el único elemento en N que pertenece a G es 1. Puesto que $k'g_1', kg_1 \in G$, entonces $r = 1$. Y ya que $g_1, g_1' \in T_G$, entonces

$$K_G k' g_1' = K_G g_1' = K_G g_1 = K_G k g_1,$$

implica $g_1 = g_1'$ y por lo tanto, $k' = k$. Para resumir, hemos probado $n = m$, $g_1 = g_1', h_1 = h_1', \ldots, g_n = g_n', h_n = h_n'$ y $k = k'$, por lo que las palabras son iguales en $G * H$ y entonces, la forma normal de cada elemento en $G *_K H$ es única. □

El anterior teorema soluciona un conocido problema en teoría de grupos conocido como el problema de la palabra, para productos amalgamados. Este problema trata sobre cómo identificar si dos elementos en cualquier grupo son iguales o no. En este caso, en el producto amalgamado habrá que buscar la forma normal de una palabra y comparar si es igual a la forma normal de otra palabra para saber si son iguales.

Por supuesto, el procedimiento anterior se puede hacer con representantes de clases laterales izquierdas, sólo que la forma normal (izquierda) sería en este caso, con las condiciones de (1.2),

$$w = g_1 h_1 g_2 h_2 \cdots g_n h_n k.$$

Así, hay unicidad en la forma normal izquierda y derecha de la palabra.

Proposición 1.3.4. *Sean G, H grupos y $K \cong K_G \cong K_H$ tales que $K_G \trianglelefteq G$ y $K_H \trianglelefteq H$. Si $x \in G *_K H$ tiene formas normales izquierda y derecha*

$$k_r g_1 h_1 \ldots g_n h_n,$$
$$g_1' h_1' \ldots g_m' h_m' k_l,$$

entonces $n = m$ y $g_j = g_j', h_j = h_j'$ para cada $1 \leq j \leq n$.

Demostración. Puesto que $K_G \trianglelefteq G$, existe $k_1^G \in K_G$ tal que $k_r g_1 = g_1 k_1^G$. En $G *_K H$ se tiene $k_1^G = \phi(k_1^G)$ para el isomorfismo ϕ sobre el que se construye el producto amalgamado, por lo que, en $G *_K H$,

$$k_r g_1 h_1 \cdots g_n h_n = g_1 \phi(k_1^G) h_1 \cdots g_n h_n,$$

Ya que $\phi(k_1^G) \in K_H$ y $K_H \trianglelefteq H$, existe $k_1^H \in K_H$ tal que $\phi(k_1^G) h_1 = h_1 k_1^H$, teniendo entonces

$$g_1 h_1 k_1^H \cdots g_n h_n.$$

Repitiendo el proceso sucesivamente, llegamos a

$$k_r g_1 h_1 \cdots g_n h_n = g_1 h_1 \cdots g_n h_n k_n^H,$$

y por lo tanto

$$k_r g_1 h_1 \cdots g_n h_n = g_1 h_1 \cdots g_n h_n \phi^{-1}(k_n^H).$$

Se tiene entonces la forma normal izquierda y debido a su unicidad, se concluye el resultado. □

Es importante resaltar que en la forma de construir el producto libre, si $G = \langle X \mid R \rangle$ y $H = \langle Y \mid Q \rangle$ son presentaciones de grupo para G y H de forma que $X \cap Y = \varnothing$, entonces

$$G * H = \langle X \cup Y \mid R \cup Q \rangle .$$

De manera similar, al ser el producto amalgamado un cociente del producto libre, si K está encajado en G, H con $K_G \leq G$ y $K_H \leq H$ de forma que $K_G \cong K_H \cong K$ por medio de un isomorfismo $\phi\colon K_G \to K_H$, el correspondiente producto amalgamado tiene la siguiente presentación.

$$G *_K H = \left\langle X, Y \mid R \cup Q \cup \{g\phi(g^{-1}) : g \in K_G\} \right\rangle .$$

Ejemplo 1.3.5. *Sean* $G_1 = \langle a \mid a^6 = 1\rangle$ *y* $G_2 = \langle b \mid b^4 = 1\rangle$. *Es posible tomar los subgrupos normales* $\langle a^3\rangle \trianglelefteq G_1$ *y* $\langle b^2\rangle \trianglelefteq G_2$. *Identificamos* a^3 *con* b^2 *ya que ambos subgrupos tienen dos elementos, con lo que* $\langle a^3\rangle \cong \langle b^2\rangle \cong \mathbb{Z}/2\mathbb{Z}$. *En el producto amalgamado* $G = G_1 *_{\mathbb{Z}/2\mathbb{Z}} G_2$, *todo elemento tiene la forma normal*

$$a^3 a^{\alpha_1} b a^{\alpha_2} b \cdots a^{\alpha_n} b^{\beta},$$

donde $\alpha_1 \in \{0,1,2\}$, $\alpha_2, \ldots, \alpha_n \in \{1,2\}$ *y* $\beta \in \{0,1\}$.

En un producto amalgamado, $G = G_1 *_N G_2$, por el teorema de la forma normal, cada $g \in G$ tiene una expresión en forma única de la forma $g = n_1 t$ ó $g = t n_2$, donde $n_1, n_2 \in N$ y t es una palabra de letras alternantes entre las transversales T_1 y T_2 de G_1 y G_2 en N, exceptuando al representante para la clase lateral N. Es decir, si el conjunto de estas palabras es T y $t \in T$, entonces,

$$t = a_1 b_1 \cdots a_n b_n, \tag{1.3}$$

donde $a_2, \ldots, a_n \in T_1$, $b_1, \ldots, b_{n-1} \in T_2$, $a_1 \in T_1 \cup \{1\}$ y $b_n \in T_2 \cup \{1\}$. Cada palabra $t \in T$ tiene una noción de longitud $\text{long}(t)$ igual a la cantidad de letras diferentes de 1 de las transversales que la componen, definiendo una función $\text{long}\colon T \to \mathbb{N} \cup \{0\}$. Por ejemplo, en (1.3), si $a_1, b_n \neq 1$, entonces $\text{long}(t) = 2n$. Si en cambio $a_1 = 1$, entonces $\text{long}(t) = 2n-1$. Para el caso de la palabra vacía 1, definimos $\text{long}(1) = 0$. Como cada $g \in G$ tiene una expresión en forma única como $g = n_1 t$ ó $g = t n_2$, $n_1, n_2 \in N$ y $t \in T$, se define $\text{long}(g) = \text{long}(t)$.

Otra noción que es útil gracias a la forma normal es la de ser cíclicamente reducido. Tomando de nueva cuenta $G = G_1 *_N G_2$ y $g \in G$ en su forma normal $g = kt$, con $k \in N$ y t como en (1.3), se dice que un elemento g es **cíclicamente reducido** si $\text{long}(g) \geq 2$ y además $a_1, b_n = 1$ ó $a_1, b_n \neq 1$.

Proposición 1.3.6. *Sea* $G = G_1 *_N G_2$. *Cualquier elemento* $g \in G$ *es conjugado a un elemento cíclicamente reducido o a un elemento de* G_1 *ó* G_2.

Demostración. Si g es el elemento neutro, es claro. Si $g \in G$ tiene longitud igual a 1 es de la forma nr con $n \in N$ y $r \in G_1$ ó $r \in G_2$. En cualquiera de los casos, $g \in G_1$ ó $g \in G_2$ y se tiene el resultado. Supongamos ahora que $m = \text{long}(g) \geq 2$ y el resultado se cumple para longitudes menores a m. Si G es cíclicamente reducido, se tiene el resultado para g. Si no lo es, g es de la forma $g = n a_1 b_2 \cdots b_{m-1} a_m$ ó $g = n b_1 a_2 \cdots a_{m-1} b_m$ para $n \in N$ y $a_i \in G_1$, $b_i \in G_2$ para cada i. Sin pérdida de generalidad se supone el primer caso, $g = n a_1 b_2 \cdots b_{m-1} a_m$. Entonces,

$$(na_1)^{-1} g (na_1) = b_2 \cdots b_{m-1} a_m (na_1).$$

Ahora, ya que $N \leq G_1$, todo elemento que está en una clase lateral izquierda de N, está en una clase lateral derecha de N, por lo que teniendo $n \in N$, existen $a'_m \in G_1$ y $n_m \in N$ tal que $a_m n = n_m a'_m$. Entonces

$$b_2 \cdots b_{m-1} a_m (na_1) = b_2 \cdots b_{m-1} n_m a'_m a_1,$$

Tras identificar las copias de N de G_1 y G_2, podemos suponer ahora que $N \leq G_2$. Entonces existen $n_{m-1} \in N$ y $b'_{m-1} \in G_2$ tales que $b_{m-1} n_m = n'_m b'_{m-1}$, es decir,

$$b_2 \cdots b_{m-1} a_m (na_1) = b_2 \cdots n_{m-1} b'_{m-1} a'_m a_1.$$

Repitiendo este proceso sucesivamente, obtenemos

$$(na_1)^{-1} g (na_1) = b_2 \cdots b_{m-1} a_m (na_1) = n_2 b'_2 \cdots b'_{m-1} a'_m a_1,$$

para $a'_3, \ldots, a'_m \in G_1$, $b'_2, b'_4, \ldots, b'_{m-1} \in G_2$ y $n'_2 \in N$. Puesto que $a'_m a_1 \in G_1$, se tiene entonces lo siguiente, $\text{long}((na_1)^{-1} g (na_1)) \leq \text{long}(g) - 1$ y por hipótesis es conjugado a un elemento de G_1 ó G_2 o a un elemento cíclicamente reducido, lo que a su vez implica lo mismo para g. Por inducción matemática, se tiene entonces el resultado. □

Proposición 1.3.7. *Sean $G = G_1 *_N G_2$ y $g \in G$. Si g es un elemento de torsión, entonces es un conjugado de un elemento de torsión de G_1 ó G_2.*

Demostración. Si $h \in G$ es un elemento cíclicamente reducido, sin pérdida de generalidad $h = na_1b_1 \dots a_mb_m$, para $n \in N$ y $a_1, \dots, a_m \in G_1$, $b_1, \dots, b_m \in G_2$, cada uno en un transversal derecho de G_1 ó G_2 sobre N, respectivamente, y todos diferentes de 1. Entonces

$$h^2 = (na_1b_1 \cdots a_mb_m)(na_1b_1 \cdots a_mb_m).$$

Como b_m es un representante de una clase lateral derecha distinta de N, entonces existe b'_m en el transversal derecho de G_2 diferente de 1 tal que $b_mn = n_{2,m}b'_m$, es decir,

$$h^2 = na_1b_1 \cdots a_mn_{2,m}b'_ma_1b_1 \cdots a_mb_m.$$

Sucesivamente se repite el proceso y se tiene

$$h^2 = n'a'_1b'_1 \cdots a'_mb'_ma_1b_1 \cdots a_mb_m,$$

donde $n' \in N$ y $a'_1, \dots, a'_m \in G_1$, $b'_1, \dots, b'_m \in G_2$ son transversales derechos distintos de 1. Por lo tanto, $\text{long}(h^2) = 2\text{long}(h)$. Igualmente se vería $\text{long}(h^r) = r\text{long}(h)$, para cada $r \in \mathbb{N}$, por lo que $h^r \neq 1$ para cada $r \in \mathbb{N}$.

Ahora, si g es conjugado de $f \in G$, entonces existe $k \in G$ tal que $f = kgk^{-1}$. Si $g^r = 1$ para cierto $r \in \mathbb{Z}$, entonces

$$f^r = (kgk^{-1})^r = kg^rk^{-1} = 1.$$

Por la proposición anterior, g es conjugado a un elemento cíclicamente reducido o a un elemento de G_1 o de G_2. Pero ya que los elementos cíclicamente reducidos no son de torsión, este caso no es posible. Debe suceder entonces, $g = k^{-1}fk$, con $f \in G_1$ ó $f \in G_2$. Ya que $g \neq 1$, también $f \neq 1$ y por lo visto antes, ya que g es de torsión, f es de torsión, lo que completa el resultado. □

Corolario 1.3.8. *Si G_1 y G_2 son libres de torsión y $N \leq G_1, G_2$, entonces $G_1 *_N G_2$ es libre de torsión.*

1.4 Anillos

Los anillos aparecieron originalmente como una generalización de los números enteros. Sin embargo, en ocasiones existe cierta discrepancia en su definición exacta, pues se suelen definir de acuerdo a los puntos convenientes de cada autor. En este texto, se usa la siguiente definición.

Definición 1.4.1. *Un **anillo** es una terna $(R, +, \cdot)$, donde R es un conjunto no vacío y $+, \cdot$ son operaciones binarias en R de manera que $(R, +)$ es un grupo abeliano, y las siguientes propiedades se cumplen.*

- $r \cdot (s \cdot t) = (r \cdot s) \cdot t$, *para cada* $r, s, t \in R$,
- *Existe* $1 \in R$ *no cero tal que* $1 \cdot r = r \cdot 1 = r$, *para cada* $r \in R$,
- $r \cdot (s + t) = r \cdot s + r \cdot t$ *y* $(s + t) \cdot r = s \cdot r + t \cdot r$, *para cada* $r, s, t \in R$.

Si no hay ambigüedad, la terna $(R, +, \cdot)$ se denota simplemente como R y la operación $a \cdot b$ se denota simplemente como ab. También es importante aclarar que el neutro aditivo de $(R, +)$ se denota 0. Si $ab = ba$ para cada $a, b \in R$, se dice que R es un **anillo conmutativo**.

En algunos textos, la segunda condición se omite y se reserva para los anillos con elemento unitario, cuya definición es justo la que se dio antes para anillo. Aquí parece favorable considerar que los anillos tienen este elemento unitario, principalmente en orientación a los anillos de grupo que se verán a lo largo del texto.

Ya que un anillo R es un grupo bajo la operación suma, R hereda los resultados ya conocidos sobre grupos bajo esta operación, lo relevante entonces en un anillo es el análisis de la operación producto y la conexión que hay entre las dos operaciones.

Un caso particular relevante de anillo, son los campos. En general, un anillo K es un **campo** si sus elementos diferentes de cero forman un grupo abeliano bajo la operación producto. En un anillo R cualquiera, si un elemento tiene inverso se dice que el elemento es una **unidad** en R. Es decir, si $r \in R$ es tal que existe $s \in R$ que cumple $rs = sr = 1$, entonces se dice que r es una unidad en R. Para cada $n \in \mathbb{N}$ se hace la siguiente identificación:

$$n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ veces}}.$$

Si existe $n \in \mathbb{N}$ tal que $n = 0$ en R, se define la **característica** de R como $\text{char}(R) = \text{mín}\{n \in \mathbb{N} \mid n = 0\}$. Si no existe tal n, se dice que la característica de R es cero y se denota $\text{char}(R) = 0$.

Proposición 1.4.2. *Sea R un anillo conmutativo de característica un número primo p. Si $a, b \in R$, entonces,*

$$(a + b)^p = a^p + b^p.$$

Demostración. El teorema del binomio es válido en general para anillos conmutativos, por lo que se puede escribir la potencia del binomio en la forma

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k.$$

Si $1 < k < p$, entonces $k, p - k < p$, por lo que al ser p un número primo, p no divide a $k!$ ni a $(p - k)!$. Así, en la siguiente expresión

$$\binom{p}{k} = \frac{p!}{k!(p - k)!},$$

no puede ser cancelado p, por lo que $\binom{p}{k}$ es un múltiplo de p. Ya que R es un anillo de característica p, entonces $\binom{p}{k} = 0$ y por lo tanto,

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k = a^p + b^p + 0 = a^p + b^p,$$

que es el resultado deseado. □

Si un subconjunto S de R es un anillo bajo las mismas operaciones de R, se dice que S es un **subanillo** de R. Si I es un subconjunto de R que es un subgrupo bajo la operación suma y además, $ri \in I$ ($ir \in I$) para cada $r \in R, i \in I$, se dice que I es un **ideal izquierdo** (**derecho**) de R. Si I es un ideal derecho e izquierdo, se dice simplemente que I es un ideal de R. Un ideal $I \neq R$ es **maximal** en R si siempre que existe un ideal J tal que $I \subseteq J \subseteq R$, entonces, $J = I$ ó $J = R$.

Proposición 1.4.3. *Si I es un ideal de R, el cociente R/I de grupos, es un anillo con las operaciones*

$$(I+r)+(I+s)=I+(r+s),$$
$$(I+r)(I+s)=I+rs.$$

Proposición 1.4.4. *Si $\mathcal{A}$ es una colección de ideales en R, entonces $\cap\mathcal{A}$ es un ideal en R.*

Uno de los principales problemas que suelen surgir en la teoría de anillos, tiene que ver con los divisores, principalmente de cero, en un anillo R. Un elemento $r \neq 0$ es un **divisor de cero** si existe $s \in R$ distinto de cero tal que $rs = 0$ ó $sr = 0$. Se descarta el caso $r = 0$, pues de hecho, si $s \in R$, entonces $0s = (0+0)s = 0s + 0s$, lo cual implica $0 = 0s$ y análogamente, $s0 = 0$. Si $r \neq 0$ no es divisor de cero, se dice que r es un **elemento regular** en R y si R no tiene divisores de cero, se dice que R es un **dominio entero**.

Como observación importante, todo campo es un dominio entero, pues si $rs = 0$, con $r \neq 0$, entonces $0 = r^{-1}0 = r^{-1}rs = s$. Dicho comportamiento no se cumple en cualquier anillo.

Definición 1.4.5. *Un anillo R es **primo** si para cualesquiera $r, s \in R$ distintos de cero, existe $t \in R$ tal que $rts \neq 0$.*

En ocasiones, la definición de anillo primo aparece en términos de ideales. Para ello, primero se define que un **ideal primo** I en R es aquel tal que si A, B son ideales en R tales que $AB \subseteq I$, entonces $A \subseteq I$ ó $B \subseteq I$.

Proposición 1.4.6. *Un anillo R es primo si y sólo si $\{0\}$ es un ideal primo.*

Demostración. Supongamos que R no es primo. Entonces existen $r, s \in R$ distintos de cero tales que $rRs = \{0\}$. Los conjuntos RrR y RsR, de sumas finitas de elementos de la forma xry y wsz con $x, y, w, z \in R$ respectivamente, son ideales. Pero si $a \in RrR$ y $b \in RsR$, entonces

$$ab = \left(\sum_{i=1}^{n} a_{il} r a_i\right)\left(\sum_{i=1}^{m} b_{jl} s b_j\right) = \sum_{i=1}^{n}\sum_{i=1}^{m} a_{il}(r a_i b_{jl} s) b_j = \sum_{i=1}^{n}\sum_{i=1}^{m} a_{il}(0) b_j = 0,$$

donde $\{a_{il}\}_{i=1}^{n}, \{a_i\}_{i=1}^{n}, \{b_{jl}\}_{j=1}^{m}, \{b_j\}_{j=1}^{m} \subseteq R$. Por lo que $RrR \cdot RsR = \{0\}$. Pero $r \in RrR$ y $s \in RsR$ son distintos de cero, así que estos ideales no son triviales y por lo tanto $\{0\}$ no es ideal primo.

Supongamos que $\{0\}$ no es ideal primo. Entonces existen ideales $A, B \neq \{0\}$ tales que $AB = \{0\}$. En particular, $ARB \subseteq AB = \{0\}$, por lo que si $a \in A$, $b \in B$ son distintos de cero (existen tales elementos porque $A, B \neq \{0\}$), entonces $arb = 0$ para cada $r \in R$. Es decir, R no es primo. □

Ejemplo 1.4.7. *El ejemplo más clásico de anillo es el conjunto $\mathbb{Z}$ de los números enteros, el cual es un anillo conmutativo con las operaciones habituales. En el caso de $\mathbb{Z}$, todos sus ideales son de la forma $n\mathbb{Z}$ con n entero no negativo, y sus ideales primos son $0\mathbb{Z}, \mathbb{Z}$ e ideales de la forma $p\mathbb{Z}$ para números primos p.*

Para cada $n \geq 2$, el cociente de $\mathbb{Z}$ con algún ideal $n\mathbb{Z}$, denotado por $\mathbb{Z}/n\mathbb{Z}$, es un anillo conocido como los enteros módulo n. Si n es un número primo, $\mathbb{Z}/n\mathbb{Z}$ es un campo conocido como el campo finito con n elementos y se denota $\mathbb{F}_n$.

Definición 1.4.8. *Sea R un anillo. Un $\mathbf{R}-$**módulo** M es un grupo abeliano, bajo la operación $+$, tal que existe un producto $M \times R \to M$, $(m, r) \mapsto mr$ que cumple lo siguiente.*

- $(m_1 + m_2)r = m_1 r + m_2 r$, *para cada $r \in R$ y $m_1, m_2 \in M$.*
- $m(r_1 + r_2) = mr_1 + mr_2$, *para cada $r_1, r_2 \in R$ y $m \in M$.*

- $(mr_1)r_2 = m(r_1r_2)$, *para cada* $r_1, r_2 \in R$ *y* $m \in M$.
- $m = m1$, *para cada* $m \in M$.

Como observación importante, en realidad todo anillo R es un $R-$módulo con la operación dada por multiplicar. Un **submódulo** N de M es un subconjunto de M que es módulo con las mismas operaciones de M. Si N es un submódulo de M, entonces el cociente de grupos M/N es de nuevo un módulo. Si M, N son $R-$módulos, una funcón $\phi\colon M \to N$ es un **homomorfismo de módulos** si es un homomorfismo de grupos y cumple $\phi(mr) = \phi(m)r$, para cada $r \in R$ y $m \in M$. Si ϕ es biyectiva, se dice que M y N son isomorfos.

2 El Anillo de Grupo

En el estudio de la teoría de grupos aparecen diversos sistemas que ayudan con el estudio de los grupos. Algunos por ejemplo, intentan ver la estructura simple de grupo en alguna otra que se ha estudiado con más detalle.

El anillo de grupo precisamente es un anillo que se obtiene a partir de un grupo, donde este grupo queda encajado en el grupo de unidades. Diversas propiedades se estudian sobre esta estructura. En este capítulo se define precisamente la noción de anillo de grupo y se presentan diversas propiedades que el anillo de grupo satisface de acuerdo al grupo sobre el que se construye.

2.1 Definición

Sea G un grupo y R un anillo. A cada elemento $g \in G$ se le asocia un único $r_g \in R$, de tal manera que solo finitos elementos r_g sean diferentes de cero. Se toman entonces las sumas formales

$$r = \sum_{g \in G} r_g g. \tag{2.1}$$

Sea RG el conjunto de las sumas formales definidas anteriormente, se dice entonces que RG es un **anillo de grupo**. En efecto, RG es un anillo si se definen las operaciones suma y producto de la siguiente manera:

$$\left(\sum_{g \in G} r_g g\right) + \left(\sum_{g \in G} s_g g\right) = \sum_{g \in G} (r_g + s_g) g,$$
$$\left(\sum_{g \in G} r_g g\right) \cdot \left(\sum_{g \in G} s_g g\right) = \sum_{g \in G} \left(\sum_{h \in G} r_h s_{h^{-1}g}\right) g = \sum_{g,h \in G} r_g s_h (gh).$$

Normalmente, tanto el elemento neutro de G, como el elemento neutro multiplicativo de R se denotan por 1 y se identifica $g = 1g$ para cada $g \in G$ y $r = r1$ para cada $r \in R$. También, en (2.1) se omite escribir los sumandos $r_g g$ tales que $r_g = 0$ y el elemento en RG tal que todas sus entradas son cero,

$$\sum_{g \in G} 0g,$$

se denota simplemente como 0.

También es importante aclarar que RG puede ser visto como lo que se conoce como un R-módulo libre, con generadores igual al conjunto G. Desde este punto de vista, los elementos del grupo G son linealmente

independientes, es decir, forman una base. Para más información sobre esto, se puede consultar principalmente [29] y [30].

De hecho, la suma y el producto se comportan de la forma agradable que se esperaría que se comportaran, como si cada elemento de RG fuera un polinomio sobre R y las variables fueran los elementos del grupo, dejando conmutar los elementos del anillo R con los elementos del grupo G. Además, con las identificaciones anteriores, se tiene que R es un subanillo de RG y G se sigue comportando de la misma manera con la operación de multiplicación de RG.

Ejemplo 2.1.1. *Sea $G = \langle b \mid b^2 = 1\rangle$. Entonces se tiene que $\mathbb{F}_2G = \{0, 1, b, 1+b\}$. Las operaciones suma y producto están dadas por las siguientes tablas.*

$\cdot$	0	1	b	$1+b$
0	0	0	0	0
1	0	1	b	$1+b$
b	0	b	1	$1+b$
$1+b$	0	$1+b$	$1+b$	0

$+$	0	1	b	$1+b$
0	0	1	b	$1+b$
1	1	0	$1+b$	b
b	b	$1+b$	0	1
$1+b$	$1+b$	b	1	0

Ejemplo 2.1.2. *Como se mencionó antes, las operaciones se comportan análogamente a como se comportan en un anillo de polinomios. De hecho, pueden ser vistos como un caso particular, pues si $\langle x\rangle$ es el grupo libre generado por x, entonces el anillo de polinomios $\mathbb{Z}[x]$ puede ser inyectado dentro de $\mathbb{Z}\langle x\rangle$ y las operaciones coinciden.*

Ejemplo 2.1.3. *En general, para cualquier grupo G, el anillo $\mathbb{F}_2G$ es el conjunto de sumas finitas formales de los elementos del grupo, con la condición de que $g + g = 0$ para cada $g \in G$.*

Otra manera de ver el anillo de grupo es verlo como un conjunto de funciones. Es decir, para R un anillo y G un grupo, se considera el conjunto R^G de funciones de G a R y se define $\mathbf{sop}\colon R^G \to \mathcal{P}(G)$, donde $\mathcal{P}(G)$ es el conjunto potencia de G, como

$$\mathbf{sop}(r) = \{g \in G \mid r(g) \neq 0\}.$$

Entonces

$$RG = \{r \in R^G \mid |\mathbf{sop}(r)| < \infty\}.$$

Ver el anillo de grupo de esta forma permite darle otra perspectiva al anillo de grupo. En este caso, si $r, s \in RG$, entonces las operaciones definidas antes pueden verse como las funciones $r + s, rs \in RG$ tales que

$$\begin{aligned}(r+s)(g) &= r(g) + s(g), \quad \forall g \in G,\\ (rs)(g) &= \sum_{h\in G} r(h)s(h^{-1}g), \quad \forall g \in G.\end{aligned}$$

Bajo esta forma de ver el anillo de grupo, habría que verificar que en efecto, $r+s$ y rs son tales que $|\mathbf{sop}(r+s)|, |\mathbf{sop}(rs)| < \infty$. Es claro que sólo una cantidad finita de elementos $g \in G$ (máximo $|\mathbf{sop}(r)| + |\mathbf{sop}(s)|$) no satisfacen $r(g) = s(g) = 0$, que implica $(r + s)(g) = 0$. Aunque un poco más complicado, también es posible ver que sólo una cantidad finita de elementos $g \in G$ (máximo $|\mathbf{sop}(r)||\mathbf{sop}(s)|$) no satisfacen que siempre que $ab = g$ para algunos $a, b \in G$, entonces, $r(a) = 0$ ó $s(b) = 0$. Y si g satisface esto, entonces para cada $h \in G$, $h \cdot h^{-1}g = g$ y por lo tanto, $r(h) = 0$ ó $s(h^{-1}g) = 0$. En cualquier caso, $(rs)(g) = 0$.

En la notación de (2.1), simplemente se consideraría en este caso $r(g) = r_g$ y las operaciones funcionan de la misma manera. En realidad, muchas veces se utilizan expresiones del tipo $r_1g + r_2g \in RG$ con $r_1, r_2 \in R$,

pero siempre es posible llevarlas a una forma más adecuada, sin repeticiones en los elementos de G, en este caso, $r_1g + r_2g = (r_1 + r_2)g$. Esta forma será la que se usará como estándar, pero cuando sea útil, también será utilizada la otra forma.

La función **sop** usada antes se llama **soporte**. Para cada $r \in RG$, se pronuncia $\mathbf{sop}(r)$ como el soporte de r y en la forma (2.1), se puede reescribir como

$$\mathbf{sop}(r) := \{g \in G \mid r_g \neq 0\}.$$

2.2 Funciones Básicas

En el estudio de los anillos de grupo, hay ciertas funciones relevantes que ayudan en el entendimiento del comportamiento de estas estructuras a partir de los grupos y/o anillos de los que se forman. En esta sección, se desarrollan propiedades, principalmente vistas en [6] y [26]. Si G es un grupo y R un anillo, se denota por $L(G)$ al conjunto de subgrupos de G y por $L_r(R)$ al conjunto de ideales derechos de R.

Definición 2.2.1. *Sea G un grupo, H un subgrupo de G y R un anillo. Se definen las siguientes funciones.*

a) $\omega\colon L(G) \to L_r(RG)$ *como* $\omega(H) = \{1 - h \mid h \in H\}RG$, *es decir, el ideal derecho generado por* $\{1 - h \mid h \in H\}$.

b) $\Omega\colon L_r(RG) \to L(G)$ *como* $\Omega(I) = \{h \in G \mid 1 - h \in I\}$.

c) $\omega_1\colon L_r(R) \to L_r(RG)$ *como* $\omega_1(I) = I(RG)$.

d) $\Omega_1\colon L_r(RG) \to L_r(R)$ *como* $\Omega_1(I) = I \cap R$.

e) $\phi_H\colon RG \to R(G/H)$ *como* $\phi_H(\sum r_g g) = \sum r_g Hg$.

f) $\varphi_I\colon RG \to (R/I)G$ *como* $\varphi_I(\sum r_g g) = \sum (I + r_g)g$.

g) $\pi_H\colon RG \to RH$ *como* $\pi_H(\sum_{g\in G} r_g g) = \sum_{g\in H} r_g g$.

h) $\varepsilon\colon RG \to R$ *como* $\varepsilon(\sum r_g g) = \sum r_g$.

Es importante aclarar que en la anterior definición, la función Ω está bien definida, es decir, que si I es un ideal derecho en RG, entonces $\{h \in G \mid 1 - h \in I\}$ es un subgrupo de G. Lo anterior se probará en la Proposición 2.2.2. Además, como G/H se toma solo el conjunto de clases laterales derechas de H en G y se le da estructura de grupo sólo si H es normal en G. En ese caso, $R(G/H)$ es simplemente el R-módulo libre con base G/H, y es un anillo de grupo si y sólo si G/H es un grupo.

Proposición 2.2.2. *Si I es un ideal derecho en RG, entonces, $\Omega(I)$ es un subgrupo de G.*

Demostración. Sean $g, g' \in \Omega(I)$. Entonces

$$1 - g^{-1}g' = 1 - g^{-1}g' + gg^{-1}g' - g' = (1 - g)(-g^{-1}g') + (1 - g') \in I,$$

ya que $1 - g, 1 - g'$ son elementos del ideal derecho I. Así, $g^{-1}g' \in \Omega(I)$. Además, $1 - 1 = 0 \in I$, luego $1 \in \omega(I)$. Entonces $\Omega(I)$ es no vacío y por lo tanto, $\Omega(I)$ es subgrupo de G. □

Proposición 2.2.3. *Sea G un grupo y $H \leq G$. Entonces $\phi_H \colon RG \to R(G/H)$ es un R-homomorfismo y* $\ker(\phi_H) = \omega(H)$.

Demostración. Se tiene que si $\alpha \in R$,

$$\begin{aligned}\phi_H\left(\sum r_g g + \alpha \sum s_g g\right) &= \phi_H\left(\sum (r_g + \alpha s_g) g\right) \\ &= \sum (r_g + \alpha s_g) Hg \\ &= \sum r_g Hg + \alpha \sum s_g Hg \\ &= \phi_H\left(\sum r_g g\right) + \alpha \phi_H\left(\sum s_g g\right),\end{aligned}$$

cumpliendo así con ser ϕ_H un R-homomorfismo. Ahora bien, si $h \in H$, $g \in G$, entonces

$$\phi_H((1-h)g) = \phi_H(h) - \phi_H(hg) = Hg - Hhg = Hg - Hg = 0.$$

Si $z \in \omega H$, entonces por definición $z = \sum r_{(1-h)g}(1-h)g$ para algunos $h \in H$ y $g \in G$. Por lo tanto, de lo anterior, $\phi_H(z) = \phi_H(\sum r_{(1-h)g}(1-h)g) = 0$, es decir, $\omega H \subseteq \ker(\phi_H)$. Sea ahora $z \in \ker(\phi_H)$, entonces

$$0 = \phi_H(z) = \phi_H\left(\sum r_g g\right) = \sum r_g Hg.$$

Sea K un conjunto de representantes de clases laterales de G/H, entonces

$$0 = \phi_H(r) = \sum r_g Hg = \sum_{g \in K} \left(\sum_{h \in H} r_{hg} \right) Hg.$$

Puesto que se eligió un solo representante para cada clase y las clases son linealmente independientes entre sí, lo anterior sucede si y sólo si

$$\sum_{h \in H} r_{hg} = 0 \quad \forall g \in K.$$

Así,

$$\begin{aligned} z &= \sum_{g \in K} \left(\sum_{h \in H} r_{hg} hg \right) \\ &= \sum_{g \in K} \left(\sum_{h \in H} r_{hg} hg - 0 \right) \\ &= \sum_{g \in K} \left(\sum_{h \in H} r_{hg} hg - \sum_{h \in H} r_{hg} g \right) \\ &= \sum_{g \in K} \sum_{h \in H} (1-h)(-r_{hg} g) \in \omega(H), \end{aligned}$$

lo que implica $\ker(\phi_H) \subseteq \omega(H)$ y por lo tanto, $\ker(\phi_h) = \omega(H)$. □

Proposición 2.2.4. *Para un anillo de grupo RG y $H \leq G$, se tiene $g \in H$ si y sólo si* $1 - g \in \omega(H)$.

Demostración. Por definición, si $g \in H$, entonces $1 - g \in \omega(H)$. Mediante la contrarrecíproca, si $g \notin H$, entonces, $\phi_H(1-g) = H - Hg \neq 0$, por lo que $1 - g \notin \ker(\phi_H) = \omega(H)$. □

Proposición 2.2.5. *Sea G un grupo y $H \leq G$. Entonces $\omega(H)$ es un ideal si y sólo si H es normal en G.*

Demostración. Supongamos que H es normal. Cada elemento $t \in \omega(H)$ puede ser escrito como

$$t = \sum_{h \in H} \left((1-h) \sum_{g \in G} r_{h,g} g \right),$$

por lo que si $s \in RG$,

$$st = \left(\sum_{g \in G} s_g g \right) \sum_{h \in H} \left((1-h) \sum_{k \in G} r_{h,k} k \right) = \sum_{g \in G} \sum_{h \in H} g(1-h) \sum_{k \in G} s_g r_{h,k} k.$$

Notemos que $g(1-h) = g - gh = g - ghg^{-1}g = (1 - ghg^{-1})g$, donde $ghg^{-1} \in H$ por ser H normal. Entonces

$$st = \sum_{g \in G} \sum_{h \in H} g(1-h) \sum_{k \in G} s_g r_{h,k} k = \sum_{g \in G} \sum_{h \in H} (1 - ghg^{-1}) \sum_{k \in G} s_g r_{h,k} gk \in \omega(H),$$

ya que por definición $\omega(H)$ es ideal derecho. De lo anterior, también es ideal izquierdo y entonces es un ideal. Si $\omega(H)$ es un ideal, dados $h \in H$ y $g \in G$, se tiene

$$1 - g^{-1}hg = g^{-1}h(1 - h^{-1})(-g) \in \omega(H).$$

Entonces $g^{-1}hg \in H$ por la proposición anterior, y por lo tanto, H es normal en G. □

Proposición 2.2.6. *Sea R un anillo e I un ideal derecho de R. Entonces φ_I es un homomorfismo de anillos y*

$$\ker(\varphi_I) = \omega_1(I).$$

Demostración. Para cada $r \in RG$, se tiene $\varphi_I(r) = 0$ si y sólo si cada una de sus entradas es cero en R/I, esto es, si $I + r_g = I$ para cada $g \in G$. Pero esto es equivalente a decir que $r_g \in I$ para cada $g \in G$ y por lo tanto

$$\ker(\varphi_I) = \{r \in RG \mid r_g \in I, \forall g \in G\}.$$

Por otro lado, I es un ideal derecho de R, por lo que $Is = I$ para cada $s \in R$. Entonces

$$\omega_1(I) = \{r \in RG \mid r_g \in I, \forall g \in G\},$$

lo que implica que $\ker(\varphi_I) = \omega_1(I)$. □

Si H es un subgrupo normal de G, entonces G/H tiene una estructura de grupo, por lo que $R(G/H)$ es de hecho un anillo de grupo. Más aún, por su definición, ϕ_H es una función sobreyectiva y por la Proposición 2.2.3 tiene núcleo igual a ωH, análogamente y por la proposición anterior, φ_I es una función sobreyectiva y con núcleo igual a $\omega_1(I)$. Entonces, por el primer teorema de isomorfismo se obtiene el siguiente resultado.

Proposición 2.2.7. *Sea G un grupo y R un anillo.*

- *Si H es un subgrupo normal de G,*

$$R(G/H) \cong RG/\ker(\phi_H) \cong (RG)/\omega(H).$$

- *Si I es un ideal derecho de R,*

$$(R/I)G \cong RG/\ker(\varphi_I) \cong (RG)/\omega_1(I).$$

El anterior es un resultado relevante, pues dice que hacer cocientes sobre el anillo o grupo original, da como resultado también cocientes del anillo de grupo.

La función ε de la definición 2.2.1 es normalmente llamada **función de aumentación** y es relevante para el estudio de los anillos de grupo. Denotaremos $\mathcal{I} := \ker(\varepsilon)$. De hecho, por la siguiente proposición y la Proposición 2.2.5, se tiene que $\mathcal{I}$ es un ideal, llamado normalmente **ideal de aumentación**.

Proposición 2.2.8. *Para todo anillo de grupo RG, se cumple $\mathcal{I} = \omega(G)$.*

Demostración. Por la Proposición 2.2.3, se tiene $\omega(G) = \ker(\phi_G)$. Entonces, si $r \in \omega(G)$,

$$0 = \phi_G(r) = \phi_G\left(\sum r_g g\right) = \sum r_g G g = \sum r_g G,$$

lo cual sólo es posible si

$$0 = \sum r_g = \varepsilon(r),$$

por lo que $r \in \mathcal{I}$. Si $r \in \mathcal{I}$, entonces

$$\begin{aligned} r &= \sum r_g g = \sum r_g(1 - 1 + g) = \sum r_g - \sum r_g(1 - g) = \varepsilon(r) - \sum r_g(1 - g) \\ &= -\sum r_g(1 - g) \in \omega(G). \end{aligned}$$

como queríamos probar. □

Gracias a la definición de soporte, es posible ver que si $H \leq G$ y R es un anillo, entonces

$$RH = \{r \in RG \mid \mathbf{sop}(r) \subseteq H\}.$$

Además, observando cómo se ve un subgrupo H de G en el anillo de grupo, se tiene la siguiente proposición.

Proposición 2.2.9. *Sea H un subgrupo de G y sean $r, s \in RG$, $t \in RH$. Entonces se cumplen las siguientes tres propiedades.*

a) $\pi_H(\alpha r + s) = \alpha\pi_H(r) + \pi_H(s)$, *para todo* $\alpha \in R$.

b) $\pi_H(tr) = t\pi_H(r)$.

c) $\pi_H(rt) = \pi_H(r)t$.

Demostración. Es posible separar r, s de manera que $r = \pi_H(r) + r_1$ y $s = \pi_H(s) + s_1$ para algunos $r_1, s_1 \in RG$ tales que $\mathbf{sop}(r_1) \cap H = \mathbf{sop}(s_1) \cap H = \varnothing$. De esta manera,

$$\alpha r + s = \alpha(\pi_H(r) + r_1) + (\pi_H(s) + s_1) = (\alpha\pi_H(r) + \pi_H(s)) + r_1 + s_1,$$

donde $\mathbf{sop}(r_1 + s_1) \cap H = \varnothing$ y por lo tanto,

$$\pi_H(\alpha r + s) = \alpha\pi_H(r) + \pi_H(s).$$

Ahora bien, como antes sea $r = \pi_H(r)+r_1$ con $r_1 \in RG$ tal que $\mathbf{sop}(r_1)\cap H = \varnothing$. Entonces $tr = t\pi_H(r)+tr_1$. Ya que $t, \pi_H(r) \in RH$, por la estructura de anillo de RH, se tiene que $t\pi_H(r) \in RH$. Ahora, si ocurriera $\mathbf{sop}(tr_1) \cap H \neq \varnothing$, entonces existiría un $h \in H$ y $g \in G\backslash H$ tal que $hg \in H$ y por lo tanto, $g \in h^{-1}H = H$, una contradicción. Así, $\mathbf{sop}(tr_1) \cap H = \varnothing$ y $\pi_H(tr) = t\pi_H(r)$. Análogamente, $\pi_H(rt) = \pi_H(r)t$. □

Proposición 2.2.10. *Sea H un subgrupo de G y $r \in RH$. Entonces,*

a) r es invertible en RH si y sólo si es invertible en RG.

b) r es divisor de cero en RH si y sólo si es divisor de cero en RG.

Demostración. Se tiene que $RH \subseteq RG$, por lo que si un elemento es invertible o divisor de cero en RH, lo será en RG. Supongamos que r es invertible en RG. Entonces, existe $r^{-1} \in RG$ tal que $rr^{-1} = r^{-1}r = 1$. Por la proposición anterior se tiene

$$r\pi_H(r^{-1}) = \pi_H(rr^{-1}) = \pi_H(1) = 1 = \pi_H(1) = \pi_H(r^{-1}r) = \pi_H(r^{-1})r.$$

Así, $\pi_H(r^{-1})$ es el inverso de r en RH.

Ahora, si r es divisor de cero en RG, existe $s \in RG$ con $s \neq 0$ tal que $rs = 0$. Sea $g \in \mathbf{sop}(s)$, el cual es no vacío ya que $s \neq 0$. Entonces $1 \in \mathbf{sop}(sg^{-1})$ y por lo tanto, $\pi_H(sg^{-1}) \neq 0$. Ahora $\pi_H(sg^{-1}) \in RH$, pero por la proposición anterior,

$$r\pi_H(sg^{-1}) = \pi_H(rsg^{-1}) = \pi_H(0g^{-1}) = \pi_H(0) = 0,$$

completando el resultado. □

2.3 Primicidad

Esta sección sirve para dar a conocer un resultado que caracteriza los anillos de grupo primos sobre anillos conmutativos. El resultado principal de esta sección hace un gran uso de índices de un grupo con respecto a un subgrupo. Por ello, comenzamos primero con una proposición preliminar para hablar sobre ellos.

Proposición 2.3.1. *Sea G un grupo y $H_1, \ldots, H_n \leq G$.*

a) Si para cada $1 \leq i \leq n$, se tiene $[G : H_i] < \infty$, entonces $\left[G : \bigcap_{i=1}^{n} H_i\right] < \infty$.

b) Si existe un número finito de elementos $\{g_{ij}\}_{i,j} \subseteq G$ tales que

$$G = \bigcup_{i,j} H_i g_{ij}, \tag{2.2}$$

entonces $[G : H_i] < \infty$ para algún i.

Demostración. Veamos cada una de las dos propiedades por separado.

a) Sea $H = \bigcap_{i=1}^{n} H_i$. Para cada $g \in G$, se tiene

$$Hg = H_1 g \cap H_2 g \cap \ldots \cap H_n g,$$

de donde, a lo más, puede haber el producto de la cantidad de clases laterales de cada H_i, es decir,

$$[G : H] \leq [G : H_1][G : H_2] \cdots [G : H_n] < \infty.$$

b) Si $n = 1$, existe un subconjunto de los elementos $\{g_{ij}\}$, que es un conjunto de representantes de clases laterales de H en G. Por lo tanto, $[G : H_1] < \infty$.

Supongamos que $n \geq 2$ y el resultado es cierto para $1 \leq i \leq n-1$. Si en la unión (2.2), están todas las clases laterales de H_n en G, entonces $[G : H_n] < \infty$. En otro caso, existe $g \in G$ tal que $H_n g \cap H_n g_{nj} = \varnothing$ para cada j. Pero ya que

$$H_n g \subseteq G = \bigcup_{i,j} H_i g_{ij},$$

entonces

$$H_n g \subseteq \bigcup_{i \neq n, j} H_i g_{ij}.$$

Pero en este caso, para cada l correspondiente se cumple

$$H_n g_{nl} = H_n g(g^{-1} g_{nl}) \subseteq \bigcup_{i \neq n, j} H_i g_{ij}(g^{-1} g_{nl}),$$

por lo que

$$G = \bigcup_{i,j} H_i g_{ij} \subseteq \left(\bigcup_{l} \bigcup_{i \neq n, j} H_i g_{ij}(g^{-1} g_{nl}) \right) \cup \left(\bigcup_{i \neq n, j} H_i g_{ij} \right) \subseteq G.$$

Es decir,

$$G = \left(\bigcup_{l} \bigcup_{i \neq n, j} H_i g_{ij}(g^{-1} g_{nl}) \right) \cup \left(\bigcup_{i \neq n, j} H_i g_{ij} \right),$$

por lo que G se puede representar como unión finita de clases laterales (como conjuntos) de $H_1, \ldots, H_{n-1}$, lo que implica que $[G : H_i] < \infty$ para algún i. Así, por inducción se tiene el resultado. □

Recordemos que el **centro** $Z(G)$ de un grupo G es el subgrupo de elementos que conmutan con todos los elementos del grupo, es decir,

$$Z(G) = \{g \in G \mid gh = hg \, \forall h \in G\}.$$

Además, el subgrupo **conmutador** (o **grupo derivado**), G', es el subgrupo generado por los conmutadores de G (elementos de la forma $ghg^{-1}h^{-1}$ para $g, h \in G$), es decir,

$$G' = \left\langle \{ghg^{-1}h^{-1} \mid g, h \in G\} \right\rangle.$$

El grupo conmutador es normal y es el subgrupo normal H más pequeño tal que G/H es abeliano. Aunque aquí no se desarrollan estos conceptos, se pueden encontrar en las Secciones 2.5 y 3.1 de [31].

Proposición 2.3.2. *Sea G un grupo tal que $[G : Z(G)] < \infty$. Entonces G' es finito.*

Demostración. Para cada $g, h \in G$, sea $[g, h] = ghg^{-1}h^{-1}$. Entonces

$$[g, h]^{-1} = (ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1} = [h, g],$$

es decir, los inversos de los conmutadores son conmutadores, por lo que G' es el conjunto de multiplicaciones finitas de conmutadores.

Sea $n = [G : Z(G)] = |G/Z(G)|$ y sean $g_1, \dots, g_n \in G$ representantes de las clases laterales de $G/Z(G)$. Si $g, h, \in G$, entonces $g = z_1 g_i, h = z_2 g_j$ para algunos i, j y $z_1, z_2 \in Z(G)$, por lo que

$$[g, h] = ghg^{-1}h^{-1} = (z_1 g_i)(z_2 g_j)(z_1 g_i)^{-1}(z_2 g_j)^{-1} = z_1 g_i z_2 g_j g_i^{-1} z_1^{-1} g_j^{-1} z_2^{-1}.$$

Pero ya que $z_1, z_2 \in Z(G)$, se cumple

$$[g, h] = z_1 g_i z_2 g_j g_i^{-1} z_1^{-1} g_j^{-1} z_2^{-1} = g_i g_j g_i^{-1} g_j^{-1} (z_1 z_1^{-1})(z_2 z_2^{-1}) = g_i g_j g_i^{-1} g_j^{-1} = [g_i, g_j].$$

Es decir, G' es el conjunto de multiplicaciones finitas de los conmutadores de $g_1, \dots, g_n$ (que son a lo más n^2 conmutadores). Ahora bien, si $u \in G'$ es el producto de m de estos conmutadores $u = c_1 \cdots c_m$ y $m > n^3$, ya que hay a lo más n^2 conmutadores, debe haber al menos un conmutador $[g_i, g_j]$ que aparezca al menos $n + 1$ veces. Pero para cada $g, h \in G$, si $c = [g_i, g_j]$, se tiene

$$\begin{aligned} [g, h][g_i, g_j] &= cc^{-1}[g, h][g_i, g_j] = [g_i, g_j]c^{-1}[g, h]c = [g_i, g_j]c^{-1}(ghg^{-1}h^{-1})c \\ &= [g_i, g_j](c^{-1}gc)(c^{-1}hc)(c^{-1}g^{-1}c)(c^{-1}h^{-1}c) \\ &= [g_i, g_j][c^{-1}gc, c^{-1}hc], \end{aligned} \tag{2.3}$$

por lo que reiterando este procedimiento, se puede reescribir $u = [g_i, g_j]^{n+1} c'_1 \cdots c'_{m-n-1}$ para algunos conmutadores $c'_1, \dots, c'_{m-n-1}$. A su vez, ya que $|G/Z(G)| = n$, en $G/Z(G)$ se cumple

$$Z(G) = (Z(G)[g_i, g_j])^n = Z(G)[g_i, g_j]^n,$$

por lo que $[g_i, g_j]^n \in Z(G)$. Así,

$$\begin{aligned} [g_i, g_j]^{n+1} &= [g_i, g_j]^n g_i g_j g_i^{-1} g_j^{-1} = g_i [g_i, g_j]^n g_j g_i^{-1} g_j^{-1} \\ &= g_i [g_i, g_j]^{n-1} (g_i g_j g_i^{-1} g_j^{-1}) g_j g_i^{-1} g_j^{-1} \\ &= g_i [g_i, g_j]^{n-1} g_i g_j g_i^{-2} g_j^{-1} \\ &= g_i [g_i, g_j]^{n-1} (g_i^{-1} g_i) g_i g_j g_i^{-2} g_j^{-1} \\ &= g_i [g_i, g_j]^{n-1} g_i^{-1} g_i^2 g_j g_i^{-2} g_j^{-1} \\ &= g_i [g_i, g_j]^{n-1} g_i^{-1} [g_i^2, g_j] \\ &= [g_i (g_i) g_i^{-1}, g_i (g_j) g_i^{-1}]^{n-1} [g_i^2, g_j] \\ &= [g_i, g_i g_j g_i^{-1}]^{n-1} [g_i^2, g_j] \end{aligned}$$

donde el conjugado se "introduce" en el conmutador de manera análoga a como en (2.3). Así,

$$u = [g_i, g_j]^{n+1} c'_1 \cdots c'_{m-n-1} = [g_i, g_i g_j g_i^{-1}]^{n-1} [g_i^2, g_j] c'_1 \cdots c'_{m-n-1},$$

por lo que u es producto de $(n-1)+1+(m-n-1)=m-1$ conmutadores. Realizando el proceso anterior repetidamente mientras la cantidad de multiplicaciones sea mayor a n^3, se llega a que u puede ser expresado como multiplicación de a lo más n^3 conmutadores.

Así, como G' es el conjunto de multiplicaciones finitas de conmutadores, cada elemento de G' puede ser expresado como una multiplicación de a lo más n^3 conmutadores. Ya que hay a lo más n^2 conmutadores, $|G'| \leq (n^2)^{n^3}$, obteniendo así el resultado. □

Las siguientes definiciones serán muy útiles para el resultado principal de esta sección junto con la Proposición 2.3.1, sobre todo mediante las Proposición 2.3.3, para la cual es importante la proposición anterior. Sea ahora

$$\Delta(G) = \{g \in G \mid [G : C_G(g)] < \infty\}.$$

Equivalentemente, $\Delta(G)$ es el subconjunto de G de los elementos que tienen una cantidad finita de conjugados. A su vez, sea

$$\Delta^+(G) = \{g \in G \mid [G : C_G(g)] < \infty \text{ y } o(g) < \infty\}.$$

Proposición 2.3.3. *Sea G un grupo.*

a) $\Delta(G), \Delta^+(G) \trianglelefteq G$.

b) $\Delta^+(G) \trianglelefteq \Delta(G)$ *y* $\Delta(G)/\Delta^+(G)$ *es abeliano y libre de torsión.*

c) $\Delta^+(G) = 1$ *si y sólo si G no tiene subgrupos finitos normales no triviales.*

Demostración. Lo probamos inciso a inciso.

a) Sean $x, y \in \Delta(G)$ y $g \in G$. Se tiene

$$g^{-1}xy^{-1}g = g^{-1}xgg^{-1}y^{-1}g = g^{-1}xg\left(g^{-1}yg\right)^{-1},$$

por lo que cada conjugado de xy^{-1} es un múltiplo de un conjugado de x y un inverso de un conjugado de y. Entonces $|G/C_G(xy^{-1})| \leq |G/C_G(x)||G/C_G(y)| < \infty$, por lo que $xy^{-1} \in \delta(G)$ y $\Delta(G) \leq G$.

Sean $g, h \in \Delta^+(G)$ y $H = \langle g, h\rangle$. Ya que $C_G(h), C_G(g)$ son el conjunto de elementos en G que conmutan con h, g, respectivamente y g, h generan a H, entonces

$$Z(H) = H \cap C_G(g) \cap C_G(h).$$

Ya que $g, h \in \Delta^+(G)$, por definición, $[G : C_G(g)], [G : C_G(h)] < \infty$ y por la Proposición 2.3.1, se cumple $[G : C_G(g) \cap C_G(h)] < \infty$, por lo cual,

$$\infty > [G : C_G(g) \cap C_G(h)] \geq [H : H \cap C_G(g) \cap C_G(h)] = [H : Z(H)].$$

Entonces, por la Proposición 2.3.2, obtenemos que H' es finito. Además, H/H' es un grupo abeliano con dos generadores de torsión, por lo que H/H' está encajado en $(\mathbb{Z}/o(g)\mathbb{Z}) \oplus (\mathbb{Z}/o(h)\mathbb{Z})$. En particular, H/H' es finito. Puesto que H/H' y H' son finitos, entonces H es finito y por lo tanto, $gh^{-1} \in \langle g, h\rangle$ es de torsión, lo que implica que $gh^{-1} \in \Delta^+(G)$. Así probamos que $\Delta^+(G) \leq G$.

Sean $g \in G$ y $x \in \Delta(G)$. Para cada $h \in G$, se tiene

$$h(gxg^{-1})h^{-1} = (hg)x(hg)^{-1},$$

por lo que todo conjugado de gxg^{-1} define un conjugado de x, y ya que $x \in \Delta(G)$ tiene un número finito de conjugados, gxg^{-1} también debe tener un número finito de conjugados. Es decir, $gxg^{-1} \in \Delta(G)$, lo cual muestra que $\Delta(G) \trianglelefteq G$. Además, si $x^n = 1$, se cumple $(gxg^{-1})^n = gx^ng^{-1} = gg^{-1} = 1$, con lo que $gxg^{-1} \in \Delta^+(G)$. Es decir, $\Delta^+(G) \trianglelefteq G$.

b) $\Delta^+(G) \leq \Delta(G)$ y $\Delta^+(G) \trianglelefteq G$, por lo que $\Delta^+(G) \trianglelefteq \Delta(G)$. De hecho, $\Delta^+(G)$ consiste en los elementos de $\Delta(G)$ que son de torsión, lo que implica que $\Delta^+(G)/\Delta(G)$ es libre de torsión.

Sean $g, h \in \Delta(G)$. De manera análoga al anterior inciso, si $H = \langle g, h\rangle$, entonces H' es finito. En particular, $ghg^{-1}h^{-1} \in H$ es de torsión, por lo que $ghg^{-1}h^{-1} \in \Delta^+(G)$ para cada $g, h \in \Delta(G)$. Así que $\Delta(G)' \subseteq \Delta^+(G)$ y por lo tanto $\Delta(G)/\Delta^+(G)$ es abeliano, completando el inciso.

c) Supongamos que $\Delta^+(G) = 1$. Sea H un subgrupo finito normal de G y $h \in H$. Por ser H normal, para cada $g \in G$, se cumple $g^{-1}hg \in H$, por lo que a lo más hay $|H|$ conjugados de h en G. Es decir, $h \in \Delta(G)$, pero ya que h pertenece a un grupo finito, es de torsión, lo que implica $h \in \Delta^+(G)$ y a su vez, $H = 1$.

Supongamos que $\Delta^+(G) \neq 1$ y sea $g_1 \in \Delta^+(G)$ no trivial. Por definición, existe solo un número finito de conjugados de g_1 en G, digamos $g_2, \ldots, g_n$. Sea $H = \langle g_1, g_2, \ldots, g_n\rangle$. Ya que

$$Z(H) = H \cap C_G(g_1) \cap \ldots \cap C_G(g_n),$$

de manera análoga a la demostración del inciso **a**, siendo $g_1, \ldots, g_n \in \Delta^+(G)$, podemos llegar a que H es finito. Ahora bien, sea $h \in H$ y $x \in G$. Por definición de H, existen $i_1, \ldots, i_m$ tales que

$$h = g_{i_1}g_{i_2}\cdots g_{i_m},$$

de donde

$$x^{-1}hx = x^{-1}(g_{i_1}g_{i_2}\cdots g_{i_m})x = (x^{-1}g_{i_1}x)(x^{-1}g_{i_2}x)\cdots(x^{-1}g_{i_m}x).$$

Ya que cada g_{i_k} es conjugado de g_1, $x^{-1}g_{i_1}x$ es conjugado de g_1, por lo que $x^{-1}g_{i_k}x \in H$ para cada k. Es decir,

$$x^{-1}hx = (x^{-1}g_{i_1}x)(x^{-1}g_{i_2}x)\cdots(x^{-1}g_{i_m}x) \in H,$$

por lo que $H \trianglelefteq G$. Así, ya que $1 \neq g_1 \in H$, concluimos que H es un subgrupo finito normal no trivial de G, lo que completa el inciso.

□

Volviendo ahora con los anillos y hacia el resultado principal de esta sección, recordemos que un anillo primo R es aquel en el que para cualesquiera $r, s \in R$ distintos de cero, existe $\alpha \in R$ tal que $r\alpha s \neq 0$. Equivalentemente, $rRs \neq \{0\}$. En el caso de los anillos conmutativos, si r, s en el anillo son tales que $rs = 0$, entonces, para cada t en el anillo, $rts = rst = 0t = 0$, por lo que de hecho, si R es un anillo con divisores de cero (distintos de cero), entonces debe ser no primo. En este sentido se tiene la última proposición preliminar.

Proposición 2.3.4. *Sea R un anillo primo conmutativo y G un grupo libre de torsión abeliano. Entonces RG no tiene divisores de cero.*

Demostración. Sean $r, s \in RG$ distintos de cero, con lo cual $\mathbf{sop}(r), \mathbf{sop}(s) \neq \varnothing$. Sea entonces

$$H = \langle \mathbf{sop}(r) \cup \mathbf{sop}(s)\rangle .$$

Ya que H es un grupo abeliano finitamente generado, por el teorema fundamental de grupos abelianos finitamente generados (Teorema 10.20 de [31]), es la suma directa de una familia finita $\{Z_i\}_{i=1}^n$ de grupos cíclicos infinitos. Definimos un orden en $\bigoplus_{k=1}^n Z_k = \bigoplus_{k=1}^n \langle z_k \rangle$ como sigue. Dados dos elementos $a = (z_1^{a_1}, z_2^{a_2}, \ldots, z_n^{a_n})$ y $b = (z_1^{b_1}, z_2^{b_2}, \ldots, z_n^{b_n})$, diremos que $a < b$ si $(a_1, \ldots, a_n) < (b_1, \ldots, b_n)$ en el orden lexicográfico. Es decir, $a_1 < b_1$ ó $a_1 = b_1$ y $a_2 < b_2$, y así sucesivamente hasta n. Sea $w_r = \max \mathbf{sop}(r)$ y $w_s = \max \mathbf{sop}(s)$. Dados $w_1 \in \mathbf{sop}(r)$ y $w_2 \in \mathbf{sop}(s)$, si se cumple $w_r > w_1$, también se tiene $w_r w_s > w_1 w_2$. Lo mismo ocurre si $w_s > w_2$. Es decir, $w_r w_s \neq w_1 w_2$ para cada $w_1 \in \mathbf{sop}(r), w_2 \in \mathbf{sop}(s)$ tal que $w_1 \neq w_r$ o $w_2 \neq w_s$. Por lo tanto, si

$$r = uw_r + x,$$
$$s = vw_s + y,$$

para $u, v \in R$ no cero y $x, y \in RG$, entonces $uv \neq 0$ porque R es primo conmutativo y $uvw_r w_s$ no se puede cancelar en rs. Es decir,$w_r w_s \in \mathbf{sop}(rs)$ y entonces $rs \neq 0$, completando el resultado. □

Teorema 2.3.5. *Sea R un anillo conmutativo y G un grupo. Entonces RG es primo si y sólo si R es primo y G no tiene subgrupos finitos normales no triviales*

Demostración. En realidad, aquí se demostrarán las proposiciones contrarrecíprocas, las cuales son equivalentes. Es decir, lo que se muestra es la proposición "RG no es primo si y sólo si R no es primo o G tiene un subgrupo finito normal no trivial".

Si R no es primo, entonces existen $r, s \in R$ distintos de cero tales que $rts = 0$ para cada $t \in R$, por lo que si $u \in RG$ está dado por

$$u = \sum_{g \in G} u_g g,$$

entonces

$$rus = r\left(\sum_{g \in G} u_g g\right) s = \sum_{g \in G} r u_g s g = \sum_{g \in G} 0 \cdot g = 0,$$

por lo que RG no es primo. Supongamos ahora que existe $H \trianglelefteq G$ finito no trivial y sea

$$r = \sum_{g \in H} g \neq 0.$$

Ya que $hH = H$ para cada $h \in H$, se tiene $hr = r$ para cada $h \in H$. Por lo que si $n = |H|$,

$$r^2 = \left(\sum_{g \in H} g\right) r = \sum_{g \in H} gr = nr.$$

Sea entonces $s = n - r$. Ya que H es no trivial, existe $1 \neq h \in H$, por lo que $h \in \mathbf{sop}(r)$. Pero $h \notin \mathbf{sop}(n)$, es decir, $s \neq 0$. Ahora bien, como $H \trianglelefteq G$, para cada $g \in G$, $Hg = gH$, es decir,

$$rg = \left(\sum_{h \in H} h\right) g = \sum_{h \in H} hg = \sum_{h \in H} gh = g\left(\sum_{h \in H} h\right) = gr.$$

Puesto que R es conmutativo, para cada $t \in RG$ se cumple $rt = tr$, por lo que

$$rts = trs = tr(n - r) = t(rn - r^2) = t(nr - r^2) = t \cdot 0 = 0,$$

con lo cual RG no es primo.

Supongamos ahora que RG no es primo. Entonces existen $r, s \in RG$ distintos de cero tales que $r(RG)s = \{0\}$. Si $1 \notin \mathbf{sop}(r)$, entonces como $r \neq 0$, existe algún $g \in G$ tal que $g^{-1}r(RG)s = 0$ y $1 \in \mathbf{sop}(g^{-1}r)$. Así, sin pérdida de generalidad, supondremos que $1 \in \mathbf{sop}(r) \cap \mathbf{sop}(s)$. Reescribimos $r = r_0 + r_1$ y $s = s_0 + s_1$ de tal forma que $\mathbf{sop}(r_0), \mathbf{sop}(s_0) \subseteq \Delta(G)$ y $\mathbf{sop}(r_1) \cap \Delta(G) = \mathbf{sop}(s_1) \cap \Delta(G) = \varnothing$. Puesto que $1 \in \mathbf{sop}(r) \cap \mathbf{sop}(s)$, sabemos que $r_0, s_0 \neq 0$.

Supongamos entonces que $r_0 s_0 \neq 0$. Si $g \notin \Delta(G)$, entonces $hg \notin \Delta(G)$ para cada $h \in \Delta(G)$, pues de lo contrario, g generaría la clase lateral $\Delta(G)$. Entonces, $\mathbf{sop}(r_0 s_1) \cap \Delta(G) = \varnothing$ y por lo tanto $r_0 s = r_0 s_0 + r_0 s_1 \neq 0$. En particular, el soporte de $r_0 s$ no es vacío.

Consideremos

$$H = \bigcap_{u \in \mathbf{sop}(r_0)} C_G(u).$$

Sea $h \in H$. Por la definición de H, ya que $\mathbf{sop}(r_0) \subseteq \Delta(G)$, se cumple $hr_0 = r_0 h$ y por lo tanto

$$0 = h^{-1}rhs = h^{-1}(r_0 + r_1)hs = h^{-1}r_0 hs + h^{-1}r_1 hs = h^{-1}hr_0 s + h^{-1}r_1 hs = r_0 s + h^{-1}r_1 hs.$$

Obtenemos que los elementos del soporte de $r_0 s$ coinciden con los del soporte de $h^{-1}r_1 hs$. Sean $\mathbf{sop}(r_1) = \{x_1, \ldots, x_n\}$ y $\mathbf{sop}(s) = \{y_1, \ldots, y_m\}$. Por lo anterior, para cada $z \in \mathbf{sop}(r_0 s)$ se debe tener $z = h^{-1}x_i h y_j$ para algunos i, j, pero esto es equivalente a

$$z y_j^{-1} = h^{-1} x_i h.$$

Es decir, x_i es conjugado de $z y_j^{-1}$, para todos los i, j para los que esto ocurra. Sea g_{ij} tal que $z y_j^{-1} = g_{ij}^{-1} x_i g_{ij}$. Entonces, para cada $h \in H$ existen i, j tales que $h g_{ij}^{-1} \in C_G(x_i)$, es decir,

$$H \subseteq \bigcup_{i,j} C_G(x_i) g_{ij}. \tag{2.4}$$

Por definición de $\Delta(G)$, para cada $u \in \mathbf{sop}(r_0)$, se tiene $[G : C_G(u)] < \infty$. Por el inciso **a)** de la Proposición 2.3.1, se tiene $[G : H] < \infty$, por lo que existen $w_1, \ldots, w_l$ tales que

$$G = \bigcup_k H w_k,$$

con lo cual, de (2.4) obtenemos

$$G = \bigcup_k H w_k = \bigcup_{i,j} C_G(x_i) g_{ij} w_k.$$

Esto muestra que G puede ser expresado como unión finita de clases laterales de los grupos $C_G(x_i)$, lo que implica, por el inciso **b)** de la Proposición 2.3.1, que existe x_i tal que $[G : C_G(x_i)] < \infty$. Entonces $x_i \in \Delta(G)$, pero esto es una contradicción, ya que $x_i \in \mathbf{sop}(r_1)$. Por lo tanto, debe suceder entonces $r_0 s_0 = 0$.

Ya que $r_0, s_0 \in \Delta(G)$ son distintos de cero y tales que $r_0 s_0 = 0$, entonces $R\Delta(G)$ tiene divisores de cero. Si R no es primo, se cumpliría lo deseado, así que supongamos que R es primo. Por la Proposición 2.3.4, el grupo $\Delta(G)$ no puede ser libre de torsión y abeliano, ya que $R\Delta(G)$ tiene divisores de cero. Por el inciso **b)** de la Proposición 2.3.3, se tiene que $\Delta^+(G) \neq 1$ y por el inciso **c)** de la misma proposición, G debe tener algún subgrupo finito normal no trivial, lo que completa el resultado. □

En particular, si K es un campo, K es conmutativo y si $a, b \in K\backslash\{0\}$ son tales que $atb = 0$ para cada $t \in K$, entonces, $a(1)b = ab = 0$. Pero ya que $a \neq 0$, sacamos $0 = (1/a)0 = (1/a)ab = b$, lo que es una contradicción con que b sea distinto de cero. Es decir, K es un anillo conmutativo primo y así se tiene el siguiente corolario.

Corolario 2.3.6. *Sea K un campo y G un grupo. KG es primo si y sólo si G no tiene subgrupos finitos normales no triviales.*

2.4 Condiciones de Cadena

En esta sección, se analizan ciertas condiciones de finitud que un anillo de grupo puede tener. En particular, estudiaremos las llamadas condiciones de cadena, que consisten en que una cadena de ideales derechos, debe parar en algún punto, en determinados casos cuando esta crece o decrece.

Sea R un anillo. Una **cadena ascendente de ideales derechos** es una colección $I_1, I_2, \ldots$ de ideales derechos en R tales que

$$I_1 \subseteq I_2 \subseteq \ldots$$

Una **cadena descendente de ideales derechos** es una colección $I_1, I_2, \ldots$ de ideales derechos en R tales que

$$I_1 \supseteq I_2 \supseteq \ldots$$

Definición 2.4.1. *Un anillo R es un **anillo noetheriano** si para cualquier cadena ascendente de ideales derechos $I_1 \subseteq I_2 \subseteq \ldots$, existe $n \in \mathbb{N}$ tal que $I_n = I_m$ para cada $m \geq n$. Un anillo R es artiniano si para cualquier cadena descendente de ideales derechos $I_1 \supseteq I_2 \supseteq \ldots$, existe $n \in \mathbb{N}$ tal que $I_n = I_m$ para cada $m \geq n$.*

*Un módulo M es un **módulo noetheriano** si para cualquier cadena ascendente de submódulos $N_1 \subseteq N_2 \subseteq \ldots$, existe $n \in \mathbb{N}$ tal que $N_n = N_m$ para cada $m \geq n$. Un módulo M es artiniano si para cualquier cadena descendente de submódulos $I_1 \supseteq I_2 \supseteq \ldots$, existe $n \in \mathbb{N}$ tal que $I_n = I_m$ para cada $m \geq n$.*

Como observación importante, si R es un anillo, los ideales derechos de R son justamente los submódulos de R como módulo, por lo que para un anillo R, ser noetheriano como R-módulo y como anillo es equivalente.

De la definición se obtiene fácilmente que si R es un anillo noetheriano (artiniano) y I es un ideal de R, entonces R/I es noetheriano (artiniano).

Proposición 2.4.2. *Sea R un anillo y G un grupo finito. Si R es noetheriano, entonces RG es noetheriano. Si R es artiniano, entonces RG es artiniano.*

Demostración. Supongamos que R es noetheriano. Sea $I_1 \subseteq I_2 \subseteq \ldots$ una cadena ascendente de ideales en RG y $G = \{g_i\}_{i=1}^n$. Se demostrará que si $1 \leq m \leq n$, entonces existe k tal que si $l \geq k$,

$$I_k \cap \left(\sum_{i=1}^{m} Rg_i\right) = I_l \cap \left(\sum_{i=1}^{m} Rg_i\right).$$

Para $m = 1$, se tiene que Rg_1 es un R-módulo isomorfo a R y $Rg_1 \cap I_i$ es la intersección de dos R-módulos, por lo que es un submódulo de Rg_1. Ya que $Rg_1 \cong R$ es noetheriano, la cadena $I_1 \cap Rg_1 \subseteq I_2 \cap Rg_1 \subseteq \ldots$ debe estabilizarse, por lo que el resultado es cierto para $m = 1$.

Supongamos ahora que $1 < m \leq n$ y que el resultado es cierto para $m - 1$. Tomamos el siguiente cociente de $R-$módulos:

$$R_{m-1} = \left(\sum_{i=1}^{m} Rg_i\right) \Big/ \left(\sum_{i=1}^{m-1} Rg_i\right) \cong Rg_m,$$

y sea $\overline{I_k}$ el conjunto de clases laterales que $I_k \cap (\sum_{i=1}^{m} Rg_i)$ genera en el anterior cociente para cada k. Análogo al caso $m = 1$, se tiene que R_{m-1} es un R-módulo noetheriano. Debido a que cada I_i es un ideal derecho de RG, se nota que $\overline{I_i}$ es un R-submódulo de R_{m-1} para cada i. Entonces, al ser $R_{m-1} \cong R$ noetheriano, existe k_1 tal que $\overline{I_{k_1}} = \overline{I_l}$ si $l \geq k_1$. Ahora bien, por hipótesis de inducción, existe k_2 tal que si $l \geq k_2$,

$$I_{k_2} \cap \left(\sum_{i=1}^{m-1} Rg_i \right) = I_l \cap \left(\sum_{i=1}^{m-1} Rg_i \right). \tag{2.5}$$

Sea entonces $k = \max\{k_1, k_2\}$ y sea $l > k$. Supongamos que existe

$$x \in \left(I_l \cap \left(\sum_{i=1}^{m} Rg_i \right) \right) \setminus \left(I_k \cap \left(\sum_{i=1}^{m} Rg_i \right) \right).$$

Ya que $\overline{I_k} = \overline{I_l}$, entonces, $x = s + y$ para algunos $s \in \sum_{i=1}^{m-1} Rg_i$ y $y \in I_k \subseteq I_l$. Entonces $s = x - y \in I_l \setminus I_k$, por lo que a su vez,

$$s \in \left(I_l \cap \left(\sum_{i=1}^{m-1} Rg_i \right) \right) \setminus \left(I_k \cap \left(\sum_{i=1}^{m-1} Rg_i \right) \right),$$

lo que es una contradicción con (2.5). De aquí se tiene entonces el resultado por inducción.

Puesto que $RG = \sum_{i=1}^{n} Rg_i$, por lo antes probado RG es noetheriano. Análogamente se comprueba que si R es artiniano entonces RG es artiniano. □

La proposición recíproca del resultado anterior es más complicada, aquí sólo se analizarán casos particulares de este recíproco.

Definición 2.4.3. *Se dice que un grupo G satisface la **condición de cadena ascendente en subgrupos** si para cada cadena ascendente $H_1 \leq H_2 \leq H_3 \leq \ldots$ de subgrupos de G, existe $n \in \mathbb{N}$ tal que $H_n = H_m$ para cada $m \geq n$.*

Proposición 2.4.4. *Sea R un anillo y G un grupo. Si RG es noetheriano, entonces R es noetheriano y G satisface la condición de cadena ascendente en subgrupos.*

Demostración. Por la Proposición 2.2.7, hay un isomorfismo de anillos $R \cong R(G/G) \cong (RG)/\omega(G)$, por lo que R es noetheriano. Si $H_1 \leq H_2 \leq H_3 \leq \ldots$ es una cadena de subgrupos en G, entonces

$$\omega(H_1) \subseteq \omega(H_2) \subseteq \omega(H_3) \subseteq \ldots.$$

Como cada $\omega(H_k)$ es un ideal derecho en RG, que es noetheriano, existe $n \in \mathbb{N}$ tal que $\omega(H_n) = \omega(H_m)$ para cada $m \geq n$. Ahora, si $m \geq n$ y $g \in H_m$, entonces $1 - g \in \omega(H_m) = \omega(H_n)$, luego $g \in H_n$, así $H_n = H_m$, lo que completa el resultado. □

De manera análoga al resultado anterior, se puede probar que si RG es artiniano, entonces R es artiniano y G satisface la condición de cadena descendente en subgrupos. Pero de hecho, es posible obtener un resultado más fuerte con la ayuda de lo visto en la sección anterior. Para ello, se necesita el siguiente resultado preliminar.

Proposición 2.4.5. *Si R es un anillo artiniano, entonces todo ideal primo derecho es maximal.*

Demostración. Sea P un ideal primo en R y $r \in R \backslash P$. Ya que P es ideal derecho, también $rR + P$ es un ideal derecho. A su vez, también lo es $r^m R + P$ para cada $m \in \mathbb{N}$ y ya que $r^m(r^{1-m}) + p = r + p \in rR + P$, entonces

$$rR + P \supseteq r^2R + P \supseteq r^3R + P \supseteq \dots$$

Ya que R es artiniano, existe $n \in \mathbb{N}$ tal que $r^nR + P = r^{n+1}R + P$. Puesto que $1 \in R$ y $0 \in P$, por ser ideal derecho, existe $h \in P$ y $s \in R$ tal que $r^n = r^{n+1}s + h$, de donde, $r^n(1 - rs) = h \in P$. Como $r \notin P$, se tiene $r^n \notin P$, pero siendo P ideal primo, lo anterior implica entonces que $1 - rs \in P$. Entonces $1 \in P + rR = rR + P$. Ya que $rR + P$ es un ideal que contiene a 1, debe ocurrir $rR + P = R$. Dado que $rR + P = R$ y $0 \in P$, se tiene $rR = R$, por lo que el ideal derecho más pequeño que contiene a $P \cup \{r\}$ es R. Como r es un elemento arbitrario de $R \backslash P$, concluimos que P es un ideal maximal derecho. □

Proposición 2.4.6. *Si RG es primo y artiniano, entonces $G = \{1\}$.*

Demostración. Por la Proposición 1.4.6, el ideal $\{0\}$ de RG es primo y por la proposición anterior, debe ser maximal. Por lo tanto, no existen ideales propios en RG distintos de $\{0\}$. Por la Proposición 2.2.5, $\omega(G)$ es un ideal en RG, pero ya que $1 \notin \ker(\varepsilon) = \omega(G)$, entonces, debe ser un ideal propio. Puesto que $\{0\}$ es el único ideal propio, obtenemos $\omega(G) = \{0\}$, pero esto implica $G = \{1\}$. □

Un resultado relevante, que es importante para la última proposición de la sección, es el conocido teorema de Hopkins-Levitzki (Teorema 8.46 en [29]) enunciado a continuación.

Teorema 2.4.7. *Todo anillo artiniano es noetheriano.*

En realidad, parece muy relevante, pues de hecho, menciona que la propiedad de ser artiniano es un caso particular a la de noetheriano. El siguiente resultado sirve ya como una aplicación interesante del Teorema 2.3.5, que da pie a uno de los pasos más complicados en la búsqueda de caracterizaciones para anillos de grupo artinianos y noetherianos.

Proposición 2.4.8. *Sea R un anillo primo conmutativo y G un grupo. Entonces RG es artiniano si y sólo si R es artiniano y G es finito.*

Demostración. Si R es artiniano y G finito, RG es artiniano por la Proposición 2.4.2. Supongamos que RG es artiniano. Ya mencionamos que R debe ser artiniano. Construimos una cadena $H_1 \leq H_2 \leq H_3 \leq \dots$ de subgrupos normales finitos de G comenzando con $H_1 = \{1\}$. Para cada k, si existe algún subgrupo normal finito de G que contiene estrictamente a H_k, escogemos H_{k+1} como un subgrupo normal finito minimal que contiene a H_k. En otro caso, daríamos por terminada la cadena. Ya que RG es artiniano, por el teorema de Hopkins-Levitzki, es noetheriano. Entonces, por la Proposición 2.4.4, la cadena está forzada a terminar, digamos en H_n. Veamos que G/H_n no tiene subgrupos finitos normales no triviales.

Supongamos que H es un subgrupo normal finito no trivial de G/H_n. Por el teorema de la correspondencia (Teorema 2.28 de [31]), existe un subgrupo normal K de G con $H_n \subsetneq K \subseteq G$ tal que $H = K/H_n$. Como H es finito y H_n es finito, también debe serlo K. Pero esto contradice que la cadena terminase en H_n.

Ya que R es primo y G/H_n no tiene subgrupos finitos normales no triviales, por la Proposición 2.3.5, $R(G/H_n)$ es primo. Por otra parte, $R(G/H_n) = (RG)/\omega(H_n)$ es artiniano, así que es primo y artiniano. Por la Proposición 2.4.6, se debe tener $G/H_n = \{1\}$, por lo que $G = H_n$ es finito, completando el resultado. □

3 Las Conjeturas de Kaplansky

En el estudio de la estructura de anillo de grupo han aparecido diferentes problemas, y uno de los más populares ha sido el problema de las conjeturas de Kaplansky, que trata acerca de algunos tipos de elementos comunes en un anillo cualquiera y qué condiciones debe satisfacer el anillo y el grupo sobre los que se construyen el anillo de grupo para tener o no estos elementos. Aparecieron por primera vez el siglo pasado y desde entonces, diversos avances se han hecho en la investigación de estas conjeturas.

En este capítulo, se muestran los casos particulares más básicos obtenidos sobre las conjeturas, así como la estrecha relación que tienen. Aún no se tiene un panorama general sobre las conjeturas, pero se han desarrollado diferentes casos y diferentes relaciones con otras áreas de las matemáticas.

Se desarrolla además un concepto muy relevante relacionado con las conjeturas, como lo son los grupos con producto único. Se demuestran varios resultados relevantes acerca de estos y características que tienen.

3.1 Enunciados

En su tesis sin publicar [13] (ver también [14] y [32]), Higman en su estudio de las unidades en el anillo de grupo, conjetura que si K es un campo y G es un grupo libre de torsión, entonces KG es un anillo sin divisores de cero ni unidades no triviales, donde una unidad es trivial si es de la forma kg donde $k \in K\backslash\{0\}$ y $g \in G$. Fue posteriormente Kaplansky quien popularizó estas conjeturas (por ejemplo, en [15]) junto con una conjetura adicional. Las tres conjeturas de Kaplansky son entonces:

Conjetura de la Unidad. *Si K es un campo y G es un grupo libre de torsión, entonces KG no tiene unidades que no sean de la forma kg, con $k \in K\backslash\{0\}$ y $g \in G$.*

Conjetura de Divisores de Cero. *Si K es un campo y G es un grupo libre de torsión, entonces KG no tiene divisores de cero.*

Conjetura de Elementos Idempotentes. *Si K es un campo y G es un grupo libre de torsión, entonces KG no tiene elementos idempotentes diferentes de 0 y 1.*

En realidad, las conjeturas fueron originalmente postuladas para dominios enteros, pero ya que todo dominio entero está incrustado en un campo, suele ser más sencillo trabajar con las conjeturas sobre campos. Además, si G es un grupo y $g \in G$ es tal que $g^n = 1$, entonces para cualquier campo K, en el anillo de grupo KG se tiene

$$(1-g)(1+g+\cdots+g^{n-1}) = 1-g^n = 0,$$

y por lo tanto, KG tiene divisores de cero. Ahora, sea $s = 1 + g + \cdots + g^{n-1}$, entonces

$$\begin{aligned} s^2 &= (1 + g + \dots g^{n-1})^2 \\ &= 1 + g + \cdots + g^{n-2} + g^{n-1} \\ &\quad + g + g^2 + \cdots + g^{n-1} + 1 \\ &\qquad \vdots \\ &\quad + g^{n-1} + 1 + \dots g^{n-2} \\ &= n(1 + g + \dots g^{n-1}) = ns. \end{aligned}$$

Suponiendo que $\text{char}(K) \nmid n - 1$, entonces $n - 1 \neq 0$ en K y en KG se tiene

$$(1 - s)\left(1 - \frac{1}{n-1}s\right) = 1 - \frac{1}{n-1}s - s + \frac{1}{n-1}s^2 = 1 - s + \frac{1}{n-1}(s^2 - s).$$

Ya que $s^2 = ns$, se cumple

$$(1 - s)\left(1 - \frac{1}{n-1}s\right) = 1 - s + \frac{1}{n-1}(ns - s) = 1 - s + \frac{1}{n-1}s(n-1) = 1 - s + s = 1,$$

por lo que, bajo la condición de que $\text{char}(K) \nmid n - 1$, el anillo de grupo KG tiene unidades no triviales. Así, suena relevante pedir que G sea libre de torsión en las conjeturas.

Proposición 3.1.1. *Sea R un anillo. Si R tiene un elemento idempotente diferente de 0 y 1, entonces tiene un divisor de cero.*

Demostración. Sea $r \in R$ un elemento idempotente diferente de 0 y 1. Entonces $r, r - 1 \neq 0$ y

$$r(r - 1) = r^2 - r = r - r = 0,$$

obteniendo el resultado. □

Proposición 3.1.2. *Sea G un grupo libre de torsión. Si K es un campo y KG tiene algún divisor de cero, entonces existe $r \in KG\backslash\{0\}$ tal que $r^2 = 0$.*

Demostración. Sean $s, t \in KG\backslash\{0\}$ tales que $st = 0$. Ya que G es libre de torsión, no tiene subgrupos finitos normales no triviales, así que por el Corolario 2.3.6 se tiene que KG es primo. Por lo tanto, existe $q \in KG$ tal que $tqs \neq 0$, pero

$$(tqs)^2 = tqstqs = tq \cdot 0 \cdot qs = 0,$$

por lo que $r = tqs$ cumple lo deseado. □

Proposición 3.1.3. *Sea G un grupo libre de torsión. Si K es un campo y KG tiene algún divisor de cero, entonces KG tiene una unidad no trivial.*

Demostración. Por el resultado anterior, existe $r \in KG\backslash\{0\}$ tal que $r^2 = 0$ y

$$(1 - r)(1 + r) = 1 - r^2 = 1.$$

Ahora, si $1 + r = kg$ para algunos $k \in K\backslash\{0\}$ y $g \in G$, entonces $r = kg - 1$ y

$$r^2 = (kg - 1)^2 = k^2g^2 - kg - kg + 1.$$

Ya que $k \in K\backslash\{0\}$, se cumple $k, k^2 \neq 0$. Y ya que G es libre de torsión, si $g \neq 1$, entonces $g^2 \neq g \neq 1$ y por lo tanto, $r^2 \neq 0$, lo que es una contradicción. Si $g = 1$, entonces $r = k - 1 \in K$, pero K no tiene divisores de cero, por lo que $r = 0$, generando también una contradicción. Así, $1 + r$ es una unidad no trivial en KG. □

Combinando las proposiciones 3.1.1 y 3.1.3, se tiene entonces la gran correlación que existe entre las conjeturas.

Teorema 3.1.4. *Sea G un grupo libre de torsión y K un campo.*

a) Si KG satisface la conjetura de la unidad, entonces satisface la conjetura de divisores de cero.

b) Si KG satisface la conjetura de divisores de cero, entonces satisface la conjetura de elementos idempotentes.

3.2 Grupos con Producto Único

Los grupos con producto único aparecieron junto con el estudio de las conjeturas de Kaplansky, pues como se verá, estos grupos son una de las grandes familias de grupos que satisfacen las tres conjeturas. Recordando, si A, B son subconjuntos de un grupo G, se toma

$$AB = \{ab \mid a \in A \text{ y } b \in B\}$$
$$A^{-1} = \{a^{-1} \mid a \in A\}$$

Definición 3.2.1. *Sea G un grupo y A, B subconjuntos finitos de G. Para cada $g \in G$ se define*

$$n_{A\cdot B}(g) = |\{(a, b) \in A \times B \mid ab = g\}|.$$

Por la anterior definición, $g \in AB$ si y sólo si $n_{A\cdot B}(g) \geq 1$.

Definición 3.2.2. *Un grupo G es de **producto único** si dados dos subconjuntos finitos no vacíos A, B de G, existe $g \in AB$ tal que $n_{A\cdot B}(g) = 1$.*

De manera equivalente, en el conjunto AB existe un elemento $x \in AB$ con representación única de la forma $x = ab$ con $a \in A$ y $b \in B$. También se dice que G es un grupo con producto único o que satisface la propiedad de producto único.

Proposición 3.2.3. *Si G es un grupo con producto único, entonces es un grupo libre de torsión.*

Demostración. Se probará la proposición contrarrecíproca. Sea G un grupo con torsión. Entonces existe $g \in G\backslash\{1\}$ tal que $g^n = 1$ y $\Gamma = \langle g \rangle$ es un subgrupo finito de G. Por lo tanto

$$\Gamma\Gamma = \Gamma.$$

Si $h \in \Gamma\backslash\{1\}$, entonces $h = 1h = h1$ son diferentes representaciones de h como elemento de $\Gamma\Gamma$. Además, $1 = 1 \cdot 1 = gg^{-1}$, cumpliéndose así que $n_{\Gamma\cdot\Gamma}(z) > 1$ para cada $z \in \Gamma\Gamma$ y por lo tanto, G no es un grupo con producto único. □

Así, la familia de grupos libres de torsión es una familia que contiene a los grupos con producto único y por lo tanto, si las conjeturas de Kaplansky fueran ciertas, entonces KG no tendría divisores de cero, unidades no triviales ni elementos idempotentes, para G con producto único y K un campo.

En [26], además de los grupos con producto único, se trabaja con grupos que satisfacen una condición más fuerte que la propiedad de producto único. Esta condición establece que siempre que en el producto AB de la definición de producto único se tenga que $|A| + |B| > 2$, entonces existe un segundo elemento $h \in AB$ tal que $n_{A\cdot B}(h) = 1$. Fue Strojnowski quien en su articulo [36] comprobó que de hecho esta condición aparentemente más fuerte es equivalente a la condición de producto único, lo que da el siguiente resultado.

Teorema 3.2.4. *Si G es un grupo con producto único y A, B son subconjuntos finitos de G tales que $|A|+|B| > 2$, entonces existen dos elementos $x, y \in AB$ con $x \neq y$ tales que $n_{A\cdot B}(x) = n_{A\cdot B}(y) = 1$.*

Demostración. Sea G un grupo con producto único. Supongamos que existen subconjuntos finitos A, B de G tales que $|A| + |B| > 2$, pero existe un único $x \in AB$ con $n_{A\cdot B}(x) = 1$. Si $x = ab$, con $a \in A$ y $b \in B$, entonces, $(a^{-1}A)(Bb^{-1})$ también satisface tener un único elemento con producto único, $1 \cdot 1$, pues si $a' \in A$ y $b' \in B$ son tales que $a^{-1}a'b'b^{-1} = 1 = a^{-1}abb^{-1}$, entonces, $a'b' = ab$ y por lo tanto, $a' = a$ y $b' = b$. Además, si $a^{-1}a_1 \cdot b_1b^{-1} \in (a^{-1}A)(Bb^{-1})$ satisface ser únicamente representado como producto, entonces a_1b_1 satisface ser únicamente representado como producto en AB y por lo tanto, ya que x es el único elemento únicamente representado en AB, se cumple $a_1 = a$ y $b_1 = b$. Así, $(a^{-1}A)(Bb^{-1})$ también tiene un único elemento únicamente representado, el cual es $1 \cdot 1$.

Sean $C = a^{-1}A$, $D = Bb^{-1}$, $E = D^{-1}C$ y $F = DC^{-1}$. Si $y \in EF$, entonces $y = d_1^{-1}c_1d_2c_2^{-1}$ y tenemos varios casos:

- Si $c_1 \neq 1$ ó $d_2 \neq 1$, entonces $c_1d_2 \neq 1$, pues 1 está únicamente representado como producto en CD como $1 \cdot 1$. Como a su vez, este es el único producto único, entonces existen $c_3 \neq c_1$ y $d_3 \neq d_2$ tales que $c_3d_3 = c_1d_2$, de donde $y = d_1^{-1}c_3d_3c_2^{-1}$ y por lo tanto, $n_{E\cdot F}(y) \geq 2$.
- Si $c_1 = d_2 = 1$ y $d_1 \neq 1$ ó $c_2 \neq 1$, entonces existen $c_4 \neq c_2$ y $d_4 \neq d_1$ tales que $c_2d_1 = c_4d_4$. Es decir, $d_1^{-1}c_2^{-1} = d_4^{-1}c_4^{-1}$ y por lo tanto, $y = d_1^{-1}c_2^{-1} = d_1^{-1}1 \cdot 1c_2^{-1} = d_4^{-1}1 \cdot 1c_4^{-1}$ con lo cual $n_{E\cdot F}(y) \geq 2$.
- Veamos que $n_{E\cdot F}(1) \geq 2$. Ya que $|A| + |B| > 2$, entonces $|C| + |D| > 2$ y entonces debe existir un elemento diferente de 1 en C o en D. Sin pérdida de generalidad, sea $c_5 \in C$ con $c_5 \neq 1$ y entonces $1 \cdot 1 \cdot 1 \cdot 1 = 1c_5 \cdot 1c_5^{-1} = 1$.

Así, EF no tiene ningún producto único, lo que es una contradicción al ser G un grupo con producto único. Por lo tanto, AB debe tener un segundo producto único. □

Ejemplo 3.2.5. *$\mathbb{Z}$ es un grupo con producto único. Para verlo, sean $A = \{a_1, a_2, \ldots, a_n\}$ y $B = \{b_1, b_2, \ldots, b_m\}$ subconjuntos de G tales que si $k < l$, entonces $a_k < a_l$ y $b_k < b_l$. Entonces $a_1 + b_1$ y $a_n + b_m$ son elementos con representación única en AB. En efecto, si por ejemplo $a_j \neq a_1$, entonces $a_1 < a_j$ y por lo tanto, para cualquier k se tiene*

$$a_1 + b_1 \leq a_1 + b_k < a_j + b_k.$$

Análogo es el caso si $b_i \neq b_1$. Así, $a_1 + b_1$ es únicamente representado y también de forma análoga, $a_n + b_m$ es únicamente representado. Si $|A| + |B| > 2$, tiene que pasar que $a_n \neq a_1$ ó $b_m \neq b_1$. En cualquiera de los dos casos se cumple $a_1 + b_1 \neq a_n + a_m$ y hay al menos dos elementos con representación única.

La siguiente es otra propiedad que satisfacen los grupos con producto único, que es muy útil en la búsqueda de grupos que no satisfagan la condición, pues reduce el número de conjuntos en los que se debe verificar el producto único.

Proposición 3.2.6. *Un grupo G satisface la propiedad de producto único si y sólo si para cada subconjunto $A \subseteq G$ finito no vacío, existe $g \in G$ tal que $n_{A\cdot A}(g) = 1$.*

Demostración. Si G es un grupo con producto único, ciertamente se satisface la condición deseada. Suponiendo que G no es de producto único, entonces existen subconjuntos finitos no vacíos $B, C \subseteq G$ tales que $n_{B\cdot C}(g) \neq 1$ para cada $g \in G$. Sea $A = CB$ y $g \in A \cdot A = CB \cdot CB$. Entonces $g = c_1b_1c_2b_2$ para algunos $c_1, c_2 \in C$ y $b_1, b_2 \in B$. Ya que $b_1c_2 \in BC$, se tiene $n_{B\cdot C}(b_1c_2) \geq 2$, por lo que existen $c_3 \in C$ y $b_3 \in B$ tales que $b_1c_2 = b_3c_3$ y $b_1 \neq b_3$ y $c_2 \neq c_3$ (Si $b_1 = b_3$, entonces $b_1c_2 = b_3c_3$ implica $c_2 = c_3$, análogamente, $c_2 = c_3$ implica $b_2 = b_3$, por lo que para que b_3c_3 sea un producto diferente a b_1c_2 tal que $b_3c_3 = b_1c_2$ se debe satisfacer que ambas entradas sean diferentes). Se tiene así lo siguiente:

$$g = c_1b_1c_2b_2 = c_1b_3c_3b_2.$$

Si $c_1b_3 = c_1b_1$, entonces $b_3 = b_1$, que es una contradicción. Esto implica que $(c_1b_3)(c_3b_2)$ es otra forma de escribir a g como producto de elementos de $A \cdot A$. Es decir, $n_{A\cdot A}(g) \geq 2$ y así $n_{A\cdot A}(g) \neq 1$ para cada $g \in G$. Por la proposición contrarrecíproca, se tiene el resultado. □

La existencia de grupos libres de torsión que no cumplen la propiedad de producto único resultó ser un problema complicado, tanto es así, que en algún momento se pensó que la propiedad podía ser equivalente a ser libre de torsión. Esto se desmintió por primera vez en [28], pero debido a la complejidad que conlleva hablar de los grupos libres de torsión sin la propiedad de producto único, se prefiere hablar de ellos en una sección aparte, la Sección 3.4. La importancia de los grupos con producto único radica en el siguiente resultado.

Teorema 3.2.7. *Sea H un subgrupo normal del grupo libre de torsión G y sea K un campo. Si KH tiene sólo unidades triviales y G/H es un grupo con producto único, entonces KG sólo tiene unidades triviales.*

Demostración. Sean $r, s \in KG$ tales que $rs = 1$. Sean además $\{a_1, \ldots, a_n\} = A \subseteq \mathbf{sop}(r)$ y también $\{b_1, \ldots, b_m\} = B \subseteq \mathbf{sop}(s)$ conjuntos de elementos que generan distintas clases laterales en G/H y a su vez, tales que para cada $g_r \in \mathbf{sop}(r)$ y $g_s \in \mathbf{sop}(s)$, existen $a_i \in A$ y $b_j \in B$ con $Hg_r = Ha_i$ y $Hg_s = Hb_j$ (A y B existen porque $\mathbf{sop}(r)$ y $\mathbf{sop}(s)$ son finitos). Como $rs = 1$, se debe tener $r, s \neq 0$ y $A, B \neq \varnothing$. Si dos elementos $x, y \in G$ son tales que $Hx = Hy$, entonces debe pasar que $hx = y$ para algún $h \in H$ y por lo tanto es posible escribir

$$r = \sum_{j=1}^{n} \alpha_j a_j,$$
$$s = \sum_{j=1}^{m} b_j \beta_j,$$

donde $\alpha_j, \beta_j \in KH$ para cada j. Si $n + m > 2$, entonces

$$1 = rs = \sum_{i=1}^{n}\sum_{j=1}^{m} \alpha_i a_i b_j \beta_j,$$

por la Proposición 3.1.3, KH no tiene divisores de cero y ya que H es normal y $a_i, b_j \in G$, entonces $\alpha_i a_i b_j \beta_j \neq 0$ para cada i, j. Ahora, puesto que G/H es un grupo con producto único y $|A| + |B| > 2$, donde cada elemento de A y cada elemento de B generan clases laterales distintas en G/H, entonces por el Teorema 3.2.4, existen Ha_dHb_l con representación única tales que $Ha_dHb_l \neq H$ ($n_{A'\cdot B'}(Ha_dHb_l) = 1$, donde $A' = \{Ha \mid a \in$

$A\}, B' = \{Hb \mid b \in B\}$). Así, en (3.2), el término $\alpha_d a_d b_l \beta_l$ no puede ser cancelado y es diferente de 1 y 0, y por lo tanto, no puede pasar $rs = 1$, lo que es una contradicción.

Luego $n = m = 1$ y entonces $\alpha_1(a_1 b_1 \beta_1) = (\alpha_1 a_1 b_1)\beta_1 = 1$, por lo que α_1, β_1 son unidades en KG y por la Proposición 2.2.10, son unidades en KH. Pero KH tiene sólo unidades triviales, así que $\alpha_1 = k_1 h_1$ y $\beta_1 = k_2 h_2$ para $k_1, k_2 \in K$ y $h_1, h_2 \in H$. Por lo tanto $r = k_1 h_1 a_1$ y $s = k_2 h_2 b_1$ son unidades triviales en KG. □

Tomando $H = \langle 1 \rangle$ se tiene entonces el siguiente corolario.

Corolario 3.2.8. *Si G es un grupo con producto único, entonces KG tiene sólo unidades triviales, para cualquier campo K.*

La prueba de que el anillo de grupo no tiene unidades no triviales se basa en que para dos elementos en el grupo con soporte no vacío debe haber al menos un elemento que no se cancela. Más aún, en el caso que alguno de los soportes tenga cardinalidad mayor que 1, debe haber al menos un elemento diferente de 1 que no se cancela.

Un análisis similar se puede realizar para el anillo de grupo sobre el anillo $\mathbb{F}_2$. Este anillo tiene la particularidad de que sus elementos son sumas finitas de elementos del grupo de tal forma que $g + g = 0$ para cada $g \in G$. Así, es posible considerar una condición más fuerte que la de producto único que, de hecho, caracteriza no tener divisores de cero en en el anillo de grupo con coeficientes en $\mathbb{F}_2$.

Sea G un grupo con dos subconjuntos finitos no vacíos $A = \{a_1, \ldots, a_n\}$ y $B = \{b_1, \ldots, b_m\}$ tales que para cada $g \in AB$, el entero $n_{A\cdot B}(g)$ es par. Entonces en $\mathbb{F}_2 G$ se tiene

$$(a_1 + \cdots + a_n)(b_1 + \cdots + b_m) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j = \sum_{g \in AB} [n_{A\cdot B}(g)]_2 g,$$

donde $[n_{A\cdot B}(g)]_2$ es la clase módulo 2 de $n_{A\cdot B}(g)$. Como $n_{A\cdot B}(g)$ es par para cada $g \in AB$,

$$(a_1 + \cdots + a_n)(b_1 + \cdots + b_m) = \sum_{g \in AB} [n_{A\cdot B}(g)]_2 g = \sum_{g \in AB} [0]_2 g = 0,$$

y existe un divisor de cero. En cambio, supongamos que en G, para cada par de subconjuntos finitos no vacíos A y B, existe un elemento $g \in AB$ tal que $n_{A\cdot B}(g)$ es impar. Si $x, y \in \mathbb{F}_2 G$, como se dijo antes, x y y son sumas finitas de elementos de G, es decir, $x = x_1 + \cdots + x_n$ y $y = y_1 + \cdots + y_m$ donde $x_1, \ldots, x_n, y_1, \ldots, y_m \in G$. Si $x, y \neq 0$, entonces, $n, m \geq 1$ y

$$xy = \sum_{i=1}^{n} \sum_{j=1}^{m} x_i y_j = \sum_{g \in \mathbf{sop}(x)\mathbf{sop}(y)} [n_{\mathbf{sop}(x)\cdot\mathbf{sop}(y)}(g)]_2 g.$$

Como $n, m \geq 1$, los soportes de x y y son no vacíos y por la propiedad de G, existe $h \in \mathbf{sop}(x)\mathbf{sop}(y)$ tal que $n_{\mathbf{sop}(x)\cdot\mathbf{sop}(y)}(h)$ es impar. Por lo tanto, $[n_{\mathbf{sop}(x)\cdot\mathbf{sop}(y)}(h)]_2 = [1]_2$, lo que implica $h \in \mathbf{sop}(xy)$, por lo que $xy \neq 0$. Básicamente, lo que se probó antes es el siguiente resultado.

Proposición 3.2.9. *$\mathbb{F}_2 G$ no tiene divisores de cero si y sólo si, para cualesquiera dos subconjuntos finitos no vacíos A, B de G, existe $g \in AB$ tal que $n_{A\cdot B}(g)$ es impar.*

Parece un caso muy particular, pero como se expresa en [33], si existieran divisores de cero en $\mathbb{Q}G$, entonces también se tendrían divisores de cero en $\mathbb{F}_2 G$. Esto se comprueba tomando $\alpha, \beta \in \mathbb{Q}G \backslash \{0\}$, donde

$$\alpha = \sum_{i=1}^{n_1} p_{1,i} a_i, \quad \beta = \sum_{i=1}^{n_2} p_{2,i} b_i,$$

con $p_{1,1},\dots,p_{1,n_1},p_{2,1},\dots,p_{2,n_2}\in\mathbb{Q}$ y $a_1,\dots,a_{n_1},b_1,\dots,b_{n_2}\in G$ tales que $\alpha\beta=0$. Como $p_{i,j}$ es racional, existe $s_{i,j}\in\mathbb{Z}$ tal que $p_{i,j}s_{i,j}\in\mathbb{Z}$. Si $s_i=\prod_{j=1}^{n_i}s_{i,j}$, entonces $s_1\alpha, s_2\beta\in\mathbb{Z}G\backslash\{0\}$ son tales que

$$(s_1\alpha)(s_2\beta)=0.$$

Ahora bien, por ser 2 un número primo, existe una única forma de escribir $s_ip_{i,j}=2^{k_{i,j}}p'_{i,j}$ para $k_{i,j}=0,1,2,\dots$ de tal manera que 2 no divide a $p'_{i,j}$. Sea entonces $k_i=\min\{k_{i,j}\mid j=1,2,\dots,n_i\}$ para $i=1,2$. Entonces $(1/2^{k_j})s_jp_{j,i}\in\mathbb{Z}$ para cada i,j y además

$$\sum_{i=1}^{n_1}\left[\frac{1}{2^{k_1}}s_1p_{1,i}\right]_2a_i \quad \text{y} \quad \sum_{i=1}^{n_2}\left[\frac{1}{2^{k_2}}s_2p_{2,i}\right]_2b_i$$

son elementos no nulos de $\mathbb{F}_2G$. Por otra parte,

$$\left(\sum_{i=1}^{n_1}\frac{1}{2^{k_1}}s_1p_{1,i}a_i\right)\left(\sum_{i=1}^{n_2}\frac{1}{2^{k_2}}s_2p_{2,i}b_i\right)=\left(\frac{1}{2^{k_1}}s_1\frac{1}{2^{k_2}}s_2\right)\left(\sum_{i=1}^{n_1}p_{1,i}a_i\right)\left(\sum_{i=1}^{n_2}p_{2,i}b_i\right)=0,$$

por lo que, tomando $\varphi_{2\mathbb{Z}}\colon\mathbb{Z}G\to\mathbb{F}_2G$ de acuerdo a la Definición 2.2.1, se tiene entonces

$$\begin{aligned}\left(\sum_{i=1}^{n_1}\left[\frac{1}{2^{k_1}}s_1p_{1,i}\right]_2a_i\right)\left(\sum_{i=1}^{n_2}\left[\frac{1}{2^{k_2}}s_2p_{2,i}\right]_2b_i\right)&=\varphi_{2\mathbb{Z}}\left(\sum_{i=1}^{n_1}\frac{1}{2^{k_1}}s_1p_{1,i}a_i\right)\varphi_{2\mathbb{Z}}\left(\sum_{i=1}^{n_2}\frac{1}{2^{k_2}}s_2p_{2,i}b_i\right)\\&=\varphi_{2\mathbb{Z}}\left(\left(\sum_{i=1}^{n_1}\frac{1}{2^{k_1}}s_1p_{1,i}a_i\right)\left(\sum_{i=1}^{n_2}\frac{1}{2^{k_2}}s_2p_{2,i}b_i\right)\right)\\&=\varphi_{2\mathbb{Z}}(0)\\&=0.\end{aligned}$$

Así, se tiene la siguiente proposición.

Proposición 3.2.10. *Si la Conjetura de divisores de cero es cierta para $\mathbb{F}_2G$, entonces es cierta para $\mathbb{Q}G$.*

La propiedad de producto único es una propiedad muy específica que solo se suele encontrar en el trabajo de las conjeturas de Kaplansky, lo que implica que probar que un grupo satisface la propiedad de producto único suele ser una tarea muy especializada. En ese sentido, se trabaja también con condiciones débiles que garantizan la propiedad de producto único. Los grupos ordenados aparecen como una de esas grandes familias que satisfacen la propiedad de producto único.

Definición 3.2.11. *Un grupo G es **ordenado por la derecha (izquierda)** si tiene un orden lineal o total $\leq$ tal que $a<b$ implica $ac<bc$ ($ca<cb$) para cualesquiera $a,b,c\in G$. Un grupo G es **ordenado** si existe un orden lineal $\leq$ tal que $a<b$ implica $ac<bc$ y $ca<cb$ para cualesquiera $a,b,c\in G$.*

Es interesante ver, que la demostración de que $\mathbb{Z}$ es un grupo con producto único vista en el Ejemplo 3.2.5 se basa en la ordenación de $\mathbb{Z}$. Así, se tiene similarmente el siguiente resultado más general.

Proposición 3.2.12. *Si G es un grupo ordenado por la derecha, entonces es un grupo con producto único.*

Demostración. Sean A, B subconjuntos finitos no vacíos de G, sea $\alpha \in A$ el mínimo de A y sea $\beta \in B$ tal que $\alpha\beta$ es el mínimo en αB. Tales elementos α y β existen porque G es linealmente ordenado y A y αB son subconjuntos finitos no vacíos. Sea $a \in A$, entonces $\alpha \leq a$ y por lo tanto, $\alpha b \leq ab$ para cualquier b, por lo que además

$$\alpha\beta \leq \alpha b \leq ab.$$

Por lo anterior, si $\alpha\beta = ab$, entonces $\alpha b = ab$, por lo que $a = \alpha$ y entonces, $a\beta = ab$ y $b = \beta$. Así, $\alpha\beta$ tiene representación única como elemento de AB y G es un grupo con producto único. □

Aplicando argumentos análogos, los grupos ordenados por la izquierda también son de producto único y por supuesto, ser ordenado implica ser ordenado por la derecha y por lo tanto, los grupos ordenados también son de producto único.

Ejemplo 3.2.13. *$\mathbb{R}^+\backslash\{0\}$ es un grupo ordenado bajo la operación producto. El orden usual funciona adecuadamente, pues si q es un número real positivo y $a \leq b$, entonces $aq \leq bq$. Al ser $\mathbb{R}^+\backslash\{0\}$ un grupo conmutativo, es un grupo ordenado (por ambos lados).*

Ejemplo 3.2.14. *Todo grupo abeliano finitamente generado libre de torsión es ordenado. Por el teorema fundamental de grupos abelianos finitamente generados (Teorema 10.20 de [31]), si G es abeliano libre de torsión y finitamente generado, entonces*

$$G \cong \bigoplus_{k=1}^{n} Z_k$$

para algún $n \in \mathbb{N}$, donde $Z_k \cong \mathbb{Z}$ para cada k. Entonces $\bigoplus_{k=1}^{n} Z_k$ tiene el orden lexicográfico. Dados dos elementos $a = (a_1, a_2, \dots a_n)$ y $b = (b_1, b_2, \dots b_n)$, diremos que $a < b$ si $a_1 < b_1$ ó si $a_1 = b_1$ y $a_2 < b_2$ y así sucesivamente hasta n. Se tiene entonces un orden para G dado por el isomorfismo.

Ejemplo 3.2.15. *En general, análogo al ejemplo anterior, si A y B son grupos ordenados, $A \times B$ es un grupo ordenado.*

Ejemplo 3.2.16. *Sea G el grupo de la botella de Klein dado por la siguiente presentación conocida.*

$$G = \left\langle r, x \mid r^2 = x^2 \right\rangle.$$

Evidentemente, G es un producto amalgamado de $\langle r \rangle$ con $\langle x \rangle$ sobre los subgrupos $\left\langle r^2 \right\rangle, \left\langle x^2 \right\rangle$, que son isomorfos a $\mathbb{Z}$. La función de pegado cumple $\phi_1(r^2) = x^2$. Es decir, $G = \langle r \rangle *_{\mathbb{Z}} \langle x \rangle$. Al ser producto amalgamado de grupos libres de torsión, por el Corolario 1.3.8, G es libre de torsión.

Tomemos el elemento $y = rx^{-1}$. Ya que $r = yx$, entonces $G = \langle x, y \rangle$ y además,

$$G = \left\langle x, y \mid (yx)^2 = x^2 \right\rangle = \langle x, y \mid yxy = x \rangle = \left\langle x, y \mid yx = xy^{-1} \right\rangle.$$

Esta es una presentación interesante para el grupo, pues la relación que queda es "casi" conmutar, excepto por un signo. En cualquier caso, mediante argumentos inductivos se puede ver que todo elemento de G se puede expresar como $x^n y^m$ para $n, m \in \mathbb{Z}$ y además, $x^n y^m = y^{\varepsilon m} x^n$, para algún $\varepsilon \in \{-1, 1\}$. Más aún, si $x^{n_1} y^{m_1} = x^{n_2} y^{m_2}$, entonces $x^{n_1 - n_2} = y^{m_2 - m_1}$. Por la relación de grupo,

$$y^{m_2 - m_1} = x^{-1} y^{m_1 - m_2} x = x^{-1} x^{n_1 - n_2} x = x^{n_1 - n_2} = y^{m_1 - m_2},$$

lo que a su vez implica $y^{2(m_1-m_2)} = 1$. Pero G es libre de torsión, por lo que esto solo ocurre si $m_1 = m_2$, y entonces $n_1 = n_2$. Es decir, todo elemento en G se puede expresar de forma única como $x^n y^m$. Se define entonces el cono positivo

$$\mathcal{P} = \{y^n \mid n > 0\} \cup \{x^n y^m \mid n > 0\},$$

el cual es una herramienta muy útil para definir un orden en un grupo. Se observa que se cumplen las propiedades $\mathcal{P} \cdot \mathcal{P} \subset \mathcal{P}$, $G = \mathcal{P} \cup \mathcal{P}^{-1} \cup \{1\}$ y $\mathcal{P} \cap \mathcal{P}^{-1} = \varnothing$. Lo cual da pie a definir el orden lineal $h < g$ si $h^{-1}g \in \mathcal{P}$. En este orden $g \in \mathcal{P}$ si y sólo si $g > 1$.

Las propiedades de $\mathcal{P}$ implican que el orden $<$ definido en efecto es un orden lineal y si $h < g$ y $c \in G$, entonces $(ch)^{-1}cg = h^{-1}c^{-1}cg = h^{-1}g \in \mathcal{P}$, por lo que en efecto $ch < cg$ y este orden hace a G un grupo ordenado por la izquierda.

En general, el grupo de la botella de Klein es un ejemplo clásico de un grupo que es ordenado por la izquierda, pero no es ordenado. Para ver esto, suponiendo que $\leq$ es un orden lineal que hace a G ordenado, se observa que $1 < g$ si y sólo si $g^{-1} = g^{-1}(1) < g^{-1}(g) = 1$, para cada $g \in G$. Suponiendo entonces sin perdida de generalidad que $1 < y$, entonces, $x^{-1} < x^{-1}y$ y $1 = x^{-1}x < x^{-1}yx$, pero de acuerdo a la relación de grupo, $y^{-1} = x^{-1}yx > 1$, lo que es una contradicción. Así G no es un grupo ordenado.

Definición 3.2.17. *Sea G un grupo. Un subconjunto A de G se dice **antisimétrico** si $A \cap A^{-1} = \varnothing$ ó $A \cap A^{-1} = \{1\}$. Sea $\Upsilon(A)$ el conjunto de $a \in A$ tales que Aa^{-1} es antisimétrico. Se dice entonces que G es **difuso** si para cualquier subconjunto A de G tal que $2 \leq |A| < \infty$, se tiene $|\Upsilon(A)| \geq 2$.*

Proposición 3.2.18. *Todo grupo difuso es un grupo con producto único.*

Demostración. Sea G un grupo difuso y A, B subconjuntos finitos no vacíos de G. Si alguno de los dos tiene cardinalidad igual a 1, entonces $n_{A\cdot B}(g) = 1$ para cada $g \in AB$. Suponiendo entonces que $|A|, |B| \geq 2$, entonces $|AB| \geq 2$ y por ser G un grupo difuso, se debe cumplir que $|\Upsilon(AB)| \geq 2$.

Sea entonces $x \in \Upsilon(AB)$ y tomemos $a_0, a_1 \in A$ y $b_0, b_1 \in B$ tales que $x = a_0b_0 = a_1b_1$, entonces

$$(a_0a_1^{-1})x = (a_0a_1^{-1})(a_1b_1) = a_0b_1 \in AB,$$
$$(a_0a_1^{-1})^{-1}x = (a_1a_0^{-1})(a_0b_0) = a_1b_0 \in AB.$$

Pero $x \in \Upsilon(AB)$, por lo que siendo que $a_0a_1^{-1}, (a_0a_1^{-1})^{-1} \in ABx^{-1}$ debe pasar entonces $a_0a_1^{-1} = 1$ y $a_0 = a_1$. Análogamente, $b_0 = b_1$, así que $n_{A\cdot B}(x) = 1$ y G es un grupo con producto único. □

Los grupos difusos tienen una motivación geométrica, que se ve principalmente en [4]. En el Apéndice B de [17], se da un ejemplo de un grupo difuso que no es ordenado por la derecha. Es decir, ya que ser difuso implica tener la propiedad de producto único, los grupos ordenados no caracterizan la propiedad de producto único. Debido a la complejidad en cuanto a herramientas de este ejemplo, sólo se brinda la referencia.

En cambio, como lo expresa en [17] y más recientemente en [10], no se conoce si la condición de grupo difuso caracteriza la de tener producto único, de momento es un problema abierto.

3.3 La Condición de Ore

Para que un anillo pueda tener alguna propiedad de división en sus elementos, es necesario que satisfaga ciertas condiciones, en este sentido, la condición de Ore ayuda para ello. En esta sección, no se analizan las propiedades de divisibilidad que tienen los anillos de Ore, pero se habla sobre un resultado importante para encontrar anillos de grupo sin divisores de cero. Recordemos que un elemento regular en un anillo es aquel que no divide a cero.

Definición 3.3.1. *Un anillo R satisface la **condición de Ore** si para cada $r, s \in R$, con r regular en R, existen $t, v \in R$, con t regular tales que $rv = st$.*

Ejemplo 3.3.2. *Si R es un anillo conmutativo, entonces satisface la condición de Ore, pues si $r, s \in R$, con r regular en R, entonces, $rs = sr$, es decir, en la definición, se toma $t = r$ y $v = s$.*

En ocasiones, a la propiedad anterior se le llama condición de Ore por la derecha. En general lo hecho en esta sección se puede generalizar de manera análoga para la condición por la izquierda. Un **dominio de Ore** es un anillo sin divisores de cero que satisface la condición de Ore.

Definición 3.3.3. *Sea R un anillo. Un subconjunto T de R es un **conjunto divisor derecho** de R si satisface,*

- $0 \notin T, 1 \in T$.
- *T es cerrado bajo la multiplicación del anillo.*
- *Si $r \in R$ y $t \in T$, existen $r_1 \in R, t_1 \in T$ tales que $rt_1 = tr_1$.*

Ya que T es cerrado multiplicativamente y $0 \notin T$, los elementos de T necesitan ser "regulares entre sí", es decir, al multiplicar dos de elementos de T el resultado no puede ser cero. La condición anterior puede ser parecida a la condición de Ore, pero en realidad solo restringe a que los "divisores" sean del mismo conjunto T.

Proposición 3.3.4. *Sea $N \trianglelefteq G$ tal que KN es un dominio de Ore. Entonces $KN\backslash\{0\}$ es un conjunto divisor derecho de elementos regulares en KG.*

Demostración. Ya que KN no tiene divisores de cero, todo elemento de $KN\backslash\{0\}$ es regular en KG por la Proposición 2.2.10. Sean $x \in KN\backslash\{0\}$ y $r \in KG$, de forma que

$$r = \sum_{i=1}^{n} r_i g_i, \quad r_i \in K, g_i \in G.$$

Ya que $N \trianglelefteq G$, se cumple $x^{g_i} \in N$ para cada g_i. Ahora, por ser KN dominio de Ore, para $x^{g_1}, x^{g_2} \neq 0$, existen $y_2, t_{1,2}, t_{2,2} \in KN\backslash\{0\}$ tales que

$$y_2 = x^{g_1} t_{1,2} = x^{g_2} t_{2,2}.$$

Supongamos que para $2 \leq m < n$, existen $y_m, t_{1,m}, \ldots t_{m,m} \in KN\backslash\{0\}$ tales que

$$y_m = x^{g_1} t_{1,m} = \cdots = x^{g_m} t_{m,m}.$$

Por la condición de Ore, existen $u_{m+1}, v_{m+1} \in KN\backslash\{0\}$ tales que $y_{m+1} = y_m v_{m+1} = x^{g_{m+1}} u_{m+1}$. Nombrando $t_{i,m+1} = t_{i,m} v_{m+1}$ si $1 \leq i \leq m$ y $t_{m+1,m+1} = u_{m+1}$, se tiene entonces

$$y_{m+1} = x^{g_1} t_{1,m+1} = \cdots = x^{g_{m+1}} t_{m+1,m+1},$$

donde $y_{m+1}, t_{1,m+1}, \ldots t_{m+1,m+1} \in KN\backslash\{0\}$. Así, por inducción, existe $y \in KN\backslash\{0\}$ y $s_1, \ldots, s_n \in KN\backslash\{0\}$ tales que

$$y = x^{g_1} s_1 = x^{g_2} s_2 = \cdots = x^{g_n} s_n.$$

Entonces por lo anterior y ya que $r_i x = x r_i$ para cada i (puesto que $r_i \in K$) se cumple

$$ry = \sum_{i=1}^{n} r_i g_i y = \sum_{i=1}^{n} r_i g_i x^{g_i} s_i = \sum_{i=1}^{n} r_i x g_i s_i = x \sum_{i=1}^{n} r_i g_i s_i,$$

donde además, ya que $ry \neq 0$ por ser $y \in KN\backslash\{0\}$ regular,

$$\sum_{i=1}^{n} r_i g_i s_i \in KG\backslash\{0\},$$

completando el resultado. □

Antes del teorema principal de la sección, demostrado por primera vez en [19], se introducirá alguna notación útil. Primero recordamos la noción de longitud en un producto amalgamado, vista en la Sección 1.3, para cada elemento g en el producto amalgamado $G = G_1 *_N G_2$, definida como el número de letras que tiene su forma normal. Esta noción se puede generalizar para el anillo de grupo de un producto amalgamado G sobre un campo K de la siguiente manera. Si $r \in KG$, entonces

$$\text{long}(r) = \text{máx}\,\{\text{long}(g) \mid g \in \mathbf{sop}(r)\}.$$

Ahora bien, en el producto amalgamado $G = G_1 *_N G_2$, tomando las transversales correspondientes T_1 y T_2 si $g = n_1 t$ está en su forma normal, donde $n_1 \in N$ y t es una palabra en T_1 y T_2 y donde la última letra diferente de 1 en t es un elemento de T_1, se dice que g termina en T_1 o en G_1, análogamente para T_2 y análogamente se dice que g inicia en T_1 ó T_2, cuando la palabra t tiene como primer letra un elemento de T_1 o T_2, respectivamente. Si $g, h \in G$ son tales que g termina en T_1 y h inicia en T_1, se dice que g se solapa con h en T_1, análogamente, si g termina en T_2 y h inicia en T_2, se dice que g se solapa con h en T_2, en cualquiera de los dos casos, $\text{long}(gh) < \text{long}(g)+\text{long}(h)$.

Si $N \trianglelefteq G_1, G_2$ y $g, h \in G$ son tales que su forma normal es $g = n_1 t_1$ y $h = n_2 t_2$, entonces $gh = n_1 t_1 n_2 t_2 = n_1 n_2' t_1 t_2$ con $n_2' \in N$. Por lo que cuando N es normal, $\text{long}(gh) = \text{long}(t_1 t_2)$. La anterior es una noción que se puede generalizar a elementos del anillo de grupo, por ejemplo, si $r, s \in KG$ son tales que r no se solapa con s, entonces $\text{long}(rs) = \text{long}(r) + \text{long}(s)$. Lo anterior será útil para la demostración del siguiente teorema.

Teorema 3.3.5. *Sean G_1, G_2 grupos, K un campo y N un subgrupo normal de G_1 y de G_2. Si KG_1, KG_2 son anillos sin divisores de cero y KN satisface la condición de Ore, entonces KG no tiene divisores de cero, donde $G = G_1 *_N G_2$.*

Demostración. Supongamos que existen $r, s \in KG\backslash\{0\}$ tales que $rs = 0$, con $\text{long}(r) = n$ mínima. Si T_1, T_2 son transversales de G_1 y G_2 en N, respectivamente, y T es el conjunto de las palabras alternantes de elementos en $T_1\backslash\{1\}$ y $T_2\backslash\{1\}$, entonces, por el teorema de la forma normal, es posible escribir

$$r = \sum_i u_i \rho_i, \quad \text{y} \quad s = \sum_i \sigma_i v_i,$$

donde $\rho_i, \sigma_i \in KN$ y $u_i, v_i \in T$, de esta forma,

$$0 = rs = \sum_i \sum_j u_i \rho_i \sigma_j v_j, \tag{3.1}$$

donde cada $u_i \rho_i \sigma_j v_j \neq 0$ ya que KN no tiene divisores de cero y $u_i, v_j \in G$. Si $\text{long}(r) = \text{long}(u_{i_0}) = n$ y $\text{long}(s) = \text{long}(v_{j_0}) = m$ son tales que u_{i_0} termina en T_1 y v_{j_0} termina en T_2, entonces, $\text{long}(u_{i_0}\rho_{i_0}\sigma_{j_0}v_{j_0}) = n + m$ y si $u_{i_0}\rho_{i_0}\sigma_{j_0}v_{j_0} = u_{i_1}\rho_{i_1}\sigma_{j_1}v_{j_1}$, debe pasar entonces que $\text{long}(u_{i_1}\rho_{i_1}\sigma_{j_1}v_{j_1}) = n + m$, pero ya que n y m son máximos en las longitudes de las palabras en r y s, entonces, $\text{long}(u_{i_1}) = n$ y ya que la representación en forma normal es única, las primeras n letras de las palabras $u_{i_0}v_{j_0}$ y $u_{i_1}v_{j_1}$ deben coincidir y por lo tanto, $u_{i_0} = u_{i_1}$, análogamente, $v_{i_0} = v_{i_1}$ y entonces, en el producto (3.1), $u_{i_0}\rho_{i_0}\sigma_{j_0}v_{j_0}$ no se puede cancelar y $rs \neq 0$,

lo que es una contradicción. Así, para todos los u_i, v_j tales que $\text{long}(u_i) = n$ y $\text{long}(v_j) = m$ debe ocurrir que u_i se solape con v_j. Sin pérdida de generalidad, se supone que en T_1.

Reescribimos $r = r' + r''$, donde $g \in \mathbf{sop}(r') \subseteq \mathbf{sop}(r)$ si $\text{long}(g) = n$ o si $\text{long}(g) = n-1$ y g termina en T_2. Entonces

$$r' = \sum x_i \epsilon_i,$$

donde $\epsilon_i \in KG_1 \backslash \{0\}$ y $x_i \in T$ termina en T_2 con longitud $n-1$. De manera similar, $s = s' + s''$, donde $g \in \mathbf{sop}(s') \subseteq \mathbf{sop}(s)$ si $\text{long}(g) = m$ o si $\text{long}(g) = m-1$ y g empieza en T_2. Entonces

$$s' = \sum \delta_i y_i,$$

donde $\delta_i \in KG_1 \backslash \{0\}$ y $y_i \in T$ empieza en T_2 con longitud $m-1$.

Ya que $\text{long}(r'') \leq n-1$ y $\text{long}(s'') \leq m-1$, entonces, $\text{long}(r''s'') \leq n+m-2$. Sean $g \in \mathbf{sop}(r')$ y $h \in \mathbf{sop}(s'')$. Si $\text{long}(g) = n$, entonces g debe terminar en T_1 y si $\text{long}(h) = m-1$, entonces h debe iniciar en T_1, por lo que g se solapa con h. Esto implica $\text{long}(gh) \leq n+m-1-1 = n+m-2$. En cualquier otro caso, también se cumple de manera más evidente $\text{long}(gh) \leq n+m-2$ y por lo tanto $\text{long}(r's'') \leq n+m-2$. Análogamente, $\text{long}(r''s') \leq n+m-2$. Por otra parte,

$$0 = rs = (r'+r'')(s'+s'') = r's' + r's'' + r''s' + r''s'' \quad \Rightarrow \quad r's' = -(r's'' + r''s' + r''s''),$$

por lo que $\text{long}(r's') \leq n+m-2$. Tenemos entonces,

$$r's' = \sum_i \sum_j x_i \epsilon_i \delta_j y_j,$$

donde cada $\epsilon_i \delta_j \neq 0$, pues KG_1 no tiene divisores de cero. Si $\epsilon_{i_0}\delta_{j_0} \in KG_1 \backslash KN$, entonces debe tener un sumando que no está en la clase lateral N, es decir, existen $n' \in N$ y $g_1' \in T_1$ tales que $n'g_1' \in \mathbf{sop}(\epsilon_{i_0}\delta_{j_0})$. Pero x_{i_0}, y_{j_0} tienen longitud igual a $n-1$ y $m-1$, respectivamente, x_{i_0} termina en T_2, y_{j_0} inicia en T_2, lo que implica entonces que x_{i_0} no se solapa con $n'g_1'$, ni $n'g_1'$ se solapa con y_{j_0}, por lo que

$$\text{long}(x_{i_0} n' g_1' y_{j_0}) = (n-1) + 1 + (m-1) = n+m-1.$$

Más aún, ya que la multiplicación tiene la longitud máxima que puede tener, no puede haber otro sumando con el mismo elemento del grupo, pues si $x_{i_1} n'' g_1'' y_{j_1} = x_{i_0} n' g_1' y_{j_0}$, entonces, $N x_{i_1} g_1'' y_{j_1} = N x_{i_0} g_1' y_{j_0}$, pero ya que cada palabra tiene longitud máxima y no se solapan, lo anterior solo pasa si $x_{i_1} = x_{i_0}, g_1'' = g_1'$ y $y_{j_1} = y_{j_0}$ y al ser $x_{i_1} n'' g_1'' y_{j_1} = x_{i_0} n' g_1' y_{j_0}$, también debe ocurrir $n'' = n'$, de esta forma, el sumando con este elemento del grupo no se puede cancelar. Así, $\text{long}(r's') \geq n+m-1$, que es una contradicción, por lo que $\epsilon_i \delta_j \in KN$ para cada i, j.

Por la Proposición 3.3.4, ya que $N \trianglelefteq G$ y KN es dominio de Ore, KN es un conjunto divisor derecho de elementos regulares en KG. Como $\epsilon_1\delta_1 \in KN$ y $\epsilon_1 s \in KG$, existen elementos $x \in KN$ y $y \in KG$ tales que $(\epsilon_1\delta_1)y = (\epsilon_1 s)x$. Puesto que $\epsilon_1 \in KG_1, x \in KN$, deben ser elementos regulares en KG por la Proposición 2.2.10. También obtenemos $s \neq 0$, de donde $(\epsilon_1 s)x \neq 0$ y $y \neq 0$. Entonces $\epsilon_1(\delta_1 y - sx) = 0$, pero ϵ_1 es regular en KG, luego $\delta_1 y = sx$. De lo anterior obtenemos $r\delta_1 y = rsx = 0$.

Ahora tenemos $(r\delta_1)y = 0$, con $y \neq 0$ y $r\delta_1 \neq 0$, por ser $\delta_1 \in KG_1$ regular en KG y $r \neq 0$. Así que $r\delta_1$ es un divisor de cero por la izquierda. Recordemos que $r = r' + r''$, por lo que $r\delta_1 = r'\delta_1 + r''\delta_1$. Pero

$$r'\delta_1 = \sum x_i \epsilon_i \delta_1,$$

donde $\epsilon_i\delta_1 \in KN$ y $\text{long}(x_i) = n-1$, por lo que $\text{long}(r'\delta_1) \leq n-1$. Ahora analizamos $r''\delta_1$. Si $g \in \mathbf{sop}(r'')$ es tal que $\text{long}(g) = n-1$, por definición g termina en $T_1 \subseteq G_1$. Ya que $\delta_1 \in KG_1$, se tiene $\text{long}(g\delta_1) \leq n-1$. Si $\text{long}(g) < n-1$, ya que $\text{long}(\delta_1) = 1$, también se tiene $\text{long}(g\delta_1) \leq n-1$. Así que $\text{long}(r''\delta_1) \leq n-1$ y por lo tanto

$$\text{long}(r\delta_1) = \text{long}(r'\delta_1 + r''\delta_1) \leq \text{máx}\{\text{long}(r'\delta_1), \text{long}(r''\delta_1)\} \leq n-1 < n = \text{long}(r),$$

lo que contradice que r fuese el divisor de cero por la izquierda con longitud mínima. Por lo tanto, KG no tiene divisores de cero. □

Ya que un campo K siempre satisface la condición de Ore al ser conmutativo, tomando $N = \langle 1 \rangle$ en el anterior teorema, se tiene el siguiente corolario.

Corolario 3.3.6. *Sea K un campo y sean G_1, G_2 grupos tales que KG_1, KG_2 no tienen divisores de cero. Entonces $K(G_1 * G_2)$ no tiene divisores de cero.*

3.4 Grupos sin Producto Único

En general, no se conocen mayores avances en el intento de demostrar que la conjetura de la unidad es cierta que los dados por el Teorema 3.2.7. Es por ello que buscar grupos que no satisfagan la condición de producto único se ha vuelto una tarea importante para esta conjetura.

Debido a la complejidad de encontrar grupos sin la condición de producto único, durante algún tiempo se creyó que podría ser una condición equivalente a la de ser libre de torsión. Sin embargo, esto fue desmentido por primera vez en [28] y poco después Promislow en su articulo [27] dio un ejemplo más sencillo de un grupo sin producto único libre de torsión, que en ocasiones se le conoce como el grupo de Promislow, este es

$$P_1 = \left\langle x, y \mid x^{-1}y^2x = y^{-2}, y^{-1}x^2y = x^{-2} \right\rangle.$$

Después, en [5] se generaliza el resultado de Promislow para la familia de grupos

$$P_k = \left\langle x, y \mid x^{-1}y^{2^k}x = y^{-2^k}, y^{-1}x^2y = x^{-2} \right\rangle,$$

Configuramos para $1 \leq i \leq 2^k$ y $0 \leq l \leq 2^k - 1$, los subconjuntos

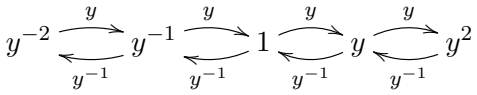
$$\begin{aligned} X_0 &= \{x^{-1}, x^{-1}y\}, \\ X_i &= \{y^i x^{-1} y^j \mid 0 \leq j \leq 2^k + 1\}, \\ Y_l &= \{y^l x y^j \mid 1 \leq j \leq 2^k + 1\}, \\ Z_0 &= \{y^j \mid -2^k \leq j \leq 2^k\}, \end{aligned}$$

de P_k. Si llamamos

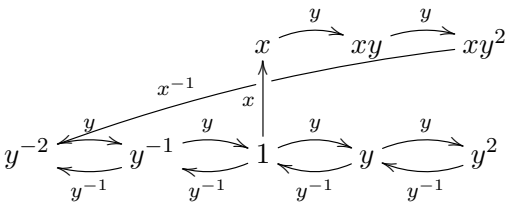
$$T = \left(\bigcup_{i=0}^{2^k-1} X_i \right) \cup \left(\bigcup_{j=0}^{2^k-1} Y_j \right) \cup Z_0,$$

entonces Carter demuestra en [5] que para cada $g \in TT$, se cumple $n_{T\cdot T}(g) > 1$, dando así el resultado. El método usado por Carter para demostrar que TT no tiene producto único, es muy elegante, se basa en progresiones en la gráfica de Cayley generada por el grupo. Es decir, representando puntos en el espacio y haciendo

progresiones a través de la gráfica, lo que se busca son ciclos y así completar dos formas de ir al mismo elemento del grupo. Por ejemplo, para el grupo P_1, se puede tomar la progresión $Z_0 = \{y^{-2}, y^{-1}, 1, y, y^2\}$ que genera los movimientos siguientes en la gráfica



donde solo los elementos y^{-2} y y^2 no son "alcanzables" por dos elementos, por lo que es necesario buscar otra manera de llegar a través de progresiones (en los generadores). Así pues, en este caso es posible usar las relaciones para llegar al elemento y^{-2} de otra forma.



Por supuesto, al momento de agregar más elementos a los conjuntos, es necesario generar más ciclos para los nuevos elementos, hasta que todos los elementos puedan estar en ciclos. Realmente lo anterior es una idea simple, pero con cuidado puede ser llevada de manera adecuada.

En este texto sólo se dará una prueba para otro grupo con conjuntos más pequeños que no tienen producto único. En [35] se analiza un grupo que satisface no tener la propiedad de producto único. Más aún, los conjuntos que no tienen esta propiedad tienen una cardinalidad relativamente pequeña, siendo esta igual a 8. Aquí se analiza este grupo, aunque con diferentes métodos a los realizados en [35].

Retomando el Ejemplo 3.2.16 del grupo libre de torsión de la botella de Klein en las siguientes dos presentaciones G_1, G_2.

$$G_1 = \langle r, x \mid r^2 = x^2 \rangle,$$
$$G_2 = \langle s, y \mid s^2 = y^{-2} \rangle.$$

Como se vio antes, para cada caso, los grupos G_1 y G_2 son productos amalgamados de $\langle r \rangle$ con $\langle x \rangle$ y $\langle s \rangle$ con $\langle y \rangle$, sobre los subgrupos $\langle r^2 \rangle, \langle x^2 \rangle, \langle s^2 \rangle, \langle y^2 \rangle$, que son isomorfos a $\mathbb{Z}$. Las funciones de pegado cumplen $\phi_1(r^2) = x^2$ y $\phi_2(s^2) = y^{-2}$. Es decir, $G_1 = \langle r \rangle *_{\mathbb{Z}} \langle x \rangle$ y $G_2 = \langle s \rangle *_{\mathbb{Z}} \langle y \rangle$.

Por el teorema de la forma normal, todo elemento en G_1, G_2 tiene una forma normal, por lo que es posible evitar el problema de la palabra. En ambos casos, ya que las transversales en cada caso constan del elemento neutro y el generador, cada elemento de G_1 y de G_2 está identificado por su única forma normal,

$$r^{2n_1} r^{\varepsilon_1} x r x \dots r x^{\varepsilon_2},$$
$$s^{2n_3} s^{\varepsilon_3} y s y \dots s y^{\varepsilon_4},$$

donde $\varepsilon_i \in \{0, 1\}$ y $n_i \in \mathbb{Z}$, para $i = 1, 2, 3, 4$. Sean $a = rx^{-1}$ y $b = sy^{-1}$, se mostrará que $\langle a, x^2 \rangle \cong \langle b, y^2 \rangle \cong \mathbb{Z}^2$. En realidad todo es análogo para los dos grupos, por lo que sólo se verá el caso $\langle a, x^2 \rangle$. Primero, para ver que a, x^2 conmutan, calculamos

$$x^{-2} a x^2 = x^{-2}(rx^{-1})x^2 = r^{-2} r x^2 x^{-1} = r^{-1} r^2 x^{-1} = r x^{-1} = a.$$

En general, usando argumentos análogos se ve que para todo $g \in G_1$ se cumple $r^2 g = gr^2$ y $x^2 g = gx^2$. De igual manera, en G_2, los elementos s^2, y^2 (y sus potencias) conmutan con todo elemento $g \in G_2$. Ahora, evidentemente, para cada potencia de x^2 su forma normal es r^2. En el caso de a se tiene

$$a = rx^{-1} = rx^{-2}x = rr^{-2}x = r^{-2}rx$$

y si suponemos que $a^n = r^{-2n}(rx)^n$, entonces

$$\begin{aligned} a^{n+1} &= a(r^{-2n}(rx)^n) \\ &= (rx^{-1})(r^{-2n}(rx)^n) \\ &= rx^{-1}x^{-2n}(rx)^n \\ &= rx^{-2n-1}(rx)^n \\ &= rx^{-2n-2}x(rx)^n \\ &= rr^{-2(n+1)}x(rx)^n \\ &= r^{-2(n+1)}rx(rx)^n \\ &= r^{-2(n+1)}(rx)^{n+1}. \end{aligned}$$

Lo que implica entonces, por inducción, que $(x^2)^m \neq r^{-2n}(rx)^n = a^n$, para cada m entero y n entero positivo, lo cual es suficiente. Pues si $(x^2)^m = a^n$ para un entero n negativo, entonces, $(x^2)^{-m} = a^{-n}$, donde $-n$ es un entero positivo. Así, ninguna potencia de a es igual a alguna potencia de x^2. Ya que a, x^2 son de orden infinito, conmutan y no comparten potencias (distintas de cero), entonces $\mathbb{Z}^2 \cong \langle a, x^2 \rangle$.

Análogamente $\langle b, y^2 \rangle \cong \mathbb{Z}^2 \cong \langle a, x^2 \rangle$. Otra observación importante es que de hecho, $\langle a, x^2 \rangle, \langle b, y^2 \rangle$ son normales en G_1, G_2, respectivamente. Para ver que $\langle a, x^2 \rangle \trianglelefteq G_1$, sólo hay que verificar la normalidad en los generadores, es decir, $r^{-1}\langle a, x^2 \rangle r \subseteq \langle a, x^2 \rangle$ y $x^{-1}\langle a, x^2 \rangle x \subseteq \langle a, x^2 \rangle$, pero a su vez, ya que $g^{-1}hg = g^{-1}hgg^{-1}hg$ y $g^{-1}h^{-1}g = (g^{-1}hg)^{-1}$ para cada $h, g \in G_1$, solo hay que verificar lo siguiente,

$$x^{-1}ax, x^{-1}x^2x, r^{-1}ar, r^{-1}x^2r \in \langle a, x^2 \rangle$$

Esto se verifica en cada caso,

- $x^{-1}ax = x^{-1}(rx^{-1})x = x^{-1}r = xx^{-2}r = xr^{-2}r = xr^{-1} = (rx^{-1})^{-1} = a^{-1} \in \langle a, x^2 \rangle$.
- $x^{-1}x^2x = x^2 \in \langle a, x^2 \rangle$.
- $r^{-1}ar = (ax)^{-1}a(ax) = x^{-1}a^{-1}aax = x^{-1}ax = a^{-1} \in \langle a, x^2 \rangle$.
- $r^{-1}x^2r = (ax)^{-1}x^2(ax) = x^{-1}a^{-1}x^2ax = x^{-1}x^2a^{-1}ax = x^2 \in \langle a, x^2 \rangle$.

Análogamente, para el caso $\langle b, y^2 \rangle \trianglelefteq G_2$, se requiere verificar lo siguiente,

$$y^{-1}by, y^{-1}y^2y, s^{-1}bs, s^{-1}y^2s \in \langle b, y^2 \rangle.$$

Esto se verifica en cada caso

- $y^{-1}by = y^{-1}(sy^{-1})y = y^{-1}s = yy^{-2}s = ys^2s = ys^{-1}s^4 = (sy^{-1})^{-1}y^{-4} = b^{-1}y^{-4} \in \langle b, y^2 \rangle$.
- $y^{-1}y^2y = y^2 \in \langle b, y^2 \rangle$.

- $s^{-1}bs = s^{-1}(sy^{-1})s = y^{-1}s = yy^{-2}s = ys^2s = ys^{-1}s^4 = (sy^{-1})^{-1}y^{-4} = b^{-1}y^{-4} \in \langle b, y^2\rangle$.
- $s^{-1}y^2s = s^{-1}s^{-2}s = s^{-2} = y^2 \in \langle b, y^2\rangle$.

Así que $\langle b, y^2\rangle \trianglelefteq G_2$. Con todo lo anterior, ya que $\langle a, x^2\rangle \cong \langle b, y^2\rangle \cong \mathbb{Z}^2$, se toma el producto amalgamado mediando la función de pegado $\phi\colon \langle a, x^2\rangle \to \langle b, y^2\rangle$ tal que $\phi(a) = \phi(rx^{-1}) = y^2$ y $\phi(x^2) = b = sy^{-1}$, es decir:

$$\begin{aligned} G = G_1 *_{\mathbb{Z}^2} G_2 &= \langle r, x, s, y \mid r^2 = x^2, s^2 = y^{-2}, rx^{-1} = y^2, x^2 = sy^{-1}\rangle \\ &= \langle r, x, s, y \mid r^2 = x^2, s^2 = y^{-2}, r = y^2x, x^2y = s\rangle = \langle x, y \mid (y^2x)^2 = x^2, (x^2y)^2 = y^{-2}\rangle. \end{aligned}$$

Si K es un campo, ya que $\mathbb{Z}$ es abeliano, $K\mathbb{Z}$ satisface la condición de Ore. Puesto que $\mathbb{Z}$ es abeliano, todo subgrupo de $\mathbb{Z}$ es normal, y ya que $\mathbb{Z}$ es un grupo con producto único, $K\mathbb{Z}$ no tiene divisores de cero. Los grupos G_1, G_2 son ambos de la forma $\mathbb{Z} *_{\mathbb{Z}} \mathbb{Z}$, así que por el Teorema 3.3.5, los anillos KG_1 y KG_2 no tienen divisores de cero. A su vez, ya que $\langle a, x^2\rangle \cong \langle b, y^2\rangle \cong \mathbb{Z}^2$ son abelianos, satisfacen la condición de Ore. Además, KG_1, KG_2 no tienen divisores de cero, y se cumple $\langle a, x^2\rangle \trianglelefteq G_1$, $\langle b, y^2\rangle \trianglelefteq G_2$. Por el Teorema 3.3.5, el anillo KG no tiene divisores de cero. Además, G es producto amalgamado de grupos libres de torsión, por lo que por el Corolario 1.3.8 es libre de torsión. Como $a = rx^{-1}$, se tiene $r = ax$ y entonces r pertenece a la clase lateral $\langle a, x^2\rangle x$. Ya que $x^2 \in \langle a, x^2\rangle$, un conjunto transversal para G_1 sobre $\langle a, x^2\rangle$ es $T_1 = \{1, x\}$. De manera similar, un transversal de G_2 sobre $\langle b, y^2\rangle$ es $T_2 = \{1, y\}$. Así, en G, todo elemento tiene una forma normal única como

$$x^{2n_1}a^{n_2}x^{\varepsilon_1}yxy\cdots xy^{\varepsilon_2},$$

donde $n_1, n_2 \in \mathbb{Z}$ y $\varepsilon_1, \varepsilon_2 \in \{0, 1\}$, pero debido a la identificación $a = y^2$, la anterior forma normal se puede reescribir de la siguiente forma,

$$x^{2n_1}y^{2n_2}x^{\varepsilon_1}yxy\cdots xy^{\varepsilon_2}.$$

En realidad, ya que $x^2 = (y^2x)^2 = y^2xy^2x$ y $y^{-2} = (x^2y)^2 = x^2yx^2y$, suceden si y solamente si $xy^2x^{-1} = y^{-2}$ y $yx^2y^3 = x^2$, se puede reescribir la presentación del grupo G de la siguiente manera,

$$G = \langle x, y \mid xy^2x^{-1} = y^{-2}, yx^2y^3 = x^2\rangle$$

Sean entonces

$$\begin{aligned} A &= \{1, x^{-1}, x, y^{-2}, y^{-2}xyx, x^2y, x^2yx, y^{-2}xy\}, \\ B &= \{1, x, x^2, y, xy, y^{-2}yx, y^2xyx, y^{-2}x\}. \end{aligned}$$

Los elementos mostrados de A son diferentes entre sí, lo mismo que los de B, pues todos están en su forma normal, exceptuando $x^{-1} = x^{-2}x$. Probaremos que AB no tiene ningún elemento con producto único. Para ver lo anterior, de la presentación de grupo, se puede verificar

$$\begin{aligned} x^{2j}y^{2l} &= y^{2l}x^{2j} \\ y^{2l}x &= xy^{-2l} \\ yx^2 &= x^{-2}y^{-3} \end{aligned}$$

para $j, l \in \mathbb{Z}$. Estas relaciones se pueden usar para reescribir

$$\begin{aligned} y^{-2}xyx = xy^2yx = xy^3x, \\ y^{-2}xy = xy^2y = xy^3, \\ y^2xyx = xy^{-2}yx = xy^{-1}x. \end{aligned}$$

De esta forma podemos expresar los elementos de A y B en la siguiente forma:

$$A = \{1, x^{-1}, x, y^{-2}, xy^3x, x^2y, x^2yx, xy^3\},$$
$$B = \{1, x, x^2, y, xy, y^{-1}x, xy^{-1}x, y^{-2}x\},$$

de donde, trivialmente, los siguientes productos son iguales en AB.

Número	Producto	Producto 1	Producto 2	Producto 3
1	1	$(1,1)$	(x^{-1},x)	-
2	x	$(1,x)$	(x^{-1},x^2)	$(x,1)$
3	x^2	$(1,x^2)$	(x,x)	-
4	y	$(1,y)$	(x^{-1},xy)	-
5	xy	$(1,xy)$	(x,y)	-
6	$y^{-1}x$	$(1,y^{-1}x)$	$(x^{-1},xy^{-1}x)$	-
7	$xy^{-1}x$	$(1,xy^{-1}x)$	$(x,y^{-1}x)$	-
8	$y^{-2}x$	$(1,y^{-2}x)$	(y^{-2},x)	-
9	x^3	(x,x^2)	$(x^2y,y^{-1}x)$	-
10	x^2y	(x,xy)	$(x^2y,1)$	-
11	$x^2y^{-1}x$	$(x,xy^{-1}x)$	$(x^2y,y^{-2}x)$	-
12	xy^3x	$(xy^3x,1)$	(xy^3,x)	-
13	xy^3x^2	(xy^3x,x)	(xy^3,x^2)	-
14	xy^3xy	(xy^3x,y)	(xy^3,xy)	-
15	$xy^3xy^{-1}x$	$(xy^3x,y^{-1}x)$	$(xy^3,xy^{-1}x)$	-
16	x^2yx	(x^2y,x)	$(x^2yx,1)$	-
17	x^2yx^2	(x^2y,x^2)	(x^2yx,x)	-
18	x^2yxy	(x^2y,xy)	(x^2yx,y)	-
19	$x^2yxy^{-1}x$	$(x^2y,xy^{-1}x)$	$(x^2yx,y^{-1}x)$	-

Lo que en total da $19 \cdot 2 + 1 = 39$ productos que no son únicos en AB. Como $|A| = |B| = 8$, entonces el total de productos en AB son $8 \cdot 8 = 64$, por lo que resta verificar $64 - 39 = 25$ productos, los cuales son

$(x^{-1},1)$	(x^{-1},y)	$(x^{-1},y^{-1}x)$	$(x^{-1},y^{-2}x)$	$(x,y^{-2}x)$
$(y^{-2},1)$	(y^{-2},x^2)	(y^{-2},y)	(y^{-2},xy)	$(y^{-2},y^{-1}x)$
$(y^{-2},xy^{-1}x)$	$(y^{-2},y^{-2}x)$	(xy^3x,xy)	$(xy^3x,y^{-2}x)$	(xy^3x,x^2)
$(xy^3x,xy^{-1}x)$	(x^2y,y)	(x^2yx,xy)	$(xy^3,y^{-1}x)$	$(x^2yx,y^{-2}x)$
$(xy^3,1)$	(x^2yx,x^2)	$(xy^3,y^{-2}x)$	$(x^2yx,xy^{-1}x)$	(xy^3,y)

Se verifica entonces, ya que $yx^2y^3 = x^{-2}$, la siguiente relación:

$$x^2 = (yx^2y^3)^{-1} = y^{-3}x^{-2}y^{-1}.$$

Así, $y^3x^2y = x^{-2}$. De esta manera, se puede escribir el primer producto como

$$(x^{-1})(1) = x^{-1} = xx^{-2} = xy^3x^2y = (xy^3x)(xy).$$

Ahora, para los demás productos se tiene lo expresado a continuación.

$$
\begin{aligned}
(x^{-1})(y) &= x^{-1}y = xx^{-2}y = x(y^3x^2y)y = xy^3x^2y^2 = xy^3xxy^2 = xy^3xy^{-2}x = (xy^3x)(y^{-2}x),\\
(x^{-1})(y^{-1}x) &= x^{-1}y^{-1}x = xx^{-2}y^{-1}x = x(y^3x^2y)y^{-1}x = xy^3x^3 = (xy^3x)(x^2),\\
(x^{-1})(y^{-2}x) &= x^{-1}y^{-2}x = xx^{-2}y^{-2}x = x(y^3x^2y)y^{-2}x = xy^3x^2y^{-1}x = (xy^3x)(xy^{-1}x),\\
(x)(y^{-2}x) &= xy^{-2}x = xxy^2 = (x^2y)(y),\\
(y^{-2})(1) &= y^{-2} = y^{-3}y = y^{-3}x^{-2}x^2y = y^{-3}(y^3x^2y)x^2y = x^2yx^2y = (x^2yx)(xy),\\
(y^{-2})(x^2) &= y^{-2}xx = xy^2x = (xy^3)(y^{-1}x),\\
(y^{-2})(y) &= y^{-1} = y^{-1}x^{-2}x^2 = y^{-1}(yx^2y^3)x^2 = x^2y^3x^2 = x^2yy^2xx = x^2yxy^{-2}x = (x^2yx)(y^{-2}x),\\
(y^{-2})(xy) &= y^{-2}xy = xy^2y = (xy^3)(1),\\
(y^{-2})(y^{-1}x) &= y^{-3}x = y^{-3}x^{-2}x^3 = y^{-3}(y^3x^2y)x^3 = x^2yx^3 = (x^2yx)(x^2),\\
(y^{-2})(xy^{-1}x) &= y^{-2}xy^{-1}x = xy^2y^{-1}x = xy^3y^{-2}x = (xy^3)(y^{-2}x),\\
(y^{-2})(y^{-2}x) &= y^{-4}x = x^2x^{-2}y^{-4}x = x^2(yx^2y^3)y^{-4}x = x^2yx^2y^{-1}x = (x^2yx)(xy^{-1}x),\\
(y^{-2})(y^{-2}x) &= y^{-4}x = xy^4 = (xy^3)(y).
\end{aligned}
$$

De esta forma, todos los productos sobrantes también tienen otros productos iguales. En la siguiente tabla se muestran todos los productos faltantes.

Número	Producto	Producto 1	Producto 2	Producto 3
20	x^{-1}	$(x^{-1},1)$	(xy^3x,xy)	-
21	$x^{-1}y$	(x^{-1},y)	$(xy^3x,y^{-2}x)$	-
22	$x^{-1}y^{-1}x$	$(x^{-1},y^{-1}x)$	(xy^3x,x^2)	-
23	$x^{-1}y^{-2}x$	$(x^{-1},y^{-2}x)$	$(xy^3x,xy^{-1}x)$	-
24	$xy^{-2}x$	$(x,y^{-2}x)$	(x^2y,y)	-
24	y^{-2}	$(y^{-2},1)$	(x^2yx,xy)	-
26	$y^{-2}x^2$	(y^{-2},x^2)	$(xy^3,y^{-1}x)$	-
27	y^{-1}	(y^{-2},y)	$(x^2yx,y^{-2}x)$	-
28	$y^{-2}xy$	(y^{-2},xy)	$(xy^3,1)$	-
29	$y^{-3}x$	$(y^{-2},y^{-1}x)$	(x^2yx,x^2)	-
30	$y^{-2}xy^{-1}x$	$(y^{-2},xy^{-1}x)$	$(xy^3,y^{-2}x)$	-
31	$y^{-4}x$	$(y^{-2},y^{-2}x)$	$(x^2yx,xy^{-1}x)$	(xy^3,y)

Por lo que ningún elemento en AB tiene producto único. Aunque es interesante ver que no todos los números $n_{A\cdot B}(g)$ son pares, pues hay dos elementos que tienen este valor igual a 3, que de hecho, tienen que ser diferentes, pues $\mathbb{F}_2G$ no tiene divisores de cero. Es importante ver también, que de hecho, como se reescribió antes,

$$x^2 = (y^2x)^2 = y^2xy^2x \quad \Rightarrow \quad x = y^2xy^2 \quad \Rightarrow \quad y^{-2} = x^{-1}y^2x,$$

por lo que la primera relación puede ser cambiada por $y^{-2} = x^{-1}y^2x$. De esta forma, también se puede ver $P_1 = G_1 *_{\mathbb{Z}^2} G_1$ y modificando las potencias adecuadas, $P_k = G_1 *_{\mathbb{Z}^2} G_1$, para cada $k \in \mathbb{N}$. Lo que a su vez, análogamente a lo que se hizo en esta sección, implica que cada P_k no tiene divisores de cero.

Como se vio antes en el Ejemplo 3.2.16, las presentaciones dadas para los grupos G_1 y G_2 son presentaciones conocidas del grupo fundamental de la botella de Klein, que como se vio es un grupo libre de torsión y al ser ordenado por la izquierda satisface la propiedad de producto único. Es interesante, pues deja claro que productos amalgamados de grupos con producto único no tienen porque ser grupos con producto único y más aún porque estos ejemplos tan representativos que no satisfacen la propiedad tienen de alguna manera "metido" este grupo.

Otro punto relevante a considerar es que el grupo G de Soelberg no es isomorfo a ningun grupo P_k. Primero, considerando los cocientes P_k/P_k' y G/G',

$$\begin{aligned} G/G' &= \langle x, y \mid (y^2x)^2 = x^2, (x^2y)^2 = y^{-2}, xy = yx \rangle = \langle x, y \mid y^4 = 1, x^4y^4 = 1, xy = yx \rangle \\ &= \langle x, y \mid y^4 = 1, x^4 = 1, xy = yx \rangle \cong \mathbb{Z}/4 \oplus \mathbb{Z}/4, \\ P_k/P_k' &= \left\langle x, y \mid x^{-1}y^{2^k}x = y^{-2^k}, y^{-1}x^2y = x^{-2}, xy = yx \right\rangle = \left\langle x, y \mid y^{2^{k+1}} = 1, x^4 = 1, xy = yx \right\rangle \\ &\cong \mathbb{Z}/2^{k+1} \oplus \mathbb{Z}/4, \end{aligned}$$

por lo que $P_k/P_k' \cong G/G'$ si y sólo si $k = 1$. Por la Proposición 1.1.9, el grupo G no es isomorfo a P_k si $k \geq 2$. El caso $k = 1$ se verifica en el Código A del Apéndice.

Teorema 3.4.1. *Sea* $G = \langle x, y \mid (y^2x)^2 = x^2, (x^2y)^2 = y^{-2} \rangle \cong \langle x, y \mid xy^2x^{-1} = y^{-2}, yx^2y^3 = x^{-2} \rangle$.

a) G no satisface la propiedad de producto único.

b) $G \ncong P_k$ para cada $k \geq 1$.

c) G satisface la conjetura de divisor de cero de Kaplansky.

4 La Conjetura de la Unidad

Diversos avances y esfuerzos se han realizado para resolver las tres conjeturas de Kaplansky. Recientemente, una de las tres conjeturas fue resuelta como falsa, pues fue dado un contraejemplo para un grupo conocido del capítulo anterior como P_1, el grupo de Promislow. En este capítulo, se analiza el contraejemplo dado, desde diferentes perspectivas y se abunda un poco en el trabajo posterior a la resolución de este contraejemplo.

4.1 El Contraejemplo de la Conjetura de la Unidad

En un articulo de 2021 [10], Giles Gardam resolvió por primera vez una de las tres conjeturas de Kaplansky, la conjetura de la unidad. La respuesta fue negativa y más aún, el contraejemplo dado satisface las otras dos conjeturas de Kaplansky, por lo que no dice nada concreto acerca de estas.

El contraejemplo dado por Gardam usa el grupo P_1 dado en la sección anterior, que por convención y siguiendo la notación que se le ha dado recientemente en este documento, se toma con generadores a y b. Es decir, se toma el siguiente grupo.

$$P_1 = \left\langle a, b \mid a^{-1}b^2a = b^{-2}, b^{-1}a^2b = a^{-2} \right\rangle.$$

Gardam demostró que el anillo de grupo $\mathbb{F}_2P_1$ tiene una unidad no trivial. Poco después al resultado de Gardam, Murray [23] generalizó un poco más el resultado para características mayores y recientemente, el mismo Gardam dio un contraejemplo para característica cero en [11]. En esta sección se analizan todos estos contrajemplos encontrados para el grupo P_1.

Para el resto de esta sección, siempre que se tomen a, b, se refiere a los generadores del grupo P_1. Además se toman, $x = a^2$, $y = b^2$ y $z = (ab)^2$. Primero es importante notar que x, y, z conmutan entre sí, pues se tienen las siguientes relaciones:

$$b^2 = (a^{-1}b^2a)^{-1} = a^{-1}b^{-2}a \quad \text{y} \quad a^2 = (b^{-1}a^2b)^{-1} = b^{-1}a^{-2}b,$$

las cuales a su vez implican las siguientes relaciones que dan pie a la conmutatividad de x, y, z entre sí.

$$x^{-1}yx = a^{-2}b^2a^2 = a^{-1}a^{-1}b^2aa = a^{-1}(b^{-2})a = b^2 = y.$$
$$x^{-1}zx = a^{-2}(ab)^2a^2 = a^{-2}ababb^{-1}a^{-2}b = a^{-1}ba^{-1}b = a^{-1}ba^{-2}ab = a^{-1}b(b^{-1}a^2b)ab = (ab)^2 = z.$$
$$y^{-1}zy = b^{-2}(ab)^2b^2 = b^{-2}ababb^2 = (ab^2a^{-1})aba(a^{-1}b^{-2}a)b = abab = z.$$

Además, también es importante ver de la presentación de grupo que $ab^{-2} = b^2a$ y $ba^{-2} = a^2b$. También

para cada x, y, z los generadores de P_1 actúan de la siguiente manera. Primero con a se tiene

$$\begin{aligned}
a^{-1}xa &= a^{-1}a^2a = a^2 = x,\\
a^{-1}ya &= a^{-1}b^2a = a^{-1}ab^{-2} = b^{-2} = y^{-1},\\
a^{-1}za &= a^{-1}(abab)a = baba = ba^{-1}a^2b^2b^{-1}a = ba^{-1}b^2a^2b^{-1}a = bb^{-2}a^{-1}b^{-1}a^{-2}a\\
&= b^{-1}a^{-1}b^{-1}a^{-1} = (b^{-1}a^{-1})^2 = (ab)^{-2} = z^{-1}.
\end{aligned}$$

Mientras que con b se cumple

$$\begin{aligned}
b^{-1}xb &= b^{-1}a^2b = b^{-1}ba^{-2} = x^{-1},\\
b^{-1}yb &= b^{-1}b^2b = b^2 = y,\\
b^{-1}zb &= b^{-1}(abab)b = b^{-1}abab^2 = b^{-1}abb^{-2}a = b^{-1}ab^{-1}a = b^{-1}a^{-1}a^2b^{-1}a = b^{-1}a^{-1}b^{-1}a^{-2}a\\
&= b^{-1}a^{-1}b^{-1}a^{-1} = (b^{-1}a^{-1})^2 = (ab)^{-2} = z^{-1}.
\end{aligned}$$

De lo anterior se tiene entonces que

$$\begin{aligned}
ax &= xa, & bx^{-1} &= xb,\\
ay^{-1} &= ya, & by &= yb,\\
az^{-1} &= za, & bz^{-1} &= zb.
\end{aligned}$$

Otra relación útil que se utilizará más adelante es la siguiente:

$$ba = b(xa^{-1}) = x^{-1}ba^{-1} = x^{-1}(yb^{-1})a^{-1} = x^{-1}yb^{-1}(ab)^{-1} = x^{-1}yz^{-1}ab. \tag{4.1}$$

Sea ahora un campo K. Bajo lo anterior, se obtiene que los elementos x, y, z generan un subanillo conmutativo $K\langle x, y, z\rangle$ de KP_1, que de hecho es muy representativo de este, como se ve a continuación.

Proposición 4.1.1. *Si $\theta \in KP_1$, entonces existe una única 4-tupla $(p, q, r, s) \in K\langle x, y, z\rangle^4$ tal que*

$$\theta = p + qa + rb + sab.$$

Demostración. Basta con ver que cada elemento $g \in P_1$ se puede representar de forma única de alguna (y sólo una) de las siguientes formas $g = ha, g = hb, g = hab$ ó $g = h$, para algún $h \in \langle x, y, z\rangle$. En particular, por la conmutatividad de x, y, z, el elemento h debe ser igual a $x^\alpha y^\beta z^\gamma$, para algunos $\alpha, \beta, \gamma \in \mathbb{Z}$. Sea $g \in P_1$. Entonces, como se observó en la Sección 3.4, por el teorema de la forma normal, g se puede expresar de forma única como

$$g = x^k y^l b^{\varepsilon_1} aba \dots ba^{\varepsilon_3} = x^k y^l b^{\varepsilon_1} z^n (ab)^{\varepsilon_2} a^{\varepsilon_3}, \tag{4.2}$$

donde $k, l \in \mathbb{Z}$, $n \in \mathbb{N} \cup \{0\}$ y $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \{0, 1\}$. Se tiene cada uno de los siguientes ocho casos.

- $\varepsilon_1 = 0, \varepsilon_2 = 0, \varepsilon_3 = 0$. Entonces, $g = x^k y^l z^n \in \langle x, y, z\rangle$.
- $\varepsilon_1 = 0, \varepsilon_2 = 0, \varepsilon_3 = 1$. Entonces, $g = x^k y^l z^n a$ y se tiene la forma deseada.
- $\varepsilon_1 = 0, \varepsilon_2 = 1, \varepsilon_3 = 0$. Entonces, $g = x^k y^l z^n ab$ y se tiene la forma deseada.

- $\varepsilon_1 = 0, \varepsilon_2 = 1, \varepsilon_3 = 1$. Entonces, $g = x^k y^l z^n aba$ y de acuerdo a (4.1),

$$g = x^k y^l z^n aba = x^k y^l z^n a x^{-1} y z^{-1} ab = x^k y^l z^n x^{-1} y^{-1} z aab = x^{k-1} y^{l-1} z^{n+1} xb = x^k y^{l-1} z^{n+1} b,$$

obteniendo la forma deseada.

- $\varepsilon_1 = 1, \varepsilon_2 = 0, \varepsilon_3 = 0$. Entonces, $g = x^k y^l bz^n = x^k y^l z^{-n} b$, obteniendo la forma deseada.

- $\varepsilon_1 = 1, \varepsilon_2 = 0, \varepsilon_3 = 1$. Entonces, $g = x^k y^l bz^n a = x^k y^l z^{-n} ba$ y se tiene lo siguiente:

$$g = x^k y^l z^{-n} ba = x^k y^l z^{-n} x^{-1} y z^{-1} ab = x^{k-1} y^{l+1} z^{-n-1} ab,$$

obteniendo la forma deseada.

- $\varepsilon_1 = 1, \varepsilon_2 = 1, \varepsilon_3 = 0$. Entonces, $g = x^k y^l bz^n ab = x^k y^l z^{-n} bab$, por lo que de acuerdo a (4.1)

$$\begin{aligned} g &= x^k y^l z^{-n} bab = x^k y^l z^{-n} (x^{-1} y z^{-1} ab) b = x^{k-1} y^{l+1} z^{-n-1} ay \\ &= x^{k-1} y^{l+1} z^{-n-1} y^{-1} a = x^{k-1} y^l z^{-n-1} a, \end{aligned}$$

obteniendo la forma deseada.

- $\varepsilon_1 = 1, \varepsilon_2 = 1, \varepsilon_3 = 1$. Entonces, $g = x^k y^l bz^n (ab) a = x^k y^l z^{-n} (ba)^2 = x^k y^l z^{-n} (x^{-1} y z^{-1} ab)^2$, luego

$$\begin{aligned} g &= x^k y^l z^{-n} x^{-1} y z^{-1} abx^{-1} y z^{-1} ab = x^{k-1} y^{l+1} z^{-n-1} axyzbab = x^{k-1} y^{l+1} z^{-n-1} xy^{-1} z^{-1} abab \\ &= x^k y^l z^{-n-2} (ab)^2 = x^k y^l z^{-n-1} \in \langle x, y, z \rangle . \end{aligned}$$

Realizando los pasos inversos hechos antes se puede observar que un elemento de la forma $x^\alpha y^\beta z^\gamma g$, con $g \in \{1, a, b, ab\}$ y $\alpha, \beta, \gamma \in \mathbb{Z}$ tiene una forma normal determinada por cada uno de los casos que se darán a continuación. De acuerdo a (4.2), ya que la forma normal es única, se obtiene la unicidad.

Caso	Forma Normal
$\gamma \geq 0, g = 1$	$x^k y^l z^n$
$\gamma < 0, g = 1$	$x^k y^l bz^n (ab) a$
$\gamma \geq 0, g = a$	$x^k y^l z^n a$
$\gamma < 0, g = a$	$x^k y^l bz^n (ab)$
$\gamma \geq 1, g = b$	$x^k y^l z^n (ab) a$
$\gamma < 1, g = b$	$x^k y^l bz^n$
$\gamma \geq 0, g = ab$	$x^k y^l z^n (ab)$
$\gamma < 0, g = ab$	$x^k y^l bz^n a$

□

Una notación útil introducida por Murray para los elementos de $K\langle x, y, z \rangle$ es la siguiente. Dado $p \in K\langle x, y, z \rangle$, denotamos por p_x, p_y, p_z a los elementos en $K\langle x, y, z \rangle$ resultantes de remplazar x, y, z por x^{-1}, y^{-1}, z^{-1}, respectivamente. Las expresiones como p_{xy}, p_{xz}, p_{yz} también son el resultado de remplazar inversos, pero ahora para ambos, x, y o x, z ó y, z respectivamente. Análogamente se definiría p_{xyz}. Por ejemplo, si $p = x + y + z$,

$$\begin{aligned} p_x &= x^{-1} + y + z, & p_y &= x + y^{-1} + z, & p_z &= x + y + z^{-1}, \\ p_{xy} &= x^{-1} + y^{-1} + z, & p_{xz} &= x^{-1} + y + z^{-1}, & p_{yz} &= x + y^{-1} + z^{-1} \end{aligned}$$

y también $p_{xyz} = x^{-1} + y^{-1} + z^{-1}$. Por las acciones vistas de los elementos a, b sobre x, y, z se tienen entonces que para cada $p \in K\langle x, y, z\rangle$ las siguientes relaciones.

$$ap = p_{yz}a, \qquad bp = p_{xz}b, \qquad (ab)p = ap_{xz}b = p_{xy}(ab). \tag{4.3}$$

En la siguiente proposición expresaremos la existencia de una inversa en KP_1 en términos de existencia de solución a un sistema de ecuaciones en $K\langle x, y, z\rangle$.

Proposición 4.1.2. *Sean $\theta, \eta \in KP_1$ tales que $\theta = p + qa + rb + sab$ y $\eta = p' + q'a + r'b + s'ab$, con $p, q, r, s, p', q', r', s' \in K\langle x, y, z\rangle$. Entonces $\eta\theta = 1$ si y sólo si se cumplen las siguientes cuatro igualdades.*

$$\begin{array}{lllllllll}
p'p & + & xq'q_{yz} & + & yr'r_{xz} & + & zs's_{xy} & = 1, \\
p'q & + & q'p_{yz} & + & x^{-1}z^{-1}r's_{xz} & + & y^{-1}s'r_{xy} & = 0, \\
p'r & + & xq's_{yz} & + & r'p_{xz} & + & y^{-1}zs'q_{xy} & = 0, \\
p's & + & q'r_{yz} & + & x^{-1}yz^{-1}r'q_{xz} & + & s'p_{xy} & = 0.
\end{array}$$

Demostración. Realizando la multiplicación $\eta\theta$, se obtiene lo siguiente:

$$\begin{aligned}
\eta\theta &= (p' + q'a + r'b + s'ab)(p + qa + rb + sab) \\
&= p'p + p'qa + p'rb + p'sab \\
&+ q'ap + q'aqa + q'arb + q'asab \\
&+ r'bp + r'bqa + r'brb + r'bsab \\
&+ s'abp + s'abqa + s'abrb + s'absab
\end{aligned}$$

Utilizando las relaciones de (4.3) para llevar a una forma única de acuerdo a la Proposición 4.1.1, se reescribe el anterior sistema de la siguiente manera:

$$\begin{aligned}
\eta\theta &= p'p + p'qa + p'rb + p'sab \\
&+ q'p_{yz}a + q'q_{yz}a^2 + q'r_{yz}ab + q's_{yz}a^2b \\
&+ r'p_{xz}b + r'q_{xz}ba + r'r_{xz}b^2 + r's_{xz}bab \\
&+ s'p_{xy}ab + s'q_{xy}aba + s'r_{xy}ab^2 + s's_{xy}(ab)^2 \\
&= p'p + p'qa + p'rb + p'sab \\
&+ q'p_{yz}a + q'q_{yz}x + q'r_{yz}ab + q's_{yz}xb \\
&+ r'p_{xz}b + r'q_{xz}ba + r'r_{xz}y + r's_{xz}bab \\
&+ s'p_{xy}ab + s'q_{xy}aba + s'r_{xy}ay + s's_{xy}z.
\end{aligned}$$

Ahora, utilizando la relación (4.1) y las acciones de a y b sobre x, y, z se tienen las siguientes relaciones.

$$\begin{aligned}
r'q_{xz}ba &= r'q_{xz}x^{-1}yz^{-1}ab, \\
r's_{xz}bab &= r's_{xz}(x^{-1}yz^{-1}ab)b = r's_{xz}x^{-1}yz^{-1}ay = r's_{xz}x^{-1}yz^{-1}y^{-1}a = r's_{xz}x^{-1}z^{-1}a, \\
s'q_{xy}aba &= s'q_{xy}a(x^{-1}yz^{-1}ab) = s'q_{xy}x^{-1}y^{-1}za^2b = s'q_{xy}x^{-1}y^{-1}zxb = s'q_{xy}y^{-1}zb, \\
s'r_{xy}ay &= s'r_{xy}y^{-1}a.
\end{aligned}$$

Con las relaciones anteriores, el cálculo anterior de $\eta\theta$ y la conmutatividad de $K\langle x,y,z\rangle$ se tiene entonces la siguiente factorización.

$$\begin{aligned}\eta\theta = &(p'p + xq'q_{yz} + yr'r_{xz} + zs's_{xy})\\ &+ (p'q + q'p_{yz} + x^{-1}z^{-1}r's_{xz} + y^{-1}s'r_{xy})a\\ &+ (p'r + xq's_{yz} + r'p_{xz} + y^{-1}zs'q_{xy})b\\ &+ (p's + q'r_{yz} + x^{-1}yz^{-1}r'q_{xz} + s'p_{xy})ab.\end{aligned}$$

Por la Proposición 4.1.1, la forma anterior es única, por lo que $\eta\theta = 1$ si y sólo si el coeficiente de 1 es 1 y los coeficientes de a, b, ab son cero, obteniendo el resultado. □

El resultado anterior convierte el problema de las unidades en KP_1 a un problema de cálculos en un anillo conmutativo, lo cual facilita el proceso. En este punto, se hace notar la forma en que Murray en [23] pudo reducir el problema aún más hacia el cálculo de operaciones solo en $K\langle z\rangle$. Esto se observa en el siguiente resultado, en el que se usa la notación $w^* = w_z$ para un elemento $w \in K\langle z\rangle$, donde w_z es como se introdujo antes para elementos en $K\langle x,y,z\rangle$, es decir, se sustituye z por z^{-1} en w.

Proposición 4.1.3. *Sean $w_1, w_2, w_3, w_4, w_5, w_6, w_7 \in K\langle z\rangle$ distintos de cero que cumplen las siguientes relaciones.*

$$\begin{aligned}w_7^*w_7 &= 1,\\ w_3^*w_3 = w_5^*w_5 &= w_7^*w_6 + w_6^*w_7 + 4w_6^*w_6,\\ w_2^*w_2 = w_4^*w_4 &= w_6^*w_6,\\ w_1^*w_1 &= w_2^*w_3 + w_4^*w_5,\\ w_2^*w_5 = zw_5^*w_2 = w_3^*w_4 &= zw_4^*w_3 = w_6^*w_1 + zw_1^*w_6 - (w_2^*w_4 + zw_4^*w_2),\\ w_3^*w_5 + zw_5 * w_3 &= w_7^*w_1 + zw_1^*w_7 + 4(w_2^*w_4 + zw_4^*w_2).\end{aligned}$$

Sean también

$$\begin{aligned}p &= (1+x)(1+y)w_1\\ q &= (1+x)(x^{-1}+y^{-1})w_2 + (1+y^{-1})w_3\\ r &= (1+y^{-1})(x+y)w_4 + (1+x)w_5\\ s &= (4+x+x^{-1}+y+y^{-1})w_6 + w_7,\end{aligned}$$

y además, sean $p' = x^{-1}p_{yz}, q' = -x^{-1}q, r' = -y^{-1}r, s' = z^{-1}s_z$. Entonces $(p' + q'a + r'b + s'ab)(p + qa + rb + sab) = 1$. Más aún, $p + qa + rb + sab$ es una unidad no trivial en KP_1.

Demostración. Por la Proposición 4.1.1, la forma $p+qa+rb+sab$ es única, por lo que para ver que es no trivial, basta con ver que existen dos sumandos distintos de cero en p. Reescribimos

$$p = (1 + x + y + xy)w_1 = w_1 + xw_1 + yw_1 + xyw_1.$$

Al ser $\langle x,y,z\rangle$ un grupo ordenado por el Ejemplo 3.2.14, es de producto único y no tiene divisores de cero. Así, ya que por hipótesis $w_1 \neq 0$, cada sumando en la expresión anterior es distinto de cero. Además w_1 es linealmente independiente a xw_1, yw_1, xyw_1 ya que $w_1 \in K\langle z\rangle$, por lo que hay dos sumandos distintos de cero.

Así, $p+qa+rb+sab$ es no trivial, resta ver que en efecto es una unidad. Para ello se hace uso de la Proposición 4.1.2 y se verifica cada una de las ecuaciones.

$$\mathbf{p'p + xq'q_{yz} + yr'r_{xz} + zs's_{xy} = 1}$$

Se toma $\alpha = p'p + xq'q_{yz} + yr'r_{xz} + zs's_{xy}$ y desarrollando la expresión,

$$\begin{aligned}
\alpha &= p'p + xq'q_{yz} + yr'r_{xz} + zs's_{xy} \\
&= (x^{-1}p_{yz})p + x(-x^{-1}q)q_{yz} + y(-y^{-1}r)r_{xz} + z(z^{-1}s_z)s_{xy} \\
&= x^{-1}[(1+x)(1+y^{-1})w_1^*][(1+x)(1+y)w_1] \\
&- [(1+x)(x^{-1}+y^{-1})w_2 + (1+y^{-1})w_3][(1+x)(x^{-1}+y)w_2^* + (1+y)w_3^*] \\
&- [(1+y^{-1})(x+y)w_4 + (1+x)w_5][(1+y^{-1})(x^{-1}+y)w_4^* + (1+x^{-1})w_5^*] \\
&+ [(4+x+x^{-1}+y+y^{-1})w_6^* + w_7^*][(4+x+x^{-1}+y+y^{-1})w_6 + w_7].
\end{aligned}$$

De lo anterior, desarrollando todos los sumandos,

$$\begin{aligned}
\alpha &= x^{-1}(1+x)^2(1+y^{-1})(1+y)w_1^*w_1 \\
&- (1+x)^2(x^{-1}+y^{-1})(x^{-1}+y)w_2w_2^* - (1+x)(x^{-1}+y^{-1})(1+y)w_2w_3^* \\
&- (1+x)(x^{-1}+y)(1+y^{-1})w_3w_2^* - (1+y^{-1})(1+y)w_3w_3^* \\
&- (1+y^{-1})^2(x+y)(x^{-1}+y)w_4w_4^* - (1+y^{-1})(x+y)(1+x^{-1})w_4w_5^* \\
&- (1+x)(1+y^{-1})(x^{-1}+y)w_5w_4^* - (1+x)(1+x^{-1})w_5w_5^* \\
&+ (4+x+x^{-1}+y+y^{-1})^2w_6^*w_6 + (4+x+x^{-1}+y+y^{-1})w_6^*w_7 \\
&+ (4+x+x^{-1}+y+y^{-1})w_7^*w_6 + w_7^*w_7.
\end{aligned}$$

Por la segunda relación de la hipótesis,

$$\begin{aligned}
-(1+y^{-1})(1+y)w_3w_3^* - (1+x)(1+x^{-1})w_5w_5^* &= -(1+y^{-1})(1+y)w_3w_3^* - (1+x)(1+x^{-1})w_3w_3^* \\
&= -[(1+y^{-1})(1+y) + (1+x)(1+x^{-1})]w_3w_3^* \\
&= -[2+y^{-1}+y+2+x+x^{-1}]w_3w_3^* \\
&= -[4+x+x^{-1}+y+y^{-1}]w_3w_3^*,
\end{aligned}$$

de donde la expresión

$$\begin{aligned}
-(1+y^{-1})(1+y)w_3w_3^* - (1+x)(1+x^{-1})w_5w_5^* + (4+x+x^{-1}+y+y^{-1})^2w_6^*w_6 \\
+(4+x+x^{-1}+y+y^{-1})w_6^*w_7 + (4+x+x^{-1}+y+y^{-1})w_7^*w_6,
\end{aligned} \tag{4.4}$$

puede ser escrita como

$$-[4+x+x^{-1}+y+y^{-1}]w_3w_3^* + (4+x+x^{-1}+y+y^{-1})^2w_6^*w_6 + (4+x+x^{-1}+y+y^{-1})(w_6^*w_7 + w_7^*w_6).$$

Factorizamos para obtener

$$[4+x+x^{-1}+y+y^{-1}][-w_3w_3^* + (4+x+x^{-1}+y+y^{-1})w_6^*w_6 + w_6^*w_7 + w_7^*w_6],$$

pero puesto que de la segunda relación de la hipótesis obtenemos $-w_3^*w_3+w_7^*w_6+w_6^*w_7+4w_6^*w_6=0$, entonces la expresión es igual a

$$(4+x+x^{-1}+y+y^{-1})(x+x^{-1}+y+y^{-1})w_6^*w_6. \tag{4.5}$$

Ahora bien, para la siguiente expresión

$$x^{-1}(1+x)^2(1+y^{-1})(1+y)w_1^*w_1-(1+x)(x^{-1}+y)(1+y^{-1})w_3w_2^*-(1+x)(1+y^{-1})(x^{-1}+y)w_5w_4^*,$$

factorizamos

$$x^{-1}(1+x)^2(1+y^{-1})(1+y)w_1^*w_1-[(1+x)(x^{-1}+y)(1+y^{-1})][w_3w_2^*+w_5w_4^*].$$

Por la cuarta expresión de la hipótesis, se puede escribir

$$x^{-1}(1+x)^2(1+y^{-1})(1+y)w_1^*w_1-[(1+x)(x^{-1}+y)(1+y^{-1})]w_1^*w_1,$$

y a su vez

$$[x^{-1}(1+x)(1+y)-(x^{-1}+y)](1+y^{-1})(1+x)w_1^*w_1.$$

Puesto que $x^{-1}(1+x)(1+y)=(1+x^{-1})(1+y)=1+y+x^{-1}+x^{-1}y$, la expresión anterior se puede expresar ahora como

$$(1+x^{-1}y)(1+y^{-1})(1+x)w_1^*w_1.$$

Así, con la reducción anterior, la reducción hecha de (4.4) a (4.5) y el hecho de que $w_7^*w_7=1$, se puede escribir α como

$$\begin{aligned}\alpha &= (1+x^{-1}y)(1+y^{-1})(1+x)w_1^*w_1\\ &-(1+x)^2(x^{-1}+y^{-1})(x^{-1}+y)w_2w_2^*-(1+x)(x^{-1}+y^{-1})(1+y)w_2w_3^*\\ &-(1+y^{-1})^2(x+y)(x^{-1}+y)w_4w_4^*-(1+y^{-1})(x+y)(1+x^{-1})w_4w_5^*\\ &+(4+x+x^{-1}+y+y^{-1})(x+x^{-1}+y+y^{-1})w_6^*w_6+1.\end{aligned}$$

Ahora, para la expresión

$$(1+x^{-1}y)(1+y^{-1})(1+x)w_1^*w_1-(1+x)(x^{-1}+y^{-1})(1+y)w_2w_3^*-(1+y^{-1})(x+y)(1+x^{-1})w_4w_5^*,$$

ya que se cumplen las siguientes relaciones:

$$\begin{aligned}(1+x)(x^{-1}+y^{-1})(1+y)&=(1+x)(x^{-1}+y^{-1})y(1+y^{-1})=(1+x)(yx^{-1}+1)(1+y^{-1}),\\ (1+y^{-1})(x+y)(1+x^{-1})&=(1+y^{-1})(x+y)x^{-1}(1+x)=(1+y^{-1})(1+x^{-1}y)(1+x),\end{aligned}$$

entonces la expresión se puede escribir de la siguiente forma.

$$(1+x^{-1}y)(1+y^{-1})(1+x)w_1^*w_1-[(1+y^{-1})(1+x^{-1}y)(1+x)][w_2w_3^*+w_4w_5^**].$$

Factorizamos para obtener

$$[(1+y^{-1})(1+x^{-1}y)(1+x)][w_1^*w_1-w_2w_3^*-w_4w_5^**].$$

De la cuarta relación de la hipótesis se tiene también

$$w_1^*w_1=(w_1^*w_1)_z=(w_2^*w_3+w_4^*w_5)_z=(w_2^*)_z(w_3)_z+(w_4^*)_z(w_5)_z=w_2w_3^*+w_4w_5^*,$$

por lo que así,

$$[(1+y^{-1})(1+x^{-1}y)(1+x)][w_1^*w_1 - w_2w_3^* - w_4w_5^**] = 0.$$

Con lo cual, α se puede expresar como

$$\begin{aligned}\alpha = &-(1+x)^2(x^{-1}+y^{-1})(x^{-1}+y)w_2w_2^* \\ &-(1+y^{-1})^2(x+y)(x^{-1}+y)w_4w_4^* \\ &+(4+x+x^{-1}+y+y^{-1})(x+x^{-1}+y+y^{-1})w_6^*w_6+1.\end{aligned}$$

Usando las relaciones $x^{-1}+y^{-1} = x^{-1}(1+xy^{-1})$ y $x+y = y(1+xy^{-1})$ y $w_2w_2^* = w_4w_4^*$, obtenemos

$$\begin{aligned}\alpha = &-[x^{-1}(1+x)^2 + y(1+y^{-1})^2](1+xy^{-1})(x^{-1}+y)w_2w_2^* \\ &+(4+x+x^{-1}+y+y^{-1})(x+x^{-1}+y+y^{-1})w_6^*w_6+1.\end{aligned}$$

Además, usando las siguientes relaciones:

$$\begin{aligned}x^{-1}(1+x)^2 + y(1+y^{-1})^2 &= (1+x^{-1})(1+x)+(1+y)(1+y^{-1}) = 2+x+x^{-1}+2+y+y^{-1}, \\ (1+xy^{-1})(x^{-1}+y) &= x^{-1}+y+y^{-1}+x,\end{aligned}$$

se puede reescribir α de la siguiente forma.

$$\begin{aligned}\alpha = &-(4+x+x^{-1}+y+y^{-1})(x+x^{-1}+y+y^{-1})w_2w_2^* \\ &+(4+x+x^{-1}+y+y^{-1})(x+x^{-1}+y+y^{-1})w_6^*w_6+1.\end{aligned}$$

Puesto que $w_2w_2^* = w_6w_6^*$, entonces, $\alpha = 0+1 = 1$, obteniendo lo deseado.

$$\mathbf{p'q + q'p_{yz} + x^{-1}z^{-1}r's_{xz} + y^{-1}s'r_{xy} = 0}$$

Se toma $\beta = p'q + q'p_{yz} + x^{-1}z^{-1}r's_{xz} + y^{-1}s'r_{xy}$. Entonces

$$\begin{aligned}\beta &= p'q + q'p_{yz} + x^{-1}z^{-1}r's_{xz} + y^{-1}s'r_{xy} \\ &= (x^{-1}p_{yz})q + (-x^{-1}q)p_{yz} + x^{-1}z^{-1}(-y^{-1}r)s_{xz} + y^{-1}(z^{-1}s_z)r_{xy} \\ &= -x^{-1}z^{-1}y^{-1}rs_{xz} + y^{-1}z^{-1}s_zr_{xy}.\end{aligned}$$

Ahora bien, por la forma de s, se cumple $s_{xy} = s_x = s_y = s$. En particular, $s_{xz} = s_z$ y además,

$$\begin{aligned}r_{xy} &= (1+y)(x^{-1}+y^{-1})w_4 + (1+x^{-1})w_5 = (1+y)x^{-1}y^{-1}(x+y)w_4 + x^{-1}(1+x)w_5 \\ &= (1+y^{-1})x^{-1}(x+y)w_4 + x^{-1}(1+x)w_5 = x^{-1}[(1+y^{-1})(x+y)w_4 + (1+x)w_5] = x^{-1}r,\end{aligned}$$

por lo que reescribiendo, obtenemos

$$\beta = -x^{-1}z^{-1}y^{-1}rs_{xz} + y^{-1}z^{-1}s_zr_{xy} = -x^{-1}z^{-1}y^{-1}rs_z + y^{-1}z^{-1}x^{-1}s_zr = 0.$$

$$\mathbf{p'r + xq's_{yz} + r'p_{xz} + y^{-1}zs'q_{xy} = 0}$$

Tomando $\gamma = p'r + xq's_{yz} + r'p_{xz} + y^{-1}zs'q_{xy}$, se tiene

$$\begin{aligned}\gamma &= p'r + xq's_{yz} + r'p_{xz} + y^{-1}zs'q_{xy}\\ &= (x^{-1}p_{yz})r + x(-x^{-1}q)s_{yz} + (-y^{-1}r)p_{xz} + y^{-1}z(z^{-1}s_z)q_{xy}\\ &= x^{-1}p_{yz}r - qs_{yz} - y^{-1}rp_{xz} + y^{-1}s_zq_{xy}.\end{aligned}$$

Ahora bien, por la relación

$$p_{yz} = (1+x)(1+y^{-1})w_1^* = xy^{-1}(1+x^{-1})(1+y)w_1^* = xy^{-1}p_{xz},$$

se puede escribir γ de la siguiente forma:

$$\begin{aligned}\gamma &= x^{-1}p_{yz}r - qs_{yz} - y^{-1}rp_{xz} + y^{-1}s_zq_{xy}\\ &= x^{-1}(xy^{-1}p_{xz})r - qs_{yz} - y^{-1}rp_{xz} + y^{-1}s_zq_{xy}\\ &= y^{-1}p_{xz}r - qs_{yz} - y^{-1}rp_{xz} + y^{-1}s_zq_{xy} = -qs_{yz} + y^{-1}s_zq_{xy}.\end{aligned}$$

También se tiene lo siguiente:

$$\begin{aligned}q_{xy} &= (1+x^{-1})(x+y)w_2 + (1+y)w_3 = (1+x^{-1})xy(x^{-1}+y^{-1})w_2 + y(1+y^{-1})w_3\\ &= y(1+x)(x^{-1}+y^{-1})w_2 + y(1+y^{-1})w_3 = y[(1+x)(x^{-1}+y^{-1})w_2 + (1+y^{-1})w_3] = yq.\end{aligned}$$

Además, como se dijo antes, $s_{yz} = s_z$, luego

$$\gamma = -qs_{yz} + y^{-1}s_zq_{xy} = -qs_z + y^{-1}s_z(yq) = -qs_z + s_zq = 0.$$

$$\mathbf{p's + q'r_{yz} + x^{-1}yz^{-1}r'q_{xz} + s'p_{xy} = 0}$$

Tomando $\delta = p's + q'r_{yz} + x^{-1}yz^{-1}r'q_{xz} + s'p_{xy}$, reescribimos

$$\begin{aligned}\delta =& p's + q'r_{yz} + x^{-1}yz^{-1}r'q_{xz} + s'p_{xy}\\ =& (x^{-1}p_{yz})s + (-x^{-1}q)r_{yz} + x^{-1}yz^{-1}(-y^{-1}r)q_{xz} + (z^{-1}s_z)p_{xy}\\ =& x^{-1}[(1+x)(1+y^{-1})w_1^*][(4+x+x^{-1}+y+y^{-1})w_6 + w_7]\\ &- x^{-1}[(1+x)(x^{-1}+y^{-1})w_2 + (1+y^{-1})w_3][(1+y)(x+y^{-1})w_4^* + (1+x)w_5^*]\\ &- x^{-1}z^{-1}[(1+y^{-1})(x+y)w_4 + (1+x)w_5][(1+x^{-1})(x+y^{-1})w_2^* + (1+y^{-1})w_3^*]\\ &+ z^{-1}[(4+x+x^{-1}+y+y^{-1})w_6^* + w_7^*][(1+x^{-1})(1+y^{-1})w_1].\end{aligned}$$

Desarrollando los sumandos, se obtiene

$$\begin{aligned}\delta =& x^{-1}(1+x)(1+y^{-1})(4+x+x^{-1}+y+y^{-1})w_1^*w_6 + x^{-1}(1+x)(1+y^{-1})w_1^*w_7\\ &- x^{-1}(1+x)(x^{-1}+y^{-1})(1+y)(x+y^{-1})w_2w_4^* - x^{-1}(1+x)(x^{-1}+y^{-1})(1+x)w_2w_5^*\\ &- x^{-1}(1+y^{-1})(1+y)(x+y^{-1})w_3w_4^* - x^{-1}(1+y^{-1})(1+x)w_3w_5^*\\ &- x^{-1}z^{-1}(1+y^{-1})(x+y)(1+x^{-1})(x+y^{-1})w_4w_2^* - x^{-1}z^{-1}(1+y^{-1})(x+y)(1+y^{-1})w_4w_3^*\\ &- x^{-1}z^{-1}(1+x)(1+x^{-1})(x+y^{-1})w_5w_2^* - x^{-1}z^{-1}(1+x)(1+y^{-1})w_5w_3^*\\ &+ z^{-1}(4+x+x^{-1}+y+y^{-1})(1+x^{-1})(1+y^{-1})w_6^*w_1 + z^{-1}(1+x^{-1})(1+y^{-1})w_7^*w_1.\end{aligned}$$

Por la quinta relación de la hipótesis, $w_2^* w_5 = z w_5^* w_2 = w_3^* w_4 = z w_4^* w_3$ y ya que

$$(1+x)(x^{-1}+y^{-1})(1+x) = (1+x^{-1})(1+xy^{-1})(1+x),$$
$$(1+y^{-1})(x+y)(1+y^{-1}) = (1+y)(1+xy^{-1})(1+y^{-1}),$$

entonces la expresión

$$\begin{aligned} &- x^{-1}(1+x)(x^{-1}+y^{-1})(1+x)w_2w_5^* - x^{-1}z^{-1}(1+x)(1+x^{-1})(x+y^{-1})w_5w_2^* \\ &- x^{-1}(1+y^{-1})(1+y)(x+y^{-1})w_3w_4^* - x^{-1}z^{-1}(1+y^{-1})(x+y)(1+y^{-1})w_4w_3^* \end{aligned}$$

se puede expresar de la siguiente forma:

$$\begin{aligned} &- x^{-1}z^{-1}[(1+x^{-1})(1+x)+(1+y)(1+y^{-1})](1+xy^{-1})w_2^*w_5 \\ &- x^{-1}z^{-1}[(1+x)(1+x^{-1})+(1+y^{-1})(1+y)](x+y^{-1})w_2^*w_5, \end{aligned}$$

W su vez, factorizando en la expresión anterior y ya que $(1+x^{-1})(1+x)+(1+y)(1+y^{-1}) = 4+x+x^{-1}+y+y^{-1}$, entonces la podemos reescribir

$$\begin{aligned} &- x^{-1}z^{-1}[(1+xy^{-1})+(x+y^{-1})](4+x+x^{-1}+y+y^{-1})w_2^*w_5 \\ =&- z^{-1}[1+x^{-1}+y^{-1}+x^{-1}y^{-1}](4+x+x^{-1}+y+y^{-1})w_2^*w_5 \end{aligned}$$

o bien,

$$-z^{-1}(1+x^{-1})(1+y^{-1})(4+x+x^{-1}+y+y^{-1})w_2^*w_5. \tag{4.6}$$

Ahora bien, la expresión

$$-x^{-1}(1+x)(x^{-1}+y^{-1})(1+y)(x+y^{-1})w_2w_4^* - x^{-1}z^{-1}(1+y^{-1})(x+y)(1+x^{-1})(x+y^{-1})w_4w_2^*$$

se puede desarrollar de la siguiente manera

$$\begin{aligned} &- (1+x^{-1})(x^{-1}+y^{-1})(1+y)(x+y^{-1})w_2w_4^* - z^{-1}(1+y^{-1})(1+x^{-1}y)(1+x^{-1})(x+y^{-1})w_4w_2^* \\ =&- [(x^{-1}+y^{-1})(1+y)y^{-1}(xy+1)w_2w_4^* + z^{-1}(1+y^{-1})(1+x^{-1}y)(x+y^{-1})w_4w_2^*](1+x^{-1}) \\ =&- z^{-1}[(x^{-1}+y^{-1})(xy+1)zw_2w_4^* + (1+x^{-1}y)(x+y^{-1})w_4w_2^*](1+y^{-1})(1+x^{-1}) \\ =&- z^{-1}[(x+x^{-1}+y+y^{-1})zw_2w_4^* + (x+x^{-1}+y+y^{-1})w_4w_2^*](1+y^{-1})(1+x^{-1}) \\ =&- z^{-1}(x+x^{-1}+y+y^{-1})(1+y^{-1})(1+x^{-1})[zw_2w_4^* + w_4w_2^*]. \end{aligned}$$

Por lo tanto, la suma

$$\begin{aligned} &x^{-1}(1+x)(1+y^{-1})(4+x+x^{-1}+y+y^{-1})w_1^*w_6 \\ &+ z^{-1}(4+x+x^{-1}+y+y^{-1})(1+x^{-1})(1+y^{-1})w_6^*w_1 \\ &- x^{-1}(1+x)(x^{-1}+y^{-1})(1+y)(x+y^{-1})w_2w_4^* \\ &- x^{-1}z^{-1}(1+y^{-1})(x+y)(1+x^{-1})(x+y^{-1})w_4w_2^*, \end{aligned}$$

puede ser escrita como

$$\begin{aligned}
&z^{-1}(1+x^{-1})(1+y^{-1})(4+x+x^{-1}+y+y^{-1})zw_1^*w_6\\
&+z^{-1}(4+x+x^{-1}+y+y^{-1})(1+x^{-1})(1+y^{-1})w_6^*w_1\\
&-z^{-1}(x+x^{-1}+y+y^{-1})(1+y^{-1})(1+x^{-1})[zw_2w_4^*+w_4w_2^*],
\end{aligned}$$

Factorizando, obtenemos

$$\begin{aligned}
&z^{-1}(1+x^{-1})(1+y^{-1})(4+x+x^{-1}+y+y^{-1})[zw_1^*w_6+w_6^*w_1-zw_2w_4^*-w_4w_2^*]\\
&+4z^{-1}(1+x^{-1})(1+y^{-1})[zw_2w_4^*+w_4w_2^*],
\end{aligned}$$

Usando esto junto a lo anterior y la reducción hecha en (4.6), se puede escribir

$$\begin{aligned}
&x^{-1}(1+x)(1+y^{-1})(4+x+x^{-1}+y+y^{-1})w_1^*w_6-x^{-1}(1+x)(x^{-1}+y^{-1})(1+y)(x+y^{-1})w_2w_4^*\\
&-x^{-1}(1+x)(x^{-1}+y^{-1})(1+x)w_2w_5^*-x^{-1}(1+y^{-1})(1+y)(x+y^{-1})w_3w_4^*\\
&-x^{-1}z^{-1}(1+y^{-1})(x+y)(1+x^{-1})(x+y^{-1})w_4w_2^*-x^{-1}z^{-1}(1+y^{-1})(x+y)(1+y^{-1})w_4w_3^*\\
&-x^{-1}z^{-1}(1+x)(1+x^{-1})(x+y^{-1})w_5w_2^*+z^{-1}(4+x+x^{-1}+y+y^{-1})(1+x^{-1})(1+y^{-1})w_6^*w_1
\end{aligned}$$

como

$$\begin{aligned}
&-z^{-1}(1+x^{-1})(1+y^{-1})(4+x+x^{-1}+y+y^{-1})w_2^*w_5\\
&+z^{-1}(1+x^{-1})(1+y^{-1})(4+x+x^{-1}+y+y^{-1})[zw_1^*w_6+w_6^*w_1-zw_2w_4^*-w_4w_2^*]\\
&+4z^{-1}(1+x^{-1})(1+y^{-1})[zw_2w_4^*+w_4w_2^*].
\end{aligned}$$

Por la quinta relación de la hipótesis, el primer y segundo renglón se anulan y la expresión se puede escribir entonces como $4z^{-1}(1+x^{-1})(1+y^{-1})[zw_2w_4^*+w_4w_2^*]$. Reescribiendo δ después de esta reducción, se tiene

$$\begin{aligned}
\delta=&4z^{-1}(1+x^{-1})(1+y^{-1})[zw_2w_4^*+w_4w_2^*]\\
&+x^{-1}(1+x)(1+y^{-1})w_1^*w_7-x^{-1}(1+y^{-1})(1+x)w_3w_5^*\\
&-x^{-1}z^{-1}(1+x)(1+y^{-1})w_5w_3^*+z^{-1}(1+x^{-1})(1+y^{-1})w_7^*w_1,
\end{aligned}$$

o bien

$$\begin{aligned}
\delta=&z^{-1}(1+x^{-1})(1+y^{-1})[4(zw_2w_4^*+w_4w_2^*)]\\
&+z^{-1}(1+x^{-1})(1+y^{-1})zw_1^*w_7-z^{-1}(1+y^{-1})(1+x^{-1})zw_3w_5^*\\
&-z^{-1}(1+x^{-1})(1+y^{-1})w_5w_3^*+z^{-1}(1+x^{-1})(1+y^{-1})w_7^*w_1,\\
=&z^{-1}(1+x^{-1})(1+y^{-1})[4(zw_2w_4^*+w_4w_2^*)+zw_1^*w_7-zw_3w_5^*-w_5w_3^*+w_7^*w_1],
\end{aligned}$$

que se anula por la sexta relación de la hipótesis. □

Después del anterior resultado, lo único que resta para encontrar una unidad en KP_1 es dar una familia de siete elementos en $K\langle z\rangle$ que satisfagan las relaciones de la proposición anterior. Murray hace precisamente este proceso en [23] para encontrar estos elementos de $K\langle z\rangle$ resolviendo simplemente el sistema de ecuaciones. Aunque Murray se encuentra con una dificultad cuando la característica del anillo es cero, es capaz de dar una familia de ejemplos para cada característica positiva. Los elementos encontrados por Murray se enlistan en la siguiente proposición.

Proposición 4.1.4. *Sean $m, n \in \mathbb{Z}$ y sea K un campo de característica positiva d. Consideremos los elementos $w_1, w_2, w_3, w_4, w_5, w_6, w_7 \in K\langle z\rangle$ dados por*

$$\begin{aligned}
w_1 &= (z^m + z^{1-m})(1 - z^{1-2m})^{d-2},\\
w_2 &= z^n(1 - z^{1-2m})^{d-2},\\
w_3 &= z^n(1 + z^{2m-1})(1 - z^{1-2m})^{d-2},\\
w_4 &= z^{m+n}(1 - z^{1-2m})^{d-2},\\
w_5 &= z^n(z^m + z^{1-m})(1 - z^{1-2m})^{d-2},\\
w_6 &= (1 - z^{1-2m})^{d-2},\\
w_7 &= z^{2m-1}.
\end{aligned}$$

Entonces $w_1, w_2, w_3, w_4, w_5, w_6, w_7$ satisfacen las relaciones de las proposición anterior. Es decir, se cumplen las siguientes igualdades.

$$\begin{aligned}
w_7^* w_7 &= 1,\\
w_3^* w_3 &= w_5^* w_5 = w_7^* w_6 + w_6^* w_7 + 4w_6^* w_6,\\
w_2^* w_2 &= w_4^* w_4 = w_6^* w_6,\\
w_1^* w_1 &= w_2^* w_3 + w_4^* w_5,\\
w_2^* w_5 &= z w_5^* w_2 = w_3^* w_4 = z w_4^* w_3 = w_6^* w_1 + z w_1^* w_6 - (w_2^* w_4 + z w_4^* w_2),\\
w_3^* w_5 + z w_5 * w_3 &= w_7^* w_1 + z w_1^* w_7 + 4(w_2^* w_4 + z w_4^* w_2).
\end{aligned}$$

Demostración. La primera relación se cumple, pues $w_7^* w_7 = (z^{2m-1})(z^{-2m+1}) = 1$. Particularmente, por la forma de los elementos se tienen las siguientes relaciones.

$$\begin{aligned}
w_1 &= (z^m + z^{1-m})w_6,\\
w_2 &= z^n w_6,\\
w_3 &= z^n(1 + z^{2m-1})w_6,\\
w_4 &= z^{m+n} w_6,\\
w_5 &= z^n(z^m + z^{1-m})w_6.
\end{aligned}$$

A su vez, ya que $z^{m-1}(z^m + z^{1-m}) = z^{2m-1} + 1$, entonces $z^{m-1} w_5 = w_3$. Así,

$$w_3^* w_3 = (z^{1-m} w_5^*)(z^{m-1} w_5) = w_5^* w_5.$$

Ahora bien, desarrollando obtenemos

$$\begin{aligned}
w_3^* w_3 &= [z^{-n}(1 + z^{-2m+1})w_6^*][z^n(1 + z^{2m-1})w_6]\\
&= (1 + z^{-2m+1})(1 + z^{2m-1})w_6^* w_6\\
&= (2 + z^{-2m+1} + z^{2m-1})w_6^* w_6\\
&= (z^{-2m+1} + z^{2m-1} - 2)w_6^* w_6 + 4w_6^* w_6. \qquad (4.7)
\end{aligned}$$

Además se tiene lo siguiente.

$$\begin{aligned}(z^{-2m+1}+z^{2m-1}-2)w_6^*w_6 &= -(1-z^{-2m+1})w_6^*w_6-(1-z^{2m-1})w_6^*w_6\\ &= -(1-z^{-2m+1})(1-z^{1-2m})^{d-2}w_6^*-(1-z^{2m-1})(1-z^{-1+2m})^{d-2}w_6\\ &= -(1-z^{1-2m})^{d-1}w_6^*-(1-z^{-1+2m})^{d-1}w_6\\ &= -(-z^{1-2m})^{d-1}(1-z^{-1+2m})^{d-1}w_6^*-(1-z^{-1+2m})^{d-1}w_6\\ &= [-(-z^{1-2m})^{d-1}w_6^*-w_6](1-z^{-1+2m})^{d-1}\\ &= [-(-z^{1-2m})(-z^{1-2m})^{d-2}(1-z^{-1+2m})^{d-2}-w_6](1-z^{-1+2m})^{d-1}\\ &= [z^{1-2m}(1-z^{1-2m})^{d-2}-w_6](1-z^{-1+2m})^{d-1}\\ &= [z^{1-2m}w_6-w_6](1-z^{-1+2m})^{d-1}\\ &= z^{1-2m}[1-z^{-1+2m}](1-z^{-1+2m})^{d-1}w_6\\ &= z^{1-2m}(1-z^{-1+2m})^{d}w_6,\end{aligned}$$

Ya que K es un campo de característica un primo d, entonces $K\langle z\rangle$ también lo es. Por lo tanto, $(1-z^{-1+2m})^d = 1-z^{d(-1+2m)}$ y lo anterior se puede reescribir de la siguiente forma.

$$\begin{aligned}(z^{-2m+1}+z^{2m-1}-2)w_6^*w_6 &= z^{1-2m}(1-z^{-1+2m})^{d}w_6\\ &= z^{1-2m}(1+(-1)^dz^{d(-1+2m)})w_6\\ &= (z^{1-2m}+(-1)^dz^{(d-1)(-1+2m)})w_6\\ &= w_7^*w_6+(-1)^dz^{(d-1)(-1+2m)}w_6. \qquad (4.8)\end{aligned}$$

También se obtiene la siguiente relación:

$$\begin{aligned}(-1)^dz^{(d-1)(-1+2m)}w_6 &= (-1)^dz^{(d-1)(-1+2m)}(1-z^{1-2m})^{d-2}\\ &= (-1)^2z^{1-2m}(-z^{-1+2m})^{d-2}(1-z^{1-2m})^{d-2}\\ &= z^{1-2m}(1-z^{-1+2m})^{d-2}\\ &= w_7^*w_6.\end{aligned}$$

Así, combinando lo anterior con (4.8) y (4.7) se obtiene

$$w_3^*w_3 = (z^{-2m+1}+z^{2m-1}-2)w_6^*w_6+4w_6^*w_6 = w_7^*w_6+w_7^*w_6+4w_6^*w_6,$$

por lo que entonces se cumple la segunda relación. La tercera relación se cumple de acuerdo a lo siguiente:

$$w_2^*w_2 = (z^{-n}w_6^*)(z^nw_6)w_6^*w_6 = w_6^*w_6 = z^{-m-n}z^{m+n}w_6^*w_6 = w_4^*w_4.$$

También se puede comprobar que

$$\begin{aligned}w_2^*w_3+w_4^*w_5 &= (z^{-n}w_6^*)(z^n(1+z^{2m-1})w_6)+(z^{-m-n}w_6^*)(z^n(z^m+z^{1-m})w_6)\\ &= (1+z^{2m-1})w_6^*w_6+z^{-m}(z^m+z^{1-m})w_6^*w_6\\ &= z^{m-1}(z^{1-m}+z^m)w_6^*w_6+z^{-m}(z^m+z^{1-m})w_6^*w_6\\ &= (z^{m-1}+z^{-m})(z^{1-m}+z^m)w_6^*w_6\\ &= w_1^*w_1,\end{aligned}$$

cumpliéndose entonces la cuarta relación. Para la quinta relación, se observa que se satisface

$$\begin{aligned} zw_5^*w_2 &= z(z^{-n}(z^{-m}+z^{-1+m})w_6^*)(z^nw_6) = (z^{-n}w_6^*)(z^n(z^{1-m}+z^m)w_6) = w_2^*w_5, \\ w_3^*w_4 &= (z^{-n}(1+z^{-2m+1})w_6^*)(z^{m+n}w_6) = (z^{-n}w_6^*)(z^n(z^m+z^{-m+1})w_6) = w_2^*w_5, \\ zw_4^*w_3 &= z(z^{-m-n}w_6^*)(z^n(1+z^{2m-1})w_6) = (z^{-n}w_6^*)(z^nz^{-m+1}(1+z^{2m-1})w_6) = w_2^*w_5. \end{aligned}$$

Además se obtiene la siguiente relación:

$$\begin{aligned} w_6^*w_1 + zw_1^*w_6 - (w_2^*w_4 + zw_4^*w_2) &= [(z^m+z^{1-m}) + z(z^{-m}+z^{-1+m}) - (z^{-n}z^{m+n} + zz^{-m-n}z^n)]w_6^*w_6 \\ &= [(z^m+z^{1-m}) + (z^{1-m}+z^m) - (z^m+z^{1-m})]w_6^*w_6 \\ &= [(z^m+z^{1-m})]w_6^*w_6 \\ &= z^{-n}z^nz^{-m+1}(z^{2m-1}+1)w_6^*w_6 \\ &= [z^{-n}w_6^*][z^nz^{-m+1}(1+z^{2m-1})w_6] \\ &= w_2^*w_5. \end{aligned}$$

Para la última relación, se toma $\alpha = w_3^*w_5 + zw_5^*w_3$ y se desarrolla de la siguiente forma.

$$\begin{aligned} \alpha &= [z^{-n}(1+z^{-2m+1})w_6^*][z^n(z^m+z^{1-m})w_6] + z[z^{-n}(z^{-m}+z^{-1+m})w_6^*][z^n(1+z^{2m-1})w_6] \\ &= [(1+z^{-2m+1})(z^m+z^{1-m}) + (z^{1-m}+z^m)(1+z^{2m-1})]w_6^*w_6 \\ &= [1+z^{-2m+1}+1+z^{2m-1}](z^m+z^{1-m})w_6^*w_6 \\ &= (1+z^{-2m+1})(1+z^{2m-1})(z^m+z^{1-m})w_6^*w_6 \\ &= (z^m+z^{1-m})w_3^*w_3. \end{aligned}$$

También se toma $\beta = w_7^*w_1 + zw_1^*w_7 + 4(w_2^*w_4 + zw_4^*w_2)$ y se desarrolla de la siguiente manera.

$$\begin{aligned} \beta &= z^{-2m+1}(z^m+z^{1-m})w_6 + z(z^{-m}+z^{-1+m})w_6^*z^{2m-1} + 4(z^{-n}w_6^*z^{m+n}w_6 + zz^{-m-n}w_6^*z^nw_6) \\ &= (z^m+z^{1-m})(z^{-2m+1}w_6 + z^{2m-1}w_6^*) + 4(z^mw_6^*w_6 + z^{-m+1}w_6^*w_6) \\ &= (z^m+z^{1-m})(z^{-2m+1}w_6 + z^{2m-1}w_6^*) + 4(z^m+z^{1-m})w_6^*w_6 \\ &= (z^m+z^{1-m})(w_7^*w_6 + w_7w_6^* + 4w_6^*w_6). \end{aligned}$$

De acuerdo a la segunda relación, se tiene

$$\begin{aligned} \beta &= (z^m+z^{1-m})(w_7^*w_6 + w_7w_6^* + 4w_6^*w_6) \\ &= (z^m+z^{1-m})w_3^*w_3. \end{aligned}$$

Con los desarrollos anteriores, concluimos $\alpha = \beta$, cumpliéndose así la última relación. □

El resultado anterior al fin abre puertas para una familia de contraejemplos para cada característica prima positiva. Aunque en este caso todas las unidades encontradas presentan similitudes, se puede intuir que hay tantas unidades en los campos KP_1, que posiblemente no siguen un patrón. El resultado principal de esta sección se sigue de la Proposición 4.1.3 y la Proposición 4.1.4.

Teorema 4.1.5. *Sea K un campo de característica positiva d, sean $m, n \in \mathbb{Z}$ y $p, q, r, s \in K\langle x, y, z\rangle$ los elementos definidos de la siguiente forma.*

$$\begin{aligned}
p &= (1+x)(1+y)(z^m + z^{1-m})(1-z^{1-2m})^{d-2},\\
q &= (1+x)(x^{-1}+y^{-1})z^n(1-z^{1-2m})^{d-2} + (1+y^{-1})z^n(1+z^{2m-1})(1-z^{1-2m})^{d-2},\\
r &= (1+y^{-1})(x+y)z^{m+n}(1-z^{1-2m})^{d-2} + (1+x)z^n(z^m+z^{1-m})(1-z^{1-2m})^{d-2},\\
s &= (4+x+x^{-1}+y+y^{-1})(1-z^{1-2m})^{d-2} + z^{2m-1}.
\end{aligned}$$

Entonces, $p + qa + rb + sab$ es una unidad no trivial en KP_1.

Con el anterior teorema, se puede conocer que existen infinitos campos K para los cuales KP_1 tiene unidades no triviales, pero está lejos de abarcar todos los campos. Pero no incluye los campos de característica cero como $\mathbb{R}$ ó $\mathbb{C}$, que suelen ser los más interesantes en trabajos relacionados con implicaciones topológicas. Fue Gardam en [11] quien basándose en las ideas de las unidades antes encontradas encontró un nuevo contraejemplo ahora sobre el campo $\mathbb{C}$.

Proposición 4.1.6. *Sean $p, q, r, s \in \mathbb{C}\langle x, y, z\rangle$ los elementos dados de la siguiente forma.*

$$\begin{aligned}
p &= 1 - ix + iy + xy - (1 + ix - iy + xy)z^{-1},\\
q &= x^{-1}y^{-1} - ix + iy^{-1}z - z,\\
r &= 1 + ix - iy^{-1}z - xyz,\\
s &= 1 + i(x - x^{-1} - y + y^{-1})z^{-1}.
\end{aligned}$$

Sea también $\omega = e^{\pi i/4}$. Entonces $p + \omega qa + \omega^{-1}rb + sab$ es una unidad no trivial en $\mathbb{C}P_1$.

El elemento inverso que se propone para la unidad anterior se logra usando los siguientes "coeficientes".

$$\begin{aligned}
p' &= ix^{-1} + 1 + x^{-1}y^{-1} - iy - (ix^{-1} + 1 + x^{-1}y^{-1} + iy^{-1})z,\\
q' &= ix^2y^{-1} - 1 + x^{-1}y^{-1}z - ix^{-1}z,\\
r' &= -iy^{-1} - xy^{-1} + y^{-2}z + ixz,\\
s' &= z^{-1} + i(x - x^{-1} - y + y^{-1})z^{-1}.
\end{aligned}$$

Entonces, se comprueba computacionalmente que $(p' + \omega q'a + \omega^{-1}r'b + s'ab)(p + \omega qa + \omega^{-1}rb + sab) = 1$.

4.2 Razonamiento de la Unidad

Los contrajemplos dados por Gardam y Murray en la sección anterior evidencian que la conjetura de la unidad es falsa, pero realmente sigue pareciendo todo muy arbitrario. Tiempo después a los resultados anteriores, hubo trabajo a desarrollar para resolver diversas preguntas sobre los contraejemplos dados. Por ejemplo, sobre determinar cuántas unidades hay en los anillos de grupo KP_1, o cómo encontrar más unidades no triviales.

En un articulo reciente, Bartholdi [2] dio algunos indicios que justificaban ciertos pasos en la elección de las unidades encontradas en la sección anterior. Junto a algunos comentarios más dados por Passman en [25], podían dejar más en claro las aparentemente arbitrarias unidades dadas antes.

Consideremos la función $*\colon KP_1 \to KP_1$ definida de la siguiente forma.

$$r = \sum_{g\in P_1} r_g g \quad \Rightarrow \quad r^* = \sum_{g\in G} r_g g^{-1}.$$

Notemos que se cumplen las siguientes propiedades,

- $(r^*)^* = \left(\left(\sum_{g\in P_1} r_g g\right)^*\right)^* = \left(\sum_{g\in P_1} r_g g^{-1}\right)^* = \sum_{g\in P_1} r_g g = r.$
- $(rs)^* = \left(\sum_{g\in G}\left(\sum_{h\in G} r_h s_g hg\right)\right)^* = \sum_{g\in G}\left(\sum_{h\in G} r_h s_g (hg)^{-1}\right) = \sum_{g\in G}\left(\sum_{h\in G} s_g r_h g^{-1}h^{-1}\right) = s^* r^*.$

A funciones que cumplen las propiedades anteriores, se les suele llamar anti-involuciones y convierten al álgebra KP_1 en algo conocido como una $*$-álgebra (pronunciado "estrella-álgebra"). Consideremos además los homomorfismos $\sigma\colon P_1 \to P_1$ y $\chi\colon P_1 \to \{-1, 1\}$ definidos en los generadores a, b de P_1 de la siguiente forma.

$$\sigma(a) = a, \quad \sigma(b) = b^{-1} \quad \text{y} \quad \chi(a) = \chi(b) = -1.$$

Las funciones σ, χ inducen el homomorfismo $\theta\colon KP_1 \to KP_1$ dado por

$$\theta\left(\sum_{g\in P_1} r_g g\right) = \sum_{g\in P_1} \chi(g) r_g \sigma(g).$$

Por la definición de σ, se cumple $\sigma(\sigma(g)) = g$ para cada $g \in P_1$, por lo que se puede verificar lo siguiente,

$$\theta\left(\theta\left(\sum_{g\in P_1} r_g g\right)\right) = \theta\left(\sum_{g\in P_1} \chi(g) r_g \sigma(g)\right) = \sum_{g\in P_1} \chi(\sigma(g))\chi(g) r_g \sigma(\sigma(g)) = \sum_{g\in P_1} \chi(\sigma(g))\chi(g) r_g g.$$

Recordemos ahora la función de longitud definida en la Sección 1.3 para productos amalgamados (como es el caso de P_1 visto en la Sección 3.4). Se puede observar que en realidad $\chi(g) = (-1)^{\text{long}(g)}$ y que $\text{long}(\sigma(g)) = \text{long}(g)$, por lo que $\chi(\sigma(g))\chi(g) = (-1)^{2\text{long}(g)} = 1$. Así,

$$\theta\left(\theta\left(\sum_{g\in P_1} r_g g\right)\right) = \sum_{g\in P_1} \chi(\sigma(g))\chi(g) r_g g = \sum_{g\in P_1} r_g g.$$

Como σ es un homomorfismo, $\sigma(g^{-1}) = (\sigma(g))^{-1}$ y por lo tanto, $\theta(r^*) = (\theta(r))^*$ para cada $r \in KP_1$. Esto significa, de acuerdo a lo siguiente, que $\theta \circ *$ es una anti-involución.

- $\theta((\theta(r^*))^*) = \theta(\theta((r^*)^*)) = \theta(\theta(r)) = r.$
- $\theta((rs)^*) = \theta(s^* r^*) = \theta(s^*)\theta(r^*).$

Así, un elemento $u \in KP_1$ se llamará θ-unitario si $u\theta(u^*) = 1$. Tomemos un elemento $u = p + qa + rb + sab$ con $p, q, r, s \in K\langle x, y, z\rangle$. Se puede ver, ya que $K\langle x, y, z\rangle$ es conmutativo, que se tiene

$$u^* = p_{xyz} + a^{-1}q_{xyz} + b^{-1}r_{xyz} + (ab)^{-1}s_{xyz}.$$

Ahora, lo anterior, de acuerdo a las relaciones (4.3), se puede reescribir de la siguiente forma:

$$\begin{aligned} u^* &= p_{xyz} + a^{-1}q_{xyz} + b^{-1}r_{xyz} + (ab)^{-1}s_{xyz} \\ &= p_{xyz} + x^{-1}aq_{xyz} + y^{-1}br_{xyz} + z^{-1}(ab)s_{xyz} \\ &= p_{xyz} + x^{-1}(q_{xyz})_{yz}a + y^{-1}(r_{xyz})_{xz}b + z^{-1}(s_{xyz})_{xy}ab \\ &= p_{xyz} + x^{-1}q_xa + y^{-1}r_yb + z^{-1}s_zab. \end{aligned}$$

Aplicando θ, obtenemos

$$\begin{aligned} \theta(u^*) &= \theta(p_{xyz} + x^{-1}q_xa + y^{-1}r_yb + z^{-1}s_zab) \\ &= \chi(1)(p_{xyz})_y + \chi(a)x^{-1}(q_x)_y\sigma(a) + \chi(b)y(r_y)_y\sigma(b) + \chi(ab)(z^{-1}s_z)_yab^{-1} \\ &= p_{xz} - x^{-1}q_{xy}a - yry^{-1}b + z^{-1}s_{yz}ay^{-1}b \\ &= p_{xz} - x^{-1}q_{xy}a - rb + z^{-1}s_{yz}yab. \end{aligned}$$

Ahora bien, considerando p, q, r, s como en la Proposición 4.1.3, se cumple entonces $s_{yz} = s_z$ y mediante algunos detalles más se observa la relación

$$y^{-1}\theta(u^*) = x^{-1}p_{yz} - x^{-1}y^{-1}q_{xy}a - y^{-1}rb + z^{-1}s_zab.$$

Además, desarrollando,

$$\begin{aligned} y^{-1}q_{xy} &= y^{-1}[(1 + x^{-1})(x + y)w_2 + (1 + y)w_3] \\ &= y^{-1}x^{-1}(1 + x)(x + y)w_2 + (1 + y^{-1})w_3 \\ &= (1 + x)((y^{-1}x^{-1})x + (y^{-1}x^{-1})y)w_2 + (1 + y^{-1})w_3 \\ &= (1 + x)(y^{-1} + x^{-1})w_2 + (1 + y^{-1})w_3 \\ &= q. \end{aligned}$$

Por lo que si p, q, r, s son como en el Teorema 4.1.5 y $u = p+qa+rb+sab$, se tiene $u^{-1} = y^{-1}\theta(u^*)$. Tomando

$v = azub^{-1}$, se tiene

$$\begin{aligned}
\theta(v^*) &= \theta((azub^{-1})^*) \\
&= \theta((b^{-1})^*)\theta(u^*)\theta((z)^*)\theta((a)^*) \\
&= \theta(b)\theta(u^*)\theta((abab)^{-1})\theta(a^{-1}) \\
&= \theta(b)\theta(u^*)\theta(b^{-1}a^{-1}b^{-1}a^{-1})\theta(a^{-1}) \\
&= [\chi(b)\sigma(b)]\theta(u^*)[\chi(b^{-1}a^{-1}b^{-1}a^{-1})\sigma(b^{-1}a^{-1}b^{-1}a^{-1})][\chi(a)\sigma(a^{-1})] \\
&= (-b^{-1})\theta(u^*)(ba^{-1}ba^{-1})(-a^{-1}) \\
&= by^{-1}\theta(u^*)bax^{-1}bx^{-1} \\
&= by^{-1}\theta(u^*)a^{-1}ababxx^{-1} \\
&= by^{-1}\theta(u^*)a^{-1}(abab) \\
&= by^{-1}\theta(u^*)a^{-1}z \\
&= by^{-1}\theta(u^*)z^{-1}a^{-1} \\
&= bu^{-1}z^{-1}a^{-1}.
\end{aligned}$$

Así que $v^{-1} = \theta(v^*)$ y por lo tanto, v es θ-unitario. Con lo cual, para cada unidad encontrada en la sección anterior, se forma un elemento θ-unitario. Una pregunta relevante, ya que se conocen unidades no triviales en el anillo de grupo KP_1 con K de característica positiva, es: ¿Cuántas unidades hay? Lo hecho anteriormente puede ayudar a resolver esta pregunta. Más concretamente, para encontrar los generadores del grupo de unidades. Evidentemente, el grupo P_1 y las unidades θ-unitarias son generadores, ¿pero son todos? Hasta ahora, para los ejemplos conocidos no hay ninguna unidad que no esté generada de esta manera, por lo que esto continúa como una posibilidad. Bartholdi encontró también las siguientes unidades u_1, u_2 en $\mathbb{F}_2P_1$ que también son θ-unitarias.

$$\begin{aligned}
u_1 = {} & xyz^{-1} + x^{-1}z^{-1} + xy^{-1}z^{-1} + y^{-2} + 1 + x^{-2} + yz^{-1} + y^2 + y^{-1}z^{-1} + x^{-1}yz^{-1} + x^{-1}y^{-1}z^{-1} \\
& + xyz + xy^{-1}z + x^2 + xz^{-1} + x^{-1}yz + x^{-1}y^{-1}z \\
& + (y^{-1}z^2 + xz + x^{-1}y^{-1}z^2 + yz^2 + x^{-1}yz^2 + xy + y^2z + y^{-1} + x^{-1}y + x^{-1}y^{-2}z + yz + x^{-1}y^{-1}z \\
& + x^{-2}y^{-1} + 1 + x^{-2}z + x^{-1})a \\
& + (y^{-1}z + x^{-1}y^{-1} + xy^{-1}z + x^{-2}y^{-1} + x^2 + x^{-1}z + z + x^{-1}y^{-1}z^{-1} + x + xyz + xy^{-1}z^{-1} \\
& + x^{-1}z^{-1} + y + x^{-1}y^{-2}z + xz^{-1} + y^{-2})b \\
& + (x^{-1}z^{-2} + yz^{-2} + z^{-2} + x^{-1}yz^{-3} + x^{-1}z^{-3} + yz^{-3} + z^{-3} + x^{-1}yz^{-2})ab.
\end{aligned}$$

$$\begin{aligned}
u_2 = {} & xyz^{-1} + xy^{-1}z^{-1} + y^{-2} + 1 + xy + xz + xy^{-1} + y^2 + y^{-1}z^{-1} + yz^{-1} + x^{-1}yz^{-1} \\
& + x^{-1}y^{-1}z^{-1} + xyz + x^{-1}z + x^{-1}y + xy^{-1}z + x^{-1}y^{-1} + x^{-1}yz + x^{-1}y^{-1}z \\
& + (y^{-2} + xy^{-1} + xz + y^{-1} + z + y + x^{-1}y^{-1} + x^{-1}z + x^{-2}yz + x^{-1}y + xy^{-1}z + z^{-1} + x^{-1}z^{-1} \\
& + yz + x^{-1}y^{-1}z + x^{-2} + y^{-1}z^{-1} + x^{-1}y^{-1}z^{-1} + yz^{-1} + x + x^{-1}yz^{-1} + x^{-2}z + x^{-1}y^2 + x^{-2}y)a \\
& + (xy^{-1}z + x^{-1}z + xz + xy^{-2}z^{-1} + y + x^{-1}yz^{-1} + x^{-1}y^{-1}z + y^{-2})b \\
& + (z^{-1} + xz^{-1} + xyz^{-2} + x^{-2}yz^{-1} + xz^{-2} + x^{-1}yz^{-3} + x^{-2}z^{-1} + x^{-1}yz^{-1} + x^{-2}yz^{-2} \\
& + x^{-1}z^{-3} + yz^{-3} + x^{-1}z^{-1} + yz^{-1} + x^{-2}z^{-2} + z^{-3} + xyz^{-1})ab.
\end{aligned}$$

Recordemos el grupo de Soelberg

$$G = \langle x, y \mid (y^2x)^2 = x^2, (x^2y)^2 = y^{-2} \rangle \cong \langle x, y \mid xy^2x^{-1} = y^{-2}, yx^2y^3 = x^{-2} \rangle,$$

visto en la Sección 3.4. Este grupo es interesante pues da otro ejemplo sencillo de un grupo que no satisface la propiedad de producto único. Fue el mismo Gardam en [11] que dio con una unidad no trivial en este grupo. Lo interesante es que se puede analizar con métodos similares a los vistos antes. Si $\phi\colon G \to G$ es el homomorfismo definido en generadores por $\phi(x) = xy^{-1}$ y $\phi(y) = x^2y^{-1}$, entonces Gardam prueba computacionalmente el siguiente resultado.

Proposición 4.2.1. *Sea $v \in \mathbb{F}_2G$ el elemento*

$$\begin{aligned} v = {} & x + x^{-1} + xy^{-1} + yx^{-1} + x^2y^{-1} + x^{-1}yx^{-1} + xy^{-1}x^{-1} + (xy^{-1})^2 + y + (yx^{-1})^2 \\ & + x^3y^{-1} + xy + x(yx^{-1})^2 + x^{-2}yx^{-1} + y^{-1}x^{-1} + y^{-1}xy^{-1} + xy^{-1}x^2y^{-1} + yx^{-2}yx^{-1} \\ & + x^2y + x^2y^{-1}x^2 + x^{-1}y^{-1}x^{-1} + x^{-1}yx^{-3} + xy^{-1}x^{-2}yx^{-1} + yx^2y^{-1} \\ & + x^3y^{-1}x^2 + xyx^2y^{-1} + x^{-2}yx^{-3} + y^{-1}x^{-2}yx^{-1} + x^2yx^2y^{-1}. \end{aligned}$$

Entonces v es un elemento ϕ-unitario.

Otra observación relevante en las unidades vistas antes y en general en el anillo de grupo KP_1, es que existe una representación del grupo en matrices 4×4 sobre $K\langle x, y, z \rangle$. Tomemos

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ x & 0 & 0 & 0 \\ 0 & 0 & 0 & x^{-1}z^{-1} \\ 0 & 0 & y^{-1}z & 0 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ y & 0 & 0 & 0 \\ 0 & y^{-1} & 0 & 0 \end{pmatrix}.$$

Simplemente se representa $a \mapsto A$ y $b \mapsto B$. Por supuesto, esta representación envía $x \mapsto A^2, y \mapsto B^2$ y $z \mapsto ABAB$. En [7] se muestra un resultado relevante en la estructura de esta representación, pues se prueba que si U es una unidad en esta representación, entonces $\det U \in K$. Hablando específicamente de las unidades propuestas por Gardam y Murray, en [25] se muestra que de hecho las unidades planteadas satisfacen $\det U = 1$.

5 Discusión

En este trabajo se dan a conocer las conjeturas de Kaplansky en anillos de grupo y se da un amplio panorama acerca de los avances actuales, pero esto es solo una pequeña fracción de todo el trabajo realizado. En este capítulo se presentan algunos resultados adicionales a los que se expusieron sin entrar mucho en detalle en cada caso y para dar pauta a un posible trabajo futuro, pues sigue habiendo muchas cuestiones sin resolver en las conjeturas de Kaplansky.

5.1 Progreso Adicional

El propósito de esta sección es dar a conocer algunos resultados extra que se han realizado para la resolución de las conjeturas, aunque sin adentrarse mucho en cada resultado. Por ejemplo, en [33] se demuestra un teorema acerca de la longitud definida para un elemento en un anillo de grupo. Si $r \in KG$, se define $\text{lon}(r) = |\mathbf{sop}(r)|$.

Teorema 5.1.1. *Si G es un grupo libre de torsión y $\alpha, \beta \in \mathbb{Q}G\backslash\{0\}$, con lon$(\alpha) = n$, lon$(\beta) = m$, son tales que $\alpha\beta = 0$, entonces se cumplen las siguientes condiciones:*

a) $n > 2$,

b) $m > 2$,

c) $n > 3$ *ó* $m > 16$,

d) $n > 16$ *ó* $m > 3$,

e) $n > 4$ *ó* $m > 7$,

f) $n > 7$ *ó* $m > 4$.

Entre otros resultados interesantes sobre la conjetura, se encuentran algunos para verificar si un grupo satisface la propiedad de producto único. Por ejemplo, Litchman en [20] introduce la siguiente condición para subgrupos. Para un grupo G y $H \leq G$, se dice que G es inerte sobre H si para cada par de subconjuntos A, B de G tales que existe $g \in AB$ con $g \notin H$, existe $x \notin H$ tal que $n_{A\cdot B}(x) = 1$. A través de esta condición, Litchman demuestra que si G y H son grupos con producto único inertes sobre algún subgrupo común K, entonces, $G *_K H$ es un grupo con producto único. Más tarde, Farbman en [9] generaliza el resultado de Litchman introduciendo una propiedad más compleja, a la cual llama condición vnn.

En la Sección 3.4 se dieron algunos ejemplos de grupos que no satisfacen la propiedad de producto único, pero actualmente se conocen bastantes ejemplos. En [24] se analizan diversos grupos que no satisfacen la propiedad de producto único, con una forma ingeniosa de buscarlos. No solo eso, pues se dan cardinalidades mínimas que dos conjuntos en un grupo deben satisfacer para poder ser considerados en la búsqueda de no productos únicos.

Teorema 5.1.2. *Sea G un grupo libre de torsión y A, B subconjuntos finitos de G. Si $n_{A\cdot B}(g) \neq 1$ para cada $g \in G$, entonces, $|A| + |B| \geq 16$.*

Más aún, si se toma

$$Y = \{(1,1,2,2),(1,2,3,3),(1,3,4,2),(1,4,3,2),(1,5,3,6),\\ (1,7,3,8),(2,1,5,8),(2,3,8,7),(2,4,5,6),(2,5,5,1)\},$$

entonces el grupo definido por la siguiente presentación no tiene producto único y es libre de torsión.

$$G_Y = \langle a_1, \ldots, a_8 \mid a_i a_j = a_k a_l \quad \text{si } (i,j,k,l) \in Y \rangle .$$

En este caso, tomando $A = \{a_1, \ldots, a_8\}$, entonces AA no tiene producto único, lo cual hace a G_Y un ejemplo muy interesante, pues de acuerdo al Teorema 5.1.2, el producto AA tiene la cardinalidad mínima posible, es decir, $|A| + |A| = 16$ y además, es un ejemplo de par de conjuntos con esta condición en el que ambos elementos del producto son iguales.

También es importante rescatar, que de hecho, las conjeturas de divisor de cero y elementos idempotentes han sido de relevancia para diferentes problemas topológicos existentes. Por ejemplo, si G es un grupo elementalmente amenable y K es un campo, entonces en [18] se prueba que KG satisface la conjetura de divisor de cero.

Por supuesto, con un enfoque dado por funciones para el anillo de grupo, hay conjeturas relacionadas con el análisis. Recordemos que si R es un anillo y G un grupo, el anillo de grupo puede ser definido también de la siguiente forma.

$$RG = \{r \in R^G \mid |\mathbf{sop}(r)| < \infty\}.$$

Pero hay diversas generalizaciones para el anillo de grupo, por el ejemplo, se puede definir el espacio de Hilbert

$$L^2G = \left\{ r \in \mathbb{C}^G \;\middle|\; \sum_{g\in G} |r(g)|^2 < \infty \right\},$$

con el producto interior

$$\langle r, s \rangle = \sum_{g\in G} \overline{r(g)} s(g).$$

Bajo la anterior perspectiva, $\mathbb{C}G \subseteq L^2G$. También se puede definir el anillo

$$C_cG = \{r \in \mathbb{C}^G \mid r \text{ es continua y } \mathbf{sop}(r) \text{ es compacto}\}.$$

Por supuesto, si G es un grupo con topología discreta, toda función en $\mathbb{C}^G$ es continua y los conjuntos compactos de G son los finitos, por lo que $C_c(G) = \mathbb{C}G$. Las operaciones en los anillos L^2G y C_cG se definen de la misma manera que fueron definidas para el anillo de grupo. Existe un encaje de C_cG en $\mathcal{L}(L^2G)$, el espacio operadores lineales continuos de L^2G. Está dado por $r \mapsto T_r$, donde $T_r(u) = ru$. Bajo todas las anteriores ideas, se define la C^*-álgebra reducida de G como $C_r^*(G) = \overline{C_c(G)}$, donde la cerradura se da en el encaje visto antes en $\mathcal{L}(L^2G)$.

Conjetura de Kaplansky-Kadison. *Si G es un grupo libre de torsión, entonces $C_r^*(G)$ no tiene elementos idempotentes diferentes de 0 y 1.*

No es difícil ver que $\mathbb{C}G$ está encajado en $C_r^*(G)$ y por lo tanto, que la conjetura anterior implica la conjetura de elementos idempotentes de Kaplansky en $\mathbb{C}$. Pero más generalmente, la importancia de la anterior conjetura es que la conjetura de Baum-Connes implica la conjetura de Kaplansky-Kadison y a su vez, la conjetura de elementos idempotentes de Kaplansky (Ver [3] y [38]). Por último, es importante comentar que las conjeturas de Kaplansky tienen relación también con la conjetura de Farrell-Jones [1] y con la conjetura fuerte de Atiyah [21], aunque no daremos más detalles al respecto, ya que implicaría una discusión más larga y complicada.

5.2 Preguntas Abiertas y Trabajo Futuro

Durante la realización de este trabajo surgieron diversos cuestionamientos sin resolver, que son interesantes para un posible trabajo futuro. Aquí se recaban algunas de las más relevantes y cómo posiblemente pueden ser tratadas.

Se pudo comprobar la relevancia que los grupos con producto único tienen para las conjeturas de Kaplansky, tanto así que dos importantes grupos que no cumplen la propiedad de producto único, tampoco satisfacen la conjetura de la unidad para diversos campos. En general, no se ha comprobado que exista un grupo que no satisfaga la propiedad de producto único, pero que si satisfaga la conjetura de la unidad. Quizás suene entonces aventurado con los pocos casos que se conocen pero es una posibilidad importante a considerar la siguiente pregunta.

- **P1.** ¿Los grupos con producto único caracterizan a los grupos que satisfacen la conjetura de la unidad de Kaplansky?

La siguiente pregunta es del estilo de la anterior, pues es aventurado decirlo, pero es curioso que el grupo de Promislow que se demostró que no satisface la conjetura de la unidad para el campo $\mathbb{F}_2$, tampoco la satisfaga para diversos campos diferentes.

- **P2.** Sea G un grupo libre de torsión y K_1 un campo tales que K_1G tiene unidades no triviales. Entonces, si K_2 es cualquier campo, ¿K_2G tiene unidades no triviales?

Fue interesante en la Sección 3.4 que de cierta manera los ejemplos dados de grupos tenían dentro el grupo de la botella de Klein y que aunque parecieran grupos algo diferentes se podían construir de la misma manera.

- **P3.** ¿Qué hace que el grupo de la botella de Klein aparezca en los ejemplos más representativos de grupos sin producto único?

Como se vio antes en la Sección 4.2, las unidades no triviales encontradas se encuentran determinadas por la condición de ser $\theta-$unitarias, lo que puede dar un indicio sobre todas las unidades posibles. Otro resultado importante en el articulo [2] es que las unidades en el anillo de grupo $\mathbb{F}_2P_1$ se pueden relacionar con las unidades en el anillo de grupo $\mathbb{F}_2D_\infty$, donde D_∞ es el grupo dihedral infinito. Lo interesante es que todas las unidades en este anillo de grupo se conocen, de acuerdo a [22], por lo que se puede ver cierta facilidad para encontrar algunas unidades más. Así, se tienen las siguientes preguntas.

- **P4.** ¿Hay una manera de relacionar las unidades no triviales de un anillo de grupo KG con G libre de torsión para algún otro anillo de grupo donde ya se conozcan las unidades?
- **P5.** ¿Todas las unidades no triviales en un anillo de grupo son θ-unitarias para algún θ?

Por último, analizando el contraejemplo que dio Gardam sobre el anillo $\mathbb{C}$, queda entonces la duda: ¿Qué tanto se puede generalizar este resultado? Durante la realización de este trabajo, se realizaron esfuerzos para encontrar una unidad no trivial en el anillo $\mathbb{R}P_1$, usando análogos de $\mathbb{C}$ como el anillo $\mathbb{Q}[\sqrt{2}]$, pero queda aún la respuesta abierta en general para cualquier campo de característica cero.

- **P6.** Si K es un campo de característica cero, ¿tiene KP_1 unidades no triviales?

Apéndice - Códigos Complementarios

A lo largo de este texto, distintos algoritmos computacionales fueron desarrollados para la ayuda de cálculos repetitivos. Durante este trabajo se utilizó principalmente la librería Sympy de Python. Para ver documentación completa de Sympy se puede consultar [37].

Algunas nociones básicas de Sympy para cálculos de grupos se dan a continuación. Durante todo el desarrollo de este apéndice se supone que se han cargados las siguientes librerías.

```
from sympy.combinatorics.free_groups import free_group
from sympy.combinatorics.fp_groups import FpGroup
from tabulate import tabulate
```

Para definir grupos dada una presentación, primero es necesario definir el grupo libre sobre el que se va a hacer cociente e implícitamente, las letras que se reservarán para el grupo, lo que se hace ejemplificado de la siguiente manera.

```
F1, l = free_group("l")
F2, x, y = free_group("x,y")
F3, a, b, c = free_group("a,b,c")
```

Lo anterior define los grupos libres en uno dos y tres generadores respectivamente, usando las letras correspondientes, es decir, si $A = \{l\}, B = \{x, y\}, C = \{a, b, c\}$, entonces, $F1 = F_A$, $F2 = F_B$ y $F3 = F_C$. Una vez definido un grupo libre, para tener un grupo dado su presentación, simplemente se hace cociente del grupo libre sobre la presentación del grupo utilizando la función FpGroup. Por ejemplo, para definir $G = \langle x, y \mid xy^2 \rangle$ se utiliza el siguiente código.

```
F, x, y = free_group("x,y")
G = FpGroup(F, [x*y**2])
```

Como se vio antes, es necesario indicar las multiplicaciones del grupo con el operador $*$. Las potencias de un elementos se escriben como habitualmente en python, es decir, x^n se escribe como $x**n$. Para saber si dos elementos a, b del grupo G son iguales, se puede usar el método equals, en este caso, de la siguiente manera.

```
G.equals(a,b)
```

Lo anterior es una variable booleana y es importante aclarar que dependiendo del grupo, el método puede sufrir el problema de la palabra, es decir, que el método puede no decidir si dos elementos son iguales o no. La identidad del grupo G se llama de la siguiente manera.

```
G.identity
```

Código A

Este código comprueba que el grupo de Soelberg usado en la Sección 3.4 no es isomorfo al grupo de Promislow P_1, usando el método siguiente, donde G es un grupo y n es un entero positivo.

```
low_index_subgroups(G,n)
```

Lo que regresa este método es, dado un grupo G, todos los subgrupos de índice a lo más n (salvo conjugación). Los regresa en forma de tablas de cosets (más información en la documentación), pero en este caso solo nos importará la cantidad de subgrupos que genera cada caso. El código para comprobarlo es el siguiente.

```
from sympy.combinatorics.fp_groups import low_index_subgroups
F, x, y = free_group("x,y")
G = FpGroup(F, [x * (y**2) * (x**-1) * (y**2),
                y * (x**2) * (y**3) * (x**2)])
P1 = FpGroup(F, [x*(y**2)*(x**-1)*(y**2),y*(x**2)*(y**-1)*(x**2)])

r = low_index_subgroups(G, 3)
s = low_index_subgroups(P1, 3)
conr = 0
cons = 0
for coset_table in r:
    print(coset_table.table)
    conr += 1
print(conr)
for coset_table in s:
    print(coset_table.table)
    cons += 1
print(cons)
```

El anterior código calcula la cantidad de subgrupos de índice a lo más tres e imprime las tablas de cosets correspondientes. En este caso se observa que el resultado es seis y siete, respectivamente, por lo que P_1 y G no son isomorfos.

Código B

La forma más obvia de comprobar que dos conjuntos tienen o no la propiedad de producto único es simplemente multiplicarlos y ver la cantidad de productos que dan igual. En este sentido, el siguiente método toma un grupo finitamente presentado G y dos conjuntos A, B de G. El método también requiere una tercer variable booleana que solo decide si se imprime una tabla en pantalla o se regresa el arreglo con los valores.

```
def multiplicar (G,A,B,imprimir_tabla) :
    total_productos = []
    contador = 0

    for i in range(len(A)):
        for j in range(len(B)):
            producto = G.reduce(A[i] * B[j])
```

```
            encontrado = False
            for elemento in total_productos:
                if G.equals(producto, elemento[0]) is not None:
                    if G.equals(producto, elemento[0]) :
                        contador += 1
                    elemento[1] += 1
                    elemento[2].append([A[i], B[j]])
                    encontrado = True
                    break
            if not encontrado:
                total_productos.append([producto, 1, [[A[i], B[j]]]])

    if imprimir_tabla :
        titulos = ["Productos","Cantidad", "Pares"]
        info_tabla = [[str(elemento[0]), elemento[1],
                    elemento[2]] for elemento in total_productos]
        tabla = tabulate(info_tabla, titulos, tablefmt="fancy_grid")
        print(tabla)
    else:
        return total_productos
```

Como se usa el método "equals", el anterior método puede no determinar que dos productos son iguales, por lo que podría generar un elemento más en la tabla final. En todo caso, si el método determina que dos conjuntos no tienen producto único, estaría en lo correcto, pero cuando el método dice que si se tiene producto único podría no ser correcto.

Código C

Aprovechando el método anterior y verificando la paridad se pueden realizar métodos que te den como resultado el soporte de la suma y el producto de dos elementos en $\mathbb{F}_2 G$. Ambos métodos piden como entrada el grupo G y dos conjuntos A, B que son los soportes de los elementos de $\mathbb{F}_2 G$. El método "su" regresa el soporte de la suma de los dos elementos y el método "mu" regresa el soporte del producto de dos elementos.

```
def mu(G,A,B):
    multiplicaciones  = multiplicar(G,A,B,False)
    soporte_total = []
    for multiplicacion in multiplicaciones :
        if multiplicacion[1]%2 == 1:
            soporte_total.append(multiplicacion[0])
    return soporte_total


def su(G,A,B) :
    sj = A + B
    suma = multiplicar(G, sj ,[G.identity],False)
```

```
soporte_total = []
for multiplicacion in suma :
    if multiplicacion[1]%2 == 1:
        soporte_total.append(multiplicacion[0])
return soporte_total
```

Bibliografía

[1] Arthur Bartels, Wolfgang Lück y Holger Reich. «On the Farrell-Jones conjecture and its applications». English. En: *J. Topol.* 1.1 (2008), págs. 57-86. ISSN: 1753-8416. DOI: 10.1112/jtopol/jtm008.

[2] L. Bartholdi. «On Gardam's and Murray's units in group rings». English. En: *Algebra Discrete Math.* 35.1 (2023), págs. 22-29. ISSN: 1726-3255. URL: admjournal.luguniv.edu.ua/index.php/adm/article/view/2053.

[3] Paul F. Baum y Rubén J. Sánchez-García. «K-theory for group C^*-algebras». English. En: *Topics in algebraic and topological K-theory. Papers based on the Sedano winter school on K-theory (Swisk), Sedano, Spain, January 22–27, 2007.* Berlin: Springer, (2011), págs. 1-43. ISBN: 978-3-642-15707-3; 978-3-642-15708-0. DOI: 10.1007/978-3-642-15708-0_1.

[4] B. H. Bowditch. «A variation on the unique product property.» English. En: *J. Lond. Math. Soc., II. Ser.* 62.3 (2000), págs. 813-826. ISSN: 0024-6107. DOI: 10.1112/S0024610700001307.

[5] William Carter. «New examples of torsion-free non-unique product groups.» English. En: *J. Group Theory* 17.3 (2014), págs. 445-464. ISSN: 1433-5883. DOI: 10.1515/jgt-2013-0051.

[6] I. G. Connell. «On the group ring». English. En: *Can. J. Math.* 15 (1963), págs. 650-685. ISSN: 0008-414X. DOI: 10.4153/CJM-1963-067-0.

[7] David A. Craven y Peter Pappas. «On the unit conjecture for supersoluble group algebras.» English. En: *J. Algebra* 394 (2013), págs. 310-356. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2013.07.014.

[8] David S. Dummit y Richard M. Foote. *Abstract algebra*. English. 3rd ed. Chichester: Wiley, (2004). ISBN: 0-471-45234-3.

[9] S. Peter Farbman. «The unique product property of groups and their amalgamated free products». English. En: *J. Algebra* 178.3 (1995), págs. 962-990. ISSN: 0021-8693. DOI: 10.1006/jabr.1995.1385.

[10] Giles Gardam. «A counterexample to the unit conjecture for group rings». En: *Ann. of Math. (2)* 194.3 (2021), págs. 967-979. ISSN: 0003-486X,1939-8980. DOI: 10.4007/annals.2021.194.3.9.

[11] Giles Gardam. *Non-trivial units of complex group rings*. (2023). arXiv: 2312.05240 [math.GR].

[12] Pierre Antoine Grillet. *Abstract algebra*. English. 2nd ed. Vol. 242. Grad. Texts Math. New York, NY: Springer, (2007). ISBN: 978-0-387-71567-4. DOI: 10.1007/978-0-387-71568-1.

[13] Graham. Higman. «The units of group rings». PhD Thesis. University of Oxford, (1940).

[14] Graham. Higman. «The units of group-rings». En: *Proc. London Math. Soc. (2)* 46 (1940), págs. 231-248. ISSN: 0024-6115. DOI: 10.1112/plms/s2-46.1.231.

[15] I. Kaplansky. «'Problems in the theory of rings' revisited». English. En: *Am. Math. Mon.* 77 (1970), págs. 445-454. ISSN: 0002-9890. DOI: 10.2307/2317376.

[16] Irving Kaplansky. *Problems in the theory of rings*. English. Report of a conference on linear algebras. June 6-8, New York, 1956, 1-3 (1957). (1957).

[17] Steffen Kionke y Jean Raimbault. «On geometric aspects of diffuse groups. With an appendix by Nathan Dunfield.» English. En: *Doc. Math.* 21 (2016), págs. 873-915. ISSN: 1431-0635.

[18] P. H. Kropholler, P. A. Linnell y J. A. Moody. «Applications of a new K-theoretic theorem on soluble group rings». English. En: *Proc. Am. Math. Soc.* 104.3 (1988), págs. 675-684. ISSN: 0002-9939. DOI: 10.2307/2046771.

[19] Jacques Lewin. «A note on zero divisors in group-rings». English. En: *Proc. Am. Math. Soc.* 31 (1972), págs. 357-359. ISSN: 0002-9939. DOI: 10.2307/2037530.

[20] A. I. Lichtman. «On unique product groups». English. En: *Commun. Algebra* 9 (1981), págs. 533-551. ISSN: 0092-7872. DOI: 10.1080/00927878108822598.

[21] Wolfgang Lück. *L^2-invariants: Theory and applications to geometry and K-theory*. English. Vol. 44. Ergeb. Math. Grenzgeb., 3. Folge. Berlin: Springer, (2002). ISBN: 3-540-43566-2.

[22] Maciej Mirowicz. «Units in group rings of the infinite dihedral groups». English. En: *Can. Math. Bull.* 34.1 (1991), págs. 83-89. ISSN: 0008-4395. DOI: 10.4153/CMB-1991-013-4.

[23] Alan G. Murray. *More Counterexamples to the Unit Conjecture for Group Rings*. (2021). arXiv: 2106.02147 [math.RA].

[24] Pace P. Nielsen y Lindsay Soelberg. «Small sets without unique products in torsion-free groups». En: *Journal of Algebra and Its Applications* 0.0 (2024), pág. 2550050. DOI: 10.1142/S0219498825500501.

[25] Donald S. Passman. *On the counterexamples to the unit conjecture for group rings*. (2021). arXiv: 2108.06570 [math.RA].

[26] Donald S. Passman. *The algebraic structure of group rings*. Reprint of the 1977 original. Robert E. Krieger Publishing Co., Inc., Melbourne, FL, (1985), págs. xiv+734. ISBN: 0-89874-789-9.

[27] S. David Promislow. «A simple example of a torsion-free non unique product group». English. En: *Bull. Lond. Math. Soc.* 20.4 (1988), págs. 302-304. ISSN: 0024-6093. DOI: 10.1112/blms/20.4.302.

[28] Eliyahu Rips y Yoav Segev. «Torsion-free group without unique product property». English. En: *J. Algebra* 108 (1987), págs. 116-126. ISSN: 0021-8693. DOI: 10.1016/0021-8693(87)90125-6.

[29] Joseph J. Rotman. *Advanced modern algebra*. English. Upper Saddle River, NJ: Prentice Hall/Pearson Education, (2002). ISBN: 0-13-087868-5.

[30] Joseph J. Rotman. *An introduction to homological algebra*. English. 2nd ed. Universitext. Berlin: Springer, (2009). ISBN: 978-0-387-24527-0. DOI: 10.1007/b98977.

[31] Joseph J. Rotman. *An introduction to the theory of groups.* English. 4th ed. Vol. 148. Grad. Texts Math. New York, NY: Springer-Verlag, (1995). ISBN: 0-387-94285-8.

[32] Robert Sandling. *Graham Higman's thesis "Units in group rings"*. English. Integral representations and applications, Proc. Conf., Oberwolfach 1980, Lect. Notes Math. 882, 93-116 (1981). 1981.

[33] Pascal Schweitzer. «On zero divisors with small support in group rings of torsion-free groups.» English. En: *J. Group Theory* 16.5 (2013), págs. 667-693. ISSN: 1433-5883. DOI: 10.1515/jgt-2013-0017.

[34] Jean-Pierre Serre. *Trees. Transl. from the French by John Stillwell*. English. Berlin-Heidelberg-New York: Springer-Verlag. IX, 142 p. DM 48.00; $ 28.40 1980. (1980).

[35] Lindsay Jennae. Soelberg. «Finding Torsion-free Groups Which Do Not Have the Unique Product Property». Msc Thesis. Brigham Young University, (2018).

[36] Andrzej Strojnowski. «A note on u.p. groups». English. En: *Commun. Algebra* 8 (1980), págs. 231-234. ISSN: 0092-7872. DOI: 10.1080/00927878008822456.

[37] *Sympy Documentation*. Consultado en Abril de 2024. (2024). URL: https://docs.sympy.org/latest/index.html.

[38] Alain Valette. *Introduction to the Baum-Connes conjecture. With notes taken by Indira Chatterji. With an appendix by Guido Mislin*. English. Basel: Birkhäuser, (2002). ISBN: 3-7643-6706-7.