UNIVERSIDAD DE MURCIA

Departamento de Matemáticas

TESIS DOCTORAL

BUSCANDO ESTRUCTURA EN EL GRUPO DE LAS UNIDADES DE UN ANILLO DE GRUPO CON COEFICIENTES ENTEROS

Manuel Ruiz Marín

2002

Quisiera agradecer a mi director Ángel del Río el gran esfuerzo y el tiempo que me ha dedicado, haciendo posible la elaboración de esta memoria.

También quiero expresar mi agradecimiento a todos mis familiares y amigos, por su paciencia a la hora de comprenderme y soportarme en aquellos momentos en los que no he sabido dedicarles el tiempo que ellos se merecían.

A Susana

A mis padres

Índice general

Introducción

El objeto de esta memoria es el estudio del grupo de unidades $\mathcal{U}(\mathbb{Z}G)$ del anillo de grupo con coeficientes enteros $\mathbb{Z}G$ de un grupo finito G. Podemos enmarcar el problema de estudiar $\mathcal{U}(\mathbb{Z}G)$ en el problema más general de estudiar el grupo de las unidades de un $\mathbb{Z}$-orden en una álgebra racional semisimple de dimensión finita. Este tipo de órdenes son conocidos con el nombre de órdenes clásicos. En un reciente "survey" [39] sobre órdenes clásicos, Ernst Kleinert escribía lo siguiente: "La aritmética de un orden clásico tiene dos partes naturales, la teoría de módulos y de unidades. La teoría de módulos, conocida como Teoría de Representaciones Enteras, ha tenido un desarrollo sistemático y ha generado poderosas técnicas... La teoría de unidades no está en tal estado y todavía tenemos que suscribir la afirmación de Eichler en la introducción de su artículo de 1935 [13]: "Allein die Einheitentheorie ist noch in keiner Weise abgerundet". Todavía hay pocos resultados generales que añadan información substancial a la información básica de que los grupos de unidades de órdenes son finitamente presentados. Esto no se puede achacar, por supuesto a una falta de interés.

Los ejemplos más conocidos de órdenes clásicos son los anillos de enteros de cuerpos numéricos. La estructura de estos grupos es bien conocida y viene dada por uno de los teoremas fundamentales de la Teoría de Números Algebraicos, el Teorema de las Unidades de Dirichlet: Si R es el anillo de enteros de un cuerpo numérico K, entonces el grupo $\mathcal{U}(R)$ de unidades de R es de la forma $C \times L$, donde C coincide con el grupo formado por las raíces de la unidad de K y L es un grupo abeliano libre de rango $r + s - 1$, donde r es el número de inclusiones reales de K y s el número de parejas de inclusiones complejas (no reales) de K. Existen varias generalizaciones del Teorema de las Unidades de Dirichlet para órdenes clásicos arbitrarios. Uno de ellos es un resultado de Hey [19] que asegura que si R es un orden en un álgebra de división racional de dimensión finita D, entonces el conjunto cociente Γ/G, de la acción natural del grupo de unidades $\mathcal{U}(R)$ de R en el grupo algebraico $\Gamma = \mathrm{SL}_1(\mathbb{R} \otimes_{\mathbb{Q}} D)$ formado por los elementos de norma reducida 1 de $\mathbb{R} \otimes_{\mathbb{Q}} D$, es compacto. Otra de las generalizaciones es debida a Bass [4] en términos de Teoría K. A pesar de que estos resultados pueden ser llamados generalizaciones del Teorema de las Unidades de Dirichlet en el sentido de que, para el caso en que R es el anillo de enteros de un cuerpo numérico, son equivalentes al Teorema de las Unidades de Dirichlet, estas generalizaciones son absolutamente insatisfactorias si

lo que se pretende es conocer la estructura de $\mathcal{U}(R)$ de forma tan precisa como la proporciona el Teorema de las Unidades de Dirichlet. Un libro reciente de Kleinert [40] recoge los resultados generales más importantes sobre los grupos de unidades de órdenes en álgebras racionales de división de dimensión finita.

Después de los anillos de enteros de cuerpos numéricos (y los demás órdenes de estos cuerpos), los órdenes clásicos que más interés han despertado son los anillos de grupo con coeficientes enteros. Varios libros se han dedicado exclusivamente al estudio de los anillos de grupo [50], [49], [64] o incluso sólo a unidades de anillos de grupo con coeficientes enteros [38], [65]. Este último libro contiene una excelente lista de problemas abiertos. Finalmente, dos recientes "surveys" de Jespers [25] [26] dan una buena idea del estado actual de la investigación en unidades de anillos de grupo con coeficientes enteros.

Nuestro interés y acicate principal se podría resumir en el siguiente problema que aparece como Problema 17 de la lista de problemas abiertos del libro de Sehgal [65].

> **Problema 17** [65]: Dar presentaciones por generadores y relaciones para $\mathcal{U}(\mathbb{Z}G)$ para algunos grupos finitos G.

En realidad es bien conocido que algunas presentaciones de un grupo pueden ser bastante inútiles para comprender la estructura de dicho grupo. Por tanto lo que buscamos son presentaciones "útiles" en el sentido de que sirvan para comprender como obtener el grupo mediante construcciones controlables (productos directos, productos libres, productos amalgamados, extensiones HNN, etc) a partir de grupos con estructura fácil (grupos abelianos, grupos libres, etc). A menudo nos conformaremos con conseguir estructura para un subgrupo de índice finito de $\mathcal{U}(\mathbb{Z}G)$. Esto se conoce a menudo como estructura virtual. Nuestra filosofía es intentar conseguir resultados concretos muy precisos, sacrificando en generalidad si es necesario.

Nuestro objetivo último sería obtener un resultado general que describiera la estructura de $\mathcal{U}(\mathbb{Z}G)$ de forma tan precisa como lo hace el Teorema de las Unidades de Dirichlet para anillos de enteros de cuerpos numéricos. Esto fue conseguido por Higman en los años cuarenta para el caso en que G es abeliano. Concretamente Higman [20, 21] demostró que si G es un grupo finito abeliano, entonces $\mathcal{U}(\mathbb{Z}G) = \pm G \times L$ para un grupo libre abeliano L cuyo rango se puede calcular de forma precisa mediante unos cálculos sencillos en el grupo G. Por tanto, si G es abeliano, $\mathcal{U}(\mathbb{Z}G)$ tiene un subgrupo abeliano libre de índice finito de rango fácilmente calculable. Además, Bass [4] demostró que se puede obtener una base de dicho grupo abeliano libre de índice finito en $\mathcal{U}(\mathbb{Z}G)$ utilizando las unidades cíclicas de Bass (véase la Sección 1.5 para la definición de las unidades cíclicas de Bass). Éstas son una especie de versión de las unidades ciclotómicas en $\mathbb{Z}G$.

Otro de los celebrados resultados de la tesis de Higman [20] es el de caracterizar los grupos finitos G para los que $\mathcal{U}(\mathbb{Z}G) = \pm G$. Los abelianos que satisfacen

esta propiedad se podrían determinar fácilmente con los resultados anteriores y el resultado de Higman prueba que los no abelianos con dicha propiedad son los de la forma $Q_8 \times C_2^n$, donde Q_8 es el grupo de cuaterniones con ocho elementos, C_2 es el grupo cíclico con dos elementos y n es un entero no negativo.

Un resultado de Hartley y Pickel (Teorema 5.1 de [65]) muestra que si G no es ni abeliano ni isomorfo a $Q_8 \times C_2^n$ para un entero no negativo n, entonces $\mathcal{U}(\mathbb{Z}G)$ contiene un subgrupo libre de rango 2. Obsérvese que de los resultados de Higman y de Hartley-Pickel podemos clasificar los grupos finitos G en tres clases: La formada por aquellos para los que $\mathcal{U}(\mathbb{Z}G)$ es abeliano (es decir, los grupos abelianos), la formada por los no abelianos tales que $\mathcal{U}(\mathbb{Z}G)$ es finito (es decir, los isomorfos a $Q_8 \times C_2^n$, para algún n) y la formada por los demás, que son aquellos para los que $\mathcal{U}(\mathbb{Z}G)$ contiene un subgrupo libre no abeliano. Los resultados de Higman proporcionan información satisfactoria para los grupos de las dos primeras clases. Sin embargo para los grupos de la tercera clase todo resulta mucho más difícil.

A mediados de los años 80, ni siquiera se conocía un método para encontrar un conjunto de generadores de un subgrupo de índice finito de $\mathcal{U}(\mathbb{Z}G)$ si G es de la tercera clase. A finales de los años 80 Ritter y Sehgal [57, 58, 59] descubrieron que podían utilizar los Teoremas de Congruencia [5, 66, 1] para demostrar que para muchos grupos finitos G (de hecho para casi todos) las unidades cíclicas de Bass junto con los unidades bicíclicas (véase la Sección 1.5 para la definición de las unidades bicíclicas) generan un subgrupo de índice finito. Sin embargo existen grupos finitos G para los que las unidades cíclicas de Bass y las unidades bicíclicas no generan un subgrupo de índice finito de $\mathcal{U}(\mathbb{Z}G)$. En [29] Jespers y Leal mostraron como se podia conseguir un conjunto de generadores de un subgrupo de índice finito para cada $\mathcal{U}(\mathbb{Z}G)$, con G un grupo finito nilpotente, añadiendo algunas unidades a la lista formada por las unidades cíclicas de Bass y las unidades bicíclicas.

Por tanto tenemos un fácil método para construir un conjunto de generadores de un subgrupo de índice finito para casi todos los grupos. El siguiente paso sería buscar relaciones entre los conjuntos de generadores. El papel representado por las unidades cíclicas de Bass es el de conseguir un conjunto de generadores de índice finito en el centro de $\mathcal{U}(\mathbb{Z}G)$. Por tanto nos enfrentamos al problema de buscar un conjunto completo de relaciones entre las unidades bicíclicas. Por desgracia, éste parece hoy en día un objetivo inalcanzable en toda su generalidad. En el Capítulo 2 de esta memoria estudiamos el grupo generado por dos unidades bicíclicas ... pero dejaremos el contenido de la memoria para más adelante.

Hasta los años 90 se podían contar con los dedos de la mano (tal vez dos manos eran necesarias) los grupos finitos de la tercera clase, para los que se podía describir de forma precisa $\mathcal{U}(\mathbb{Z}G)$ o un subgrupo de índice finito suyo. Para tres de estos pocos grupos, a saber S_3 [33], D_4 [28] y Q_{12} [48], se sabía que $\mathcal{U}(\mathbb{Z}G)$ contiene un subgrupo libre no abeliano. De forma ingenua se podía pensar en la posibilidad de que para los grupos G de la tercera clase $\mathcal{U}(\mathbb{Z}G)$ contuviera un subgrupo libre no abeliano de índice finito, es decir que $\mathcal{U}(\mathbb{Z}G)$ fuera virtualmente libre no abeliano. Tan ingenua

es esta posibilidad que Jespers [24] demostró que sólo existen cuatro grupos finitos G para los que $\mathcal{U}(\mathbb{Z}G)$ es virtualmente libre no abeliano.

Si profundizamos en como aparecen los grupos libres no abelianos observaremos que no sólo es fácil encontrar grupos libres no abelianos sino también productos directos de éstos con más de un factor, excepto para los cuatros grupos citados en el párrafo anterior. En efecto, si consideramos la descomposición de Wedderburn del álgebra $\mathbb{Q}G$, es decir la descomposición de $\mathbb{Q}G$ como suma directa de anillos de matrices sobre anillos de división, observaremos que si $M_n(D)$ es una de las componentes simples con $n \geq 2$ y O es un orden en D, entonces $\mathrm{GL}_n(O)$ contiene un subgrupo libre no abeliano. Esto es consecuencia inmediata del Teorema de Sanov [63] que asegura que si z es un números complejo de módulo ≥ 2, entonces el grupo generado por las matrices

$$\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} \tag{1}$$

es libre de rango 2. Utilizando propiedades elementales sobre los grupos de unidades de órdenes (ver la Sección 1.2) es fácil deducir del Teorema de Sanov que $\mathcal{U}(\mathbb{Z}G)$ contiene un producto directo de grupos libres no abelianos con tantos factores como componentes de la forma $M_n(D)$ con $n \geq 2$ aparezcan en la descomposición de Wedderburn de $\mathbb{Q}G$. De hecho trabajando un poco más se puede ver como algunas de las componentes de la descomposición de Wedderburn que son anillos de división proporcionan más factores. Por tanto es natural pensar en la posibilidad de que $\mathcal{U}(\mathbb{Z}G)$ contuviera un subgrupo de índice finito que fuera un producto directo de grupos libres, es decir, que $\mathcal{U}(\mathbb{Z}G)$ fuera virtualmente un producto directo de grupos libres. Por supuesto que esto no ocurre para todos los grupos finitos G. Los grupos G para los que $\mathcal{U}(\mathbb{Z}G)$ es virtualmente un producto directo de grupos libres fueron caracterizados en la segunda mitad de los noventa en una serie de artículos [32, 42, 35]. En el Capítulo 3 de la memoria nos ocuparemos de estos grupos.

Si observamos los métodos y resultados utilizados en la caracterización de los grupos finitos G para los que $\mathcal{U}(\mathbb{Z}G)$ es virtualmente un producto directo de grupos libres observamos que la descomposición de Wedderburn de $\mathbb{Q}G$ proporciona información substancial sobre la estructura de un subgrupo de índice finito de $\mathcal{U}(\mathbb{Z}G)$ o sobre los posibles métodos para estudiar esta estructura. En efecto, si $\mathbb{Q}G = \prod_{i=1}^{k} S_i$ es la descomposición de Wedderburn de $\mathbb{Q}G$ y O_i es un orden en S_i $(i = 1, 2, \ldots, k)$, entonces $O = \prod_{i=1}^{k} O_i$ es un orden en $\mathbb{Q}G$. Como $\mathbb{Z}G$ es otro orden en $\mathbb{Q}G$, los grupos de unidades de $\mathbb{Z}G$ y de O comparten un subgrupo de índice finito. Pero el grupo de unidades de O es el producto directo de los grupos de unidades $\mathcal{U}(O_i)$ de O_i. Luego podemos encontrar un subgrupo de índice finito en $\mathcal{U}(\mathbb{Z}G)$ de la forma $\prod_{i=1}^{k} H_i$ donde cada H_i es un subgrupo de índice finito de $\mathcal{U}(O_i)$. Por tanto, se puede estudiar la estructura virtual de $\mathcal{U}(\mathbb{Z}G)$ estudiando la estructura virtual de cada $\mathcal{U}(O_i)$. Ocurre que $\mathcal{U}(\mathbb{Z}G)$ es virtualmente un producto directo de grupos libres si y sólo si cada componente de la descomposición de Wedderburn de $\mathbb{Q}G$ es o un cuerpo, o un álgebra de cuaterniones totalmente definida ó isomorfa a $M_2(\mathbb{Q})$. Si

S_i es un cuerpo, entonces la estructura virtual de $\mathcal{U}(O_i)$ viene dada por el Teorema de las Unidades de Dirichlet; si S_i es un álgebra de cuaterniones totalmente definida y R_i es el centro de O_i, entonces $\mathcal{U}(R_i)$ tiene índice finito en $\mathcal{U}(O_i)$, por tanto estos dos grupos tienen la misma estructura virtual y, de nuevo el Teorema de las Unidades de Dirichlet nos proporciona la estructura virtual de $\mathcal{U}(O_i)$. Finalmente si S_i es isomorfo a $M_2(\mathbb{Q})$, entonces $M_2(\mathbb{Z})$ es un orden en $M_2(\mathbb{Q})$ y la estructura (virtual o no) de $\mathrm{GL}_2(\mathbb{Z})$ ha sido ampliamente estudiada.

Profundicemos un poco más en algunos de los métodos de estudio de $\mathrm{GL}_2(\mathbb{Z})$. En realidad $\mathrm{GL}_2(\mathbb{Z})$ y el grupo modular $M = \mathrm{PSL}_2(\mathbb{Z})$ tienen la misma estructura virtual y nos vamos a concentrar en M. El grupo modular M actúa por transformaciones de Möbius de forma discontinua en el plano hiperbólico. Si identificamos el plano hiperbólico con el semiplano positivo $\mathbb{H}^2 = \{z = x + yi \in \mathbb{C} : y > 0\}$, entonces el conjunto $\{z = x + yi : 2|x| \leq 1, |z| \leq 1\}$ es un dominio fundamental de la acción de M en $\mathbb{H}^2$. Utilizando esto se deduce, utilizando métodos clásicos, que $\mathrm{PSL}_2(\mathbb{Z})$ es un producto libre de los grupos libres C_2 y C_3 con 2 y 3 elementos respectivamente.

Esta forma de estudiar un grupo a partir de su acción en un objeto topológico-geométrico comenzó con Minkowski, fue explotada por Dirichlet para demostrar el Teorema de las Unidades y ha sido ampliamente generalizada por múltiples autores como Eichler, Poincaré, Borel, Harish-Chandra, Siegel y otros. El método clásico consiste en obtener un dominio fundamental de la acción, es decir un conjunto del objeto geométrico sobre el que el grupo actúa que sea, salvo un conjunto pequeño (por ejemplo de medida nula), igual a un conjunto representantes de las órbitas de la acción y a partir de este dominio fundamental deducir presentaciones del grupo. Por desgracia salvo que el objeto geométrico tenga una dimensión pequeña y la acción sea muy controlable, como ocurre con el caso de la acción de M en el plano hiperbólico, es normalmente imposible o por lo menos muy difícil encontrar un dominio fundamental y, en el caso en el que sea posible encontrarlo, es computacionalmente intratable el problema de deducir una presentación del grupo que se está estudiando, de manera que es imposible obtener ningún resultado concreto satisfactorio. Pero, como hemos explicado más arriba preferimos sacrificar generalidad para ganar concreción.

La acción de $\mathrm{PSL}_2(\mathbb{Z})$ en $\mathbb{H}^2$ es, en realidad, la restricción de la acción de $\mathrm{PSL}_2(\mathbb{C})$ por transformaciones de Möbius en la compactificación por un punto $\hat{\mathbb{C}}$ del cuerpo de los números complejos. Esta acción se puede extender a una acción en el espacio hiperbólico tridimensional $\mathbb{H}^3$. De hecho $\mathrm{PSL}_2(\mathbb{C})$ es isomorfo al grupo de isometrías de $\mathbb{H}^3$ que conservan la orientación. Los subgrupos de $\mathrm{PSL}_2(\mathbb{C})$ que actúan discontinuamente en $\mathbb{H}^3$, son exactamente los subgrupos discretos de $\mathrm{PSL}_2(\mathbb{C})$, es decir las proyecciones en $\mathrm{PSL}_2(\mathbb{C})$ de los subgrupos de $\mathrm{SL}_2(\mathbb{C})$ que tienen topología euclídea discreta. En el último capítulo de la memoria comenzamos un proyecto en el que pretendemos explorar las posibilidades que proporciona esta acción en el estudio de $\mathcal{U}(\mathbb{Z}G)$.

Pasemos ya a una descripción detallada de los contenidos de esta memoria. El

Capítulo 1 lo dedicaremos a introducir la notación y propiedades elementales que utilizaremos a lo largo de la memoria.

Como ya avisamos más arriba, dedicamos el Capítulo 2 al estudio del grupo generado por dos unidades bicíclicas. Si G es un grupo finito entonces las unidades bicíclicas de $\mathbb{Z}G$ son los elementos de la forma

$$u_{g,h} = 1 + (1-g)h\sum_{i=1}^{n} g^i \quad \text{ó} \quad v_{g,h} = 1 + \sum_{i=1}^{n} g^i h(1-g),$$

donde g y h son dos elementos de G y n es el orden de g. Llamaremos a las primeras unidades bicíclicas del primer tipo y a las segundas unidades bicíclicas del segundo tipo. Obsérvese que $u_{g,h} = 1$ si y sólo si h normaliza el subgrupo generado por g. Por tanto, $\mathbb{Z}G$ tiene unidades bicíclicas no triviales si y sólo si el grupo G no es Hamiltoniano, es decir algún subgrupo de G no es normal. El problema de determinar la estructura del grupo generado por dos unidades bicíclicas entronca con el Teorema de Hartley-Pickel. En efecto, Marciniak y Sehgal [46] mostraron que el subgrupo libre no abeliano, que Hartley y Pickel demostraron que existía de forma teórica para los grupos de la tercera clase, se puede concretar como el grupo generado por dos unidades bicíclicas concretas. Más concretamente, si $u_{g,h}$ es una unidad bicíclica no trivial entonces el grupo generado por $u_{g,h}$ y $v_{g^{-1},h^{-1}}$ es libre de rango 2. Esto fue generalizado por Salwa [62] que demostró que si $u = 1 + a$ y $v = 1 + b$ son dos elementos de un anillo libre de torsión con $a^2 = b^2 = 0$ y ab no es nilpotente, entonces existe un entero positivo m tal que el grupo multiplicativo generado por u^m y v^m es libre de rango 2. Las unidades bicíclicas son de la forma anterior, excepto que ab puede ser nilpotente. En el primer resultado del Capítulo 2 estudiamos el grupo $\langle u, v\rangle$ generado por $u = 1 + a$ y $v = 1 + b$, dos elementos de un álgebra de dimensión finita sobre un subcuerpo de los números complejos, tales que $a^2 = b^2 = 0$, para el caso que no estudio Salwa, es decir para el caso en que ab es nilpotente. Demostramos que en tal caso $\langle u, v\rangle$ es un grupo nilpotente. En particular, si u y v son dos unidades bicíclicas, entonces o bien $\langle u, v\rangle$ es nilpotente o bien existe un entero positivo m tal que $\langle u^m, v^m\rangle$ es libre de rango 2. El siguiente problema que nos planteamos es como de grande ha de ser m para que en el segundo caso $\langle u^m, v^m\rangle$ sea libre de rango 2. Nuestra sospecha es que para el caso en que u y v son unidades bicíclicas del mismo tipo basta coger $m = 1$. El teorema principal de este capítulo demuestra que esta sospecha se verifica para algunas unidades bicíclicas del grupo diédrico. Concretamente, demostraremos que si $u = u_{g,x}$ y $v = u_{h,y}$ son dos unidades bicíclicas del mismo tipo que no conmuten sobre un grupo diédrico D_n y $\langle h, y\rangle \subseteq \langle g, x\rangle$ entonces $\langle u, v\rangle$ es libre no abeliano. En particular si u y v son dos unidades bicíclicas del mismo tipo sobre el grupo diédrico D_p, con p un primo, entonces $\langle u, v\rangle$ es o bien libre abeliano o bien libre no abeliano de rango 2. La herramienta principal en la demostración es el Teorema de Sanov que se puede interpretar como un Teorema sobre puntos libres. Un número complejo z es un punto libre si las matrices (1) generan un grupo libre de rango 2. El Teorema de Sanov

asegura que los números complejos de módulo al menos 2 son libres. Nos hubiera gustado eliminar la hipótesis $\langle h, y\rangle \subseteq \langle g, x\rangle$. Sin embargo esto nos lleva al problema de decidir si $\sqrt{3}$ es un punto libre. Hemos consultado esto con varios especialistas sobre puntos libres pero ninguno de ellos ha podido dar una respuesta a la pregunta de si $\sqrt{3}$ es un punto libre o no. Bamberg [2] ha desarrollado un programa que decide de forma determinista si un número complejo es un punto libre o no. Por desgracia su ordenador no pudo dar una respuesta a nuestra pregunta después de varias horas de cálculo.

El Capítulo 3 de la memoria lo dedicamos a estudiar $\mathcal{U}(\mathbb{Z}G)$ para los grupos finitos G para los que $\mathcal{U}(\mathbb{Z}G)$ es virtualmente un producto directo de grupos libres. Como ya hemos explicado, estos grupos fueron clasificados en una serie de artículos de Jespers, Leal y del Río [32, 42, 35]. El objetivo es encontrar para cada uno de estos grupos un subgrupo de índice finito concreto en $\mathcal{U}(\mathbb{Z}G)$ que sea un producto directo de grupos libres y que además sea óptimo en el sentido de que tenga índice mínimo en $\mathcal{U}(\mathbb{Z}G)$. Si no exigimos optimalidad existe un método teórico de encontrar tal subgrupo simplemente buscando un grupo libre en cada una de las componentes de la descomposición de Wedderburn, intersecándola con $\mathcal{U}(\mathbb{Z}G)$ y cogiendo el producto directo de los subgrupos libres obtenidos. Esto nos proporcionaría muchos subgrupos de índice finito con la estructura deseada. Lo que mostraremos es que el método más simple para construirlo resulta ser el óptimo, salvo para unos pocos casos en los que hay que hacer pequeñas variaciones. Además calcularemos los rangos de los subgrupos libres que aparecen en $\mathcal{U}(\mathbb{Z}G)$.

En el Capítulo 4 comenzamos un proyecto de clasificación de los grupos finitos G para los que teóricamente se podría estudiar $\mathcal{U}(\mathbb{Z}G)$ mediante la acción de las componentes simples de la descomposición de Wedderburn de $\mathbb{Q}G$ en el espacio hiperbólico tridimensional. El objetivo es clasificar los grupos G para los cuales cada cociente simple S de $\mathbb{Q}G$ sea o bien un cuerpo o una álgebra de cuaterniones totalmente definida positiva o un álgebra de cuaterniones de forma que el grupo de unidades de norma reducida 1 de un orden de S sea un subgrupo discreto de $\mathrm{SL}_2(\mathbb{C})$. La razón de clasificar estos grupos es que en principio podríamos aplicar esta acción para estudiar $\mathcal{U}(\mathbb{Z}G)$, utilizando técnicas que fueron introducidas por Poincaré [52]; aplicadas por Bianchi [7] para los grupos que llevan su nombre es decir los grupos de la forma $\mathrm{PSL}_2(O)$ donde O es el anillo de enteros de una extensión cuadrática imaginaria de los racionales; y desarrolladas posteriormente por diversos autores (ver [14], [6], [15]). Esperamos que este proyecto nos lleve a largo plazo a obtener resultados precisos sobre la estructura de $\mathcal{U}(\mathbb{Z}G)$ para una amplia clase de grupos G. Nosotros hemos conseguido algunos resultados parciales en la mencionada clasificación. Concretamente hemos conseguido clasificar los grupos finitos nilpotentes G cuyo subgrupo derivado es central y para los que $\mathbb{Q}G$ tiene una descomposición de Wedderburn de la forma deseada. Nuestra herramienta principal es un resultado de Jespers y Leal [29] en el que se clasifican las componentes simples de la descomposición de Wedderburn de $\mathbb{Q}G$ para G un grupo nilpotente que son de la forma $M_n(D)$

para D un anillo de división y $n \leq 2$. Todas las componentes simples de los grupos que nos interesan son de esta forma.

Capítulo 1

Preliminares

En este capítulo estableceremos la notación y recordaremos los hechos básicos que se utilizarán a lo largo del trabajo. Todos los resultados que se incluyen son bien conocidos. No obstante dos de las demostraciones nos parecen útiles para la lectura de esta memoria y por tanto las hemos incluido.

1.1. Grupos

Sea G un grupo. Denotaremos por $\circ(x)$ el orden de cualquier elemento de x de G y por $Z(G)$ el centro de G.

Si G es finitamente generado se llama rango de G al menor de los cardinales de sus conjuntos de generadores y lo denotaremos $r(G)$.

Sea G un grupo abeliano finitamente generado. Entonces G es un producto directo de grupos cíclicos. El número de grupos cíclicos infinitos que aparece en cualquier descomposición de G es un invariante de G que se llama rango libre de torsión y denotamos $\rho(G)$. Un subgrupo H de G tiene índice finito en G precisamente si $\rho(G) = \rho(H)$.

Diremos que G tiene periodo finito si existe un número natural n tal $g^n = 1$, para todo $g \in G$. Si G tiene periodo finito, se llama periodo de G al menor número natural n que satisface dicha condición.

Para cada número natural n, denotamos por C_n el grupo cíclico de orden n.

Sea p un número primo. Un p-grupo abeliano elemental es un grupo abeliano finito de periodo p. Los p-grupos abelianos elementales son los isomorfos a uno de la forma C_p^n, para algún entero no negativo n.

Recordemos que un grupo G se dice nilpotente si existe una serie normal de subgrupos de G,

$$1 = G_0 \subset G_1 \subset \ldots \subset G_n = G$$

tal que $G_i/G_{i-1} \subseteq Z(G/G_{i-1})$, para todo $i = 1, \ldots, n$. Un grupo es nilpotente precisamente si todos sus subgrupos de Sylow son normales o equivalentemente si es un producto directo de sus subgrupos de Sylow [60]. En particular todo p-grupo es nilpotente.

Sean G y N dos grupos y $\varphi : G \to \mathrm{Aut}(N)$ un homomorfismo de G en el grupo de los automorfismos de N. Se llama producto semidirecto de N por G inducido por la acción φ, que denotamos por $N \rtimes_\varphi G$, ó $N \rtimes G$ si la acción está clara por el contexto, al conjunto $N \times G$ con la multiplicación dada por

$$(n_1, g_1)(n_2, g_2) = (n_1 g_1 n_2 g_1^{-1}, g_1 g_2).$$

Entonces $N \times 1$ es un subgrupo normal de $N \rtimes G$ isomorfo a N, que identificaremos con éste, y $1 \times G$ es un subgrupo de $N \rtimes G$ isomorfo a G, que identificaremos con G.

Si $n \in \mathbb{N}$, entonces el grupo dado por la siguiente presentación

$$D_n = \langle a, b \mid a^n = b^2 = 1, ba = a^{-1}b \rangle$$

tiene orden $2n$ y se llama grupo diédrico de orden n. Obsérvese que $D_n = \langle a \rangle \rtimes_\varphi \langle b \rangle$, donde $\varphi(b)$ es el automorfismo de $\langle a \rangle$ que transforma cada elemento en su inverso.

Si n es par, entonces otro grupo que utilizaremos es el grupo de cuaterniones de orden $2n$ que viene dado por la presentación

$$Q_{2n} = \langle a, b \mid a^n = b^2, a^{n/2} = 1, ba = a^{-1}b \rangle.$$

1.2. Álgebras y órdenes clásicos

Supondremos que todos los anillos son asociativos y tienen unidad. Sea A un anillo. El centro de A será denotado $Z(A)$ y $\mathcal{U}(A)$ denotará el grupo de sus unidades. Si n es un número natural, entonces $M_n(A)$ denota el anillo de matrices cuadradas n-dimensionales con entradas en A.

Recordemos que un anillo semisimple es un anillo en el que todo ideal por la izquierda es un sumando directo del anillo, o equivalentemente la misma propiedad se verifica para ideales por la derecha. El Teorema de Wedderburn-Artin caracteriza los anillos semisimples como aquellos que son isomorfos a productos directos de anillos simples artinianos y estos son precisamente los anillos de matrices sobre un anillo de división. Por tanto si A es un anillo semisimple, entonces existen idempotentes centrales ortogonales (únicos) $e_1, \ldots, e_n$ tales que $1 = e_1 + \ldots + e_n$ y, para cada

$i = 1, \ldots, n$, Ae_i es isomorfo a $M_{k_i}(D_i)$ para algún número natural k_i y algún anillo de división D_i. En tal caso, con las identificaciones necesarias escribiremos

$$A = M_{k_1}(D_1) \times \ldots \times M_{k_n}(D_n)$$

y llamaremos esta descomposición, la descomposición de Wedderburn de A. Los idempotentes $e_1, \ldots, e_n$ se llaman idempotentes centrales primitivos de A y los anillos $M_{k_i}(D_i)$ son los cocientes simples de A.

Un álgebra clásica es una $\mathbb{Q}$-álgebra semisimple de dimensión finita. Los anillos de división D_i que aparecen en la descomposición de Wedderburn de A son también álgebras clásicas.

Sea A un álgebra clásica. Un $\mathbb{Z}$-orden (o simplemente orden) en A es un subanillo O de A tal que el grupo aditivo de O es finitamente generado y $\mathbb{Q}O = A$. Si O es un orden de A, entonces el grupo aditivo de O es libre de rango finito y su rango coincide con la dimensión de A como espacio vectorial racional. Los $\mathbb{Z}$-órdenes en álgebras clásicas se conocen con el nombre de órdenes clásicos.

A lo largo de esta memoria, salvo mención expresa en sentido contrario, cuando hablemos de cuerpos nos referiremos a subcuerpos de $\mathbb{C}$, cuando hablemos de álgebras nos referiremos a álgebras clásicas y cuando hablemos de órdenes a órdenes clásicos.

Proposición 1.2.1 *Sea A un $\mathbb{Q}$-álgebra semisimple de dimensión finita (o álgebra clásica).*

1. *Todo orden de A está contenido en un orden maximal.*
2. *La intersección de dos órdenes de A es otro orden de A.*
3. *Si R y S son órdenes de A, tales que $R \subseteq S$, entonces el grupo de las unidades de R tiene índice finito en S. Además, un elemento de R es una unidad de R precisamente si es una unidad de S.*

Demostración. Las demostraciones de 1 y 2 se pueden ver en [54]. También se puede ver la demostración de 3 en [65] pero la incluiremos a modo de aperitivo. Tenemos que $R \subseteq S \subseteq A$, así que los grupos aditivos de R y S son grupos abelianos libres del mismo rango. Por lo tanto existe un número natural n tal que $nS \subseteq R$. Sean $x, y \in \mathcal{U}(S)$ tales que $x + nS = y + nS$, entonces $x^{-1}y - 1 \in nS \subseteq R$ de donde deducimos que $x^{-1}y \in R$. Análogamente tenemos que $y^{-1}x \in R$. Por lo tanto $xy \in \mathcal{U}(R)$ y $x\mathcal{U}(R) = y\mathcal{U}(R)$. Hemos demostrado que si $x\mathcal{U}(R) \neq y\mathcal{U}(R)$ también $x + nS \neq y + nS$. Por tanto $[\mathcal{U}(S) : \mathcal{U}(R)] \leq [S : nS] < \infty$.

Sea $u \in R$ tal que u es una unidad de S. Entonces

$$[S : uR] = [uS : uR] \leq [S : R]$$

y, por tanto $R = uR$, lo que implica que $u \in \mathcal{U}(R)$. $\square$

El ejemplo más clásico de álgebras clásicas son los cuerpos numéricos, es decir las extensiones finitas de $\mathbb{Q}$. Sea K un cuerpo numérico y pongamos $n = [K : \mathbb{Q}]$. Entonces existen n homomorfismos inyectivos de cuerpos de K en $\mathbb{C}$ que llamaremos inclusiones de K en $\mathbb{C}$. Las inclusiones de K en $\mathbb{C}$ cuya imagen esté contenida en $\mathbb{R}$ se llaman inclusiones reales y las demás se llaman inclusiones complejas. El número de inclusiones complejas es par, ya que la composición de una inclusión compleja con el automorfismo de conjugación de $\mathbb{C}$ es otra inclusión compleja distinta. Un cuerpo numérico se dice que es totalmente real si no tiene inclusiones complejas.

Un cuerpo numérico K tiene un único orden maximal: el anillo de enteros de K. La estructura del grupo de las unidades de cualquier orden de K viene dado por el siguiente resultado central de Teoría de Números.

Teorema 1.2.2 (Teorema de las Unidades de Dirichlet) *Sea K un cuerpo numérico y O un orden en K. Sea s el número de inclusiones reales de K y t el grupo de las inclusiones complejas de K. Entonces*

$$\mathcal{U}(O) = F \times T$$

donde F es un grupo libre abeliano de rango $s + t - 1$ y T es un grupo cíclico finito de orden par.

El asunto de este trabajo se encuentra dentro de un problema más amplio que es el estudio del grupo de las unidades de un orden en un álgebra clásica. Es decir el objetivo es encontrar un Teorema de Unidades de Dirichlet para álgebras clásicas no conmutativas. Existen muy pocos resultados generales sobre este problema sobre el que Kleinert [39] ha escrito una recopilación. Uno de estos pocos resultados generales es el siguiente:

Teorema 1.2.3 *El grupo de las unidades de un orden en un álgebra clásica es finitamente presentado.*

Sea R un anillo conmutativo y a, b son elementos no nulos de R. Denotaremos por $\left(\frac{a,b}{R}\right)$ la R-álgebra de cuaterniones generalizada con base $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ de forma que se verifican las siguientes relaciones:

$$\mathbf{i}^2 = a, \mathbf{j}^2 = b, \mathbf{k} = \mathbf{ij} = -\mathbf{ji}.$$

Pondremos $\mathbb{H}(R) = \left(\frac{-1,-1}{R}\right)$.

Si K es un cuerpo, entonces $A = \left(\frac{a,b}{K}\right)$ es una K-álgebra simple no conmutativa de dimensión 4. Por tanto A es un anillo de división o es isomorfo a $M_2(K)$. La siguiente Proposición (ver por ejemplo, [51]) caracteriza cuando es un caso u otro.

Proposición 1.2.4 *Sea K un cuerpo y sean $a, b \in K$, entonces $\left(\frac{a,b}{K}\right)$ es un anillo de división precisamente si la única solución en K de la ecuación*

$$X^2 = aY^2 + bZ^2$$

es $X = Y = Z = 0$.

Un álgebra de cuaterniones totalmente definida es un álgebra del tipo $\left(\frac{a,b}{K}\right)$ donde K es totalmente real y $a, b < 0$. De la Proposición 1.2.4 se deduce que toda álgebra de cuaterniones totalmente definida es un anillo de división, de hecho es una subálgebra del algebra de cuaterniones hamiltonianos $\mathbb{H}(\mathbb{R})$

El siguiente resultado de Kleinert (ver por ejemplo [65, Lema 21.3] nos será de gran utilidad en el Capítulo 3.

Lema 1.2.5 *Sea A un álgebra clásica no conmutativa con centro K. Sea $\mathcal{O}$ un orden de A y $O = K \cap A$.Entonces las siguientes condiciones son equivalentes:*

1. $[\mathcal{U}(\mathcal{O}) : \mathcal{U}(O)] < \infty$
2. *A es un álgebra de cuaterniones totalmente definida.*

Para cerrar esta sección vamos a recordar la definición de norma reducida $nr : A \to Z(A)$, donde A es una álgebra central simple. Consideremos las aplicación $\varphi : A \to \mathbb{C} \otimes_{Z(A)} A \cong M_n(\mathbb{C})$ definida por $\varphi(a) = 1 \otimes a$, donde $n^2 = dim_{Z(A)}A$. Entonces se define la norma reducida de un elemento $a \in A$ como $nr(a) = det(\varphi(a))$. Existe una versión de norma reducida para álgebras más generales pero en esta memoria no la utilizamos.

1.3. Grupos lineales

Sea A un anillo y n un número natural. Denotaremos por $\mathrm{GL}_n(A)$ el grupo de las unidades del anillo de matrices $M_n(A)$. Si además A es un anillo conmutativo, entonces $\mathrm{SL}_n(A)$ denota el subgrupo de $\mathrm{GL}_n(A)$ formado por las matrices de determinante 1. Si A es un álgebra central simple se define $\mathrm{SL}_n(A)$ como el conjunto de elementos de $M_n(A)$ de norma reducida 1.

Supongamos que A es conmutativo. Consideraremos $\mathrm{GL}_1(A)$ incluido en $\mathrm{GL}_n(A)$ de forma diagonal. Entonces $\mathrm{GL}_1(A)$ es el centro de $\mathrm{GL}_n(A)$ y utilizamos la siguiente notación: $\mathrm{PGL}_n(A) = \mathrm{GL}_n(A)/\mathrm{GL}_1(A)$ y $\mathrm{PSL}_n(A) = \mathrm{SL}_n(A)/\mathrm{GL}_1(A)$.

Si I es un ideal de A con A un anillo conmutativo, entonces el núcleo del homomorfismo canónico

$$\mathrm{SL}_n(A) \to \mathrm{SL}_n(A/I)$$

se llama subgrupo de congruencia de $\mathrm{SL}_n(A)$ de nivel I. Si $a \in A$, entonces se llama grupo de congruencia de nivel a al grupo de congruencia de nivel Aa.

Sea $n \in \mathbb{N}$. Denotaremos por $\Gamma(n)$ el subgrupo de congruencia de $\mathrm{SL}_2(\mathbb{Z})$ de nivel n y por $\widehat{\Gamma}(n)$ la imagen de $\Gamma(n)$ en $\mathrm{PSL}_2(\mathbb{Z})$. Observemos que $\widehat{\Gamma}(n) = \Gamma(n)$ para $n \geq 3$. Definimos $G(n) = \Gamma(1)/\Gamma(n)$ y $\widehat{G}(n) = \widehat{\Gamma}(1)/\widehat{\Gamma}(n)$. Denotamos por $\mu(n)$ y $\widehat{\mu}(n)$ los ordenes de $G(n)$ y $\widehat{G}(n)$ respectivamente. El siguiente resultado [47] nos proporciona fórmulas para $\mu(n)$ y $\widehat{\mu}(n)$.

Teorema 1.3.1 *Si $n \in \mathbb{N}$, entonces*

$$\mu(n) = n^3 \prod_{p/n}(1 - \frac{1}{p^2}),$$

donde el producto se toma sobre todos los primos p que dividen a n. Además $\mu(n) = \widehat{\mu}(n)$ para $n = 1, 2$ y $\widehat{\mu}(n) = \frac{1}{2}\mu(n)$ para $n \geq 3$

La estructura de $\Gamma(n)$ es bien conocida tal y como muestra el siguiente resultado que resume una serie de resultados que se pueden encontrar en el libro de Newman [47].

Teorema 1.3.2 *$\widehat{\Gamma}(1)$ es el producto libre $C_3 * C_2$ y si $n \geq 2$ entonces $\widehat{\Gamma}(n)$ es libre no abeliano. En particular si $n \geq 3$, $\Gamma(n)$ es libre no abeliano.*

1.4. Anillos de grupos

El anillo grupo de un grupo G sobre un anillo R es el anillo RG formado por todas las sumas formales $\lambda = \sum_{g \in G} \lambda_g g$, $\lambda_g \in R$, tal que el conjunto

$$sop(\lambda) = \{g : \lambda_g \neq 0\},$$

llamado el soporte de λ, es finito; con las siguientes reglas de operación:

$$\sum_{g \in G} \lambda_g g + \sum_{g \in G} \mu_g g = \sum_{g \in G} (\lambda_g + \mu_g) g$$

$$(\sum_{g \in G} \lambda_g g)(\sum_{g \in G} \mu_g g) = \sum_{g \in G} \nu_g g,$$

donde

$$\nu(g) = \sum_{h \in G} \lambda_h \mu_{h^{-1}g} = \sum_{xy=g} \lambda_x \mu_y.$$

La aplicación $r \mapsto re_G$, donde e_G es el neutro del grupo G es un homomorfismo inyectivo de R en RG. Después de la identificación de R con Re_G, a través de este

homomorfismo consideraremos R contenido en RG. También la aplicación $g \mapsto 1g$ es un homomorfismo de G en el grupo de las unidades de RG y consideraremos G incluido en RG a través de este homomorfismo. Mediante estas identificaciones, la unidad de RG coincide con la unidad de G y con la unidad de R.

La aplicación

$$\begin{array}{c} \omega : RG \longrightarrow R \\ \sum\limits_{g\in G} \lambda_g g \to \sum\limits_{g\in G} \lambda_g \end{array}$$

es un homomorfismo de anillos llamado homomorfismo de aumento de RG. Su núcleo

$$\triangle_R(G) = \{\lambda = \sum_{g\in G} \lambda_g g \in RG : \sum_{g\in G} \lambda_g = 0\}$$

se llama el ideal de aumento de RG. Para un subgrupo normal N de G tenemos el homomorfismo

$$\begin{array}{c} \omega_N : RG \longrightarrow R(G/N) \\ \sum\limits_{g\in G} \lambda_g g \to \sum\limits_{g\in G} \lambda_g gN \end{array} \quad .$$

En particular $\omega = \omega_G$. Denotamos por $\triangle_R(G,N)$, el núcleo de ω_N.

Proposición 1.4.1 *Si N es un subgrupo normal de G, entonces*

$$\begin{aligned} \triangle_R(G,N) &= \{\sum_{g\in G} \lambda_g g \in RG : \sum_{x\in N} \lambda_{gx} = 0, \text{ para todo } g \in G\} \\ &= \sum_{n\in N} RG(n-1) \\ &= \sum_{n\in N} (n-1)RG \\ &= \sum_{n\in X} RG(n-1) \\ &= \sum_{n\in X} (n-1)RG \end{aligned}$$

donde X es un conjunto de generadores de N.

Demostración. La primera igualdad es consecuencia inmediata de la definición. Como $n-1 \in \triangle_R(G,N)$, por simetría, para acabar la demostración basta demostrar que

$$\triangle_R(G,N) \subseteq \sum_{n\in X} RG(n-1).$$

Sea $\sum\limits_{g\in G} \lambda_g g \in \triangle_R(G,N)$ entonces $\sum\limits_{x\in N} \lambda_{gx} = 0$ para todo $g \in G$. Sea A un conjunto de representantes de las clases de G/N. Entonces

$$\sum_{g\in G} \lambda_g g = \sum_{g\in A}(\sum_{x\in N} \lambda_{gx} gx) = \sum_{g\in A}(\sum_{x\in N} \lambda_{gx} gx - \sum_{x\in N} \lambda_{gx} g) = \sum_{g\in A}(\sum_{x\in N} \lambda_{gx} g(x-1)).$$

Por tanto $\triangle_R(G,N) \subseteq \sum_{n\in N} RG(n-1)$. Por otro lado, si $n \in N$, entonces $n = x_1^{k_1} \dots x_n^{k_n}$, donde $x_1, \dots, x_n \in X$ y $k_1, \dots, k_n \in \mathbb{Z}$. La demostración se acaba por inducción utilizando las fórmulas

$$x^{-1} - 1 = -x^{-1}(x-1); xy - 1 = (x-1)(y-1) + (x-1) + (y-1).$$

□

En particular

$$\begin{aligned} \triangle_R(G) &= \triangle_R(G,G) \\ &= \sum_{n\in G} RG(n-1) \\ &= \sum_{n\in G} (n-1)RG \\ &= \sum_{n\in X} RG(n-1) \\ &= \sum_{n\in X} (n-1)RG \end{aligned}$$

donde X es un conjunto de generadores de G. Siempre que el anillo R esté claro por el contexto, simplemente escribiremos $\triangle(G,N)$ en vez de $\triangle_R(G,N)$.

Los anillos de grupo semisimples están caracterizados por el siguiente Teorema.

Teorema 1.4.2 (Maschke) *Un anillo de grupo RG es semisimple precisamente si R es semisimple, G es finito y el orden de G es una unidad de R.*

Sea G un grupo finito. Por el Teorema de Maschke, $\mathbb{Q}G$ es un álgebra clásica. Claramente $\mathbb{Z}G$ es un orden en $\mathbb{Q}G$. Llamaremos denominador de un elemento α de $\mathbb{Q}G$ al menor número natural n tal que $n\alpha \in \mathbb{Z}G$.

Si H es un subgrupo de G, denotamos

$$\widehat{H} = \frac{\sum_{h\in H} h}{\mid H \mid} \in \mathbb{Q}G.$$

Si $g \in G$, escribimos

$$\widehat{g} = \widehat{\langle g \rangle}.$$

Obsérvese que $\widehat{H}$ es un idempotente de $\mathbb{Q}G$. Además, $\widehat{H}$ pertenece al centro de $\mathbb{Q}G$ precisamente si H es normal en G. Si $h \in H$, entonces $h\widehat{H} = \widehat{H}$. Utilizando esto se puede ver que si X es un conjunto de representantes por la izquierda de G/H, entonces $\{x\widehat{H} : x \in X\}$ es una base de $\mathbb{Q}G\widehat{H}$ como espacio vectorial sobre $\mathbb{Q}$ y

$$(\sum_{g\in G} \lambda_g g)\widehat{H} = \sum_{x\in X} (\sum_{h\in H} \lambda_{xh}) x\widehat{H}.$$

En particular si H es un subgrupo normal, entonces

$$\triangle_{\mathbb{Q}}(G,H) = \{a \in \mathbb{Q}G : a\widehat{H} = 0\}$$

y por tanto

$$\mathbb{Q}(G/H) \simeq (\mathbb{Q}G)\widehat{H}\,.$$

Obsérvese que esto implica que $(\mathbb{Q}G)\widehat{G'} \simeq \mathbb{Q}(G/G')$ es conmutativo. Por tanto si e es un idempotente central primitivo de $\mathbb{Q}G$ tal que $e\widehat{G'} \neq 0$, entonces $(\mathbb{Q}G)e$ es un cuerpo numérico. De hecho el recíproco también se verifica [10], es decir, todos los cocientes simples de $\mathbb{Q}(1-\widehat{G'})$ son no conmutativos.

Sea $u \in \mathcal{U}(\mathbb{Z}G)$. Entonces $\omega(u)$ es una unidad de $\mathbb{Z}$ y por tanto u tiene aumento ± 1. Luego $\mathcal{U}(\mathbb{Z}G) = \pm\mathcal{U}_1(\mathbb{Z}G)$ donde $\mathcal{U}_1(\mathbb{Z}G)$ es el conjunto de todas las unidades que tienen aumento uno.

1.5. Unidades de $\mathbb{Z}G$

Veamos ahora algunos ejemplos de unidades de $\mathbb{Z}G$.

Los elementos de la forma $\pm g$ con $g \in G$ son claramente unidades, siendo el inverso $\pm g^{-1}$. Éstas son las llamadas unidades triviales. Se conocen pocas maneras de construir unidades en $\mathbb{Z}G$ pero mencionamos las dos siguientes:

1. Unidades bicíclicas

Estas unidades fueron introducidas por Ritter y Sehgal en [56]. Sean $a, b \in G$ y sea n el orden de b. Entonces $((1-b)a\widehat{b})^2 = 0$. Así

$$u_{b,a} = 1 + (1-b)a(1+b+\cdots+b^n) = 1 + (1-b)an\widehat{b}$$

$$v_{b,a} = 1 + (1+b+\cdots+b^n)a(1-b) = 1 + n\widehat{b}a(1-b)$$

tienen inversos y son

$$u_{b,a}^{-1} = 1 - (1-b)a(1+b+\cdots+b^n) = 1 - (1-b)an\widehat{b}$$

$$v_{b,a}^{-1} = 1 - (1+b+\cdots+b^n)a(1-b) = 1 - n\widehat{b}a(1-b)$$

.

Obsérvese que solamente las unidades del estilo $u_{b,a}$ son llamadas unidades bicíclicas en [65]. Obsérvese también que $u_{b,a} = 1$ si y sólo si $v_{b,a} = 1$ si y sólo si a normaliza a $\langle b \rangle$.

Por tanto todas las unidades bicíclicas son 1 si y sólo si todos los subgrupos de G son normales, en particualr las unidades bicíclicas de $\mathcal{U}(\mathbb{Z}G)$ para G un grupo abeliano son 1.

2. Unidades cíclicas de Bass

Se definen como:

$$b = b(g,i) = (1 + g + \cdots + g^{i-1})^{\varphi(m)} + (1 - i^{\varphi(m)})\widehat{g}$$

donde $g \in G$ es un elemento de orden m, $1 < i < m$ es coprimo con m y φ es la función de Euler. Obsérvese que $b(g,i) \in \mathbb{Z}G$ ya que m divide a $1 - i^{\varphi(m)}$. La inversa de una unidad cíclica de Bass es de nuevo una unidad cíclica de Bass, de hecho tenemos que

$$b^{-1} = (1 + g + \cdots + g^{i(k-1)})^{\varphi(m)} + (1 - k^{\varphi(m)})\widehat{g} = b(g^i, k)$$

donde k es es el inverso de i módulo m.

Las unidades cíclicas de Bass son una especie de unidades ciclotómicas. Vamos a justificar esto a la vez que damos una demostración alternativa de porque las unidades cíclicas de Bass son unidades de $\mathbb{Z}G$.

Recuérdese que las unidades ciclotómicas de un cuerpo ciclotómico $\mathbb{Q}(\xi_n)$ (ξ_n una raíz n-ésima primitiva de 1) son las de la forma $\frac{1-\xi_n^i}{1-\xi_n} = 1 + \xi_n + \cdots + \xi_n^{i-1}$ donde $(i,n) = 1$. En tal caso la inversa de $\frac{1-\xi_n^i}{1-\xi_n}$ es $\frac{1-\xi_n}{1-\xi_n^i} = \frac{1-\xi_n^{ik}}{1-\xi_n^i}$ siendo k el inverso de i módulo n. Si g tiene orden n los idempotentes primitivos de $\mathbb{Q}\langle g\rangle$ son $e_1 = \widehat{g}$ y los elementos de la forma $e_d = \widehat{g^d} - \widehat{g}$ donde d es un divisor de n diferente de 1. Entonces $\mathbb{Q}Ge_d \cong_{\varphi_d} \mathbb{Q}(\xi_d)$ donde ξ_d se identifica mediante este isomorfismo con ge_d. Por tanto la aplicación lineal $f : \mathbb{Q}G \to \prod_{d|n} \mathbb{Q}(\xi_d)$ que asocia g con $\sum_{d|m} \xi_d$ es un isomorfismo entre $\mathbb{Q}G$ y $\prod_{d|n} \mathbb{Q}(\xi_d)$ que transforma $R = \mathbb{Z}G$ en un subanillo de $\prod_{d|m} \mathbb{Z}[\xi_d] = S$. Ahora observemos que $\varphi_d(b(g,i))$ es una unidad ciclotómica de $\mathbb{Z}[\xi_d]$ para cada $d|n$ y por tanto $\varphi_d(b(g,i))$ es una unidad de S. Como R es un orden de $\mathbb{Q}G$ y S es un orden de $\prod_{d|n} \mathbb{Q}(\xi_d)$ de la Proposición 1.2.1 se deduce que $b(g,i)$ es una unidad de $\mathbb{Z}G$.

Bass [4] demostró que si G es un grupo abeliano las unidades cíclicas de Bass generan un subgrupo que contiene un subgrupo de índice finito del centro de $\mathcal{U}(\mathbb{Z}G)$.

Se sabe que el grupo B_G generado por la unidades cíclicas de Bass y las unidades bicíclicas (de un sólo tipo) genera un subgrupo de índice finito en $\mathcal{U}(\mathbb{Z}G)$ en los siguientes casos (véase [58] y [59]):

1. G un $2-$grupo tal que $\mathbb{Q}G \cong \sum_i M_{n_i}(D_i)$ donde D_i son cuerpos y si $n_i = 2$ entonces $D_i \neq \mathbb{Q}$ o una extensión cuadrática imaginaria.

2. G es un grupo finito nilpotente de orden impar.

3. G es el grupo simétrico S_n.

Además Jespers y Leal [28] han extendido estos resultados a clases más amplias de grupos.

Sin embargo no es cierto en general que B_G tenga índice finito en $\mathcal{U}(\mathbb{Z}G)$. De hecho $G = D_8$ es el único 2-grupo no abeliano indescomponible para el que B_G genera un subgrupo de índice finito en $\mathcal{U}(\mathbb{Z}G)$ [34].

Capítulo 2

Grupos generados por dos unidades bicíclicas en $\mathbb{Z}G$

2.1. Introducción

Ritter y Sehgal [56] introdujeron las siguientes unidades, llamadas unidades bicíclicas en el grupo de unidades $\mathcal{U}(\mathbb{Z}G)$ para un grupo finito G:

$$u_{g,a} = 1 + (1-g)a\widehat{g}, \quad v_{g,a} = 1 + \widehat{g}a(1-g),$$

donde $a, g \in G$.

Se ha demostrado que estas unidades generan gran parte del grupo de las unidades de $\mathbb{Z}G$. De hecho para la mayoría de los grupos finitos G, las unidades bicíclicas de uno de los dos tipos u ó v junto con las unidades cíclicas de Bass generan un subgrupo de índice finito en $\mathcal{U}(\mathbb{Z}G)$ (véase por ejemplo [28, 58]). Si G es un grupo finito abeliano, las unidades bicíclicas son triviales y las unidades cíclicas de Bass generan un subgrupo de índice finito en $\mathcal{U}(\mathbb{Z}G)$.

Las unidades cíclicas de Bass sólo se necesitan para cubrir un subgrupo de índice finito en el centro de $\mathcal{U}(\mathbb{Z}G)$ y el grupo B generado por todas las unidades bicíclicas contiene un subgrupo de índice finito en el grupo de las unidades de norma reducida 1 de un $\mathbb{Z}$-orden maximal de cada componente simple no conmutativa de la descomposición de Wedderburn de la $\mathbb{Q}$-álgebra $\mathbb{Q}G$. En particular, si $n > 1$, entonces B contiene un subgrupo de índice finito en $\mathrm{SL}_n(\mathcal{O})$ donde $\mathcal{O}$ es un orden maximal en D y por lo tanto B contiene grupos libres de rango 2. El próximo paso para determinar la estructura de $\mathcal{U}(\mathbb{Z}G)$ sería investigar las distintas relaciones entre los generadores

que hemos obtenido, esto parece hoy en dia una tarea intratable. Una meta a superar más realista sería estudiar la estructura del grupo generado por dos unidades bicíclicas. Marciniak y Sehgal [46] demostraron que si $u_{g,a}$ es una unidad no trivial en $\mathbb{Z}G$ (aquí G no es necesariamente finito) entonces el grupo $\langle u_{g,a}, v_{g^{-1},a^{-1}} \rangle$ es libre de rango 2. Claramente, las unidades bicíclicas son de la forma $1+a$ con $a^2=0$. Salwa, en [62], utilizó las ideas de Marciniak y Sehgal para demostrar que si x e y son dos elementos de un anillo cuyo grupo aditivo es libre de torsión tales que $x^2=y^2=0$ y xy no es nilpotente entonces $\langle (1+x)^m, (1+y)^m \rangle$ es libre de rango 2 para algún entero positivo m. En particular, si b_1 y b_2 son dos unidades bicíclicas y $(b_1-1)(b_2-1)$ no es nilpotente, entonces $\langle b_1^m, b_2^m \rangle$ es libre de rango 2 para algún entero positivo m. En este Capítulo vamos a estudiar cual es el menor entero positivo m tal que $\langle b_1^m, b_2^m \rangle$ es libre suponiendo que b_1 y b_2 son dos unidades bicíclicas tal que $(b_1-1)(b_2-1)$ no es nilpotente. Demostraremos el siguiente Teorema que nos indica si b_1 y b_2 son del mismo tipo entonces frecuentemente $m=1$.

Teorema 2.1.1 *Sean $b_1 = u_{g,x}$ y $b_2 = u_{h,y}$ dos unidades bicíclicas de $\mathbb{Z}D_n$ del mismo tipo donde D_n es el grupo diédrico*

$$D_n = \langle a, b | a^n = b^2 = 1, ba = a^{-1}b \rangle$$

tales que $\langle y, h \rangle \subseteq \langle x, g \rangle$. Entonces $\langle b_1, b_2 \rangle$ es o bien abeliano libre de torsión o bien libre de rango 2.

Como una consecuencia del Teorema 2.1.1 obtenemos el siguiente resultado

Corolario 2.1.2 *Si p es primo y b_1 y b_2 son dos unidades bicíclicas del mismo tipo del grupo diédrico D_p entonces $\langle b_1, b_2 \rangle$ es abeliano libre de torsión o libre de rango 2.*

Antes de demostrar estos resultados demostraremos en la siguiente sección un resultado que completa el resultado de Salwa [62] antes mencionado mostrando que si x e $y \in A$ son tales que $x^2=y^2=0$ y xy es nilpotente, entonces $\langle 1+x, 1+y \rangle$ es un grupo nilpotente.

Los resultados de este capítulo aparecieron en [36]

2.2. La dicotomía Nilpotente-Libre

En esta sección demostraremos el siguiente Teorema que completa el resultado de Salwa con el caso en que ab es nilpotente.

Teorema 2.2.1 *Sea K un subcuerpo de $\mathbb{C}$ y R una K-algebra de dimensión finita. Supongamos que a y b son dos elementos de R tales que $a^2=b^2=0$. Entonces se verifican las siguientes afirmaciones:*

1. *Si ab es nilpotente, entonces $\langle 1+a, 1+b\rangle$ es nilpotente;*

2. *Si ab no es nilpotente entonces existe un entero positivo m tal que $\langle 1+a, (1+b)^m\rangle$ es libre de rango 2.*

La mayoría de las ideas que aparecen en la demostración de 2 ya estaban en [62] y de hecho la base principal de estas ideas aparecían en el artículo original de Marciniak y Sehgal [46]. Incluimos las demostraciones completas tanto por completitud como por que utilizaremos los lemas previos en la Sección 3.3 en la que demostramos el Teorema 2.1.1

Para demostrar el Teorema 2.2.1 podemos suponer que $R = K[a,b]$. Sea $J(R)$ el radical de Jacobson de R, luego $R/J(R) = \sum_{i=1}^{k} M_{n_i}(D_i)$, donde D_i es una K-algebra de división para todo i. Empezamos viendo que los valores posibles de n_i y D_i están restringidos.

Si x es un número real entonces $\lfloor x \rfloor$ (resp. $\lceil x \rceil$) denota el mayor (resp. menor) entero más pequeño (resp. más grande) que x.

Lema 2.2.2 *En las condiciones anteriores, para todo $i = 1, \ldots, k$ se verifica que $n_i \leq 2$ y D_i es un cuerpo. Además si $n_i = 1$ entonces $D_i = K$.*

Demostración. Sea $A = \mathbb{C}[a,b] = \mathbb{C} \otimes_K K[a,b] = \mathbb{C} \otimes_K R$. Primero demostraremos que todo cociente simple de $A/J(A)$ es de la forma $M_m(\mathbb{C})$ con $m \leq 2$. Podemos suponer sin pérdida de generalidad que A es simple, luego $A = M_m(\mathbb{C})$ para algún entero positivo m e identificamos A con el anillo de endomorfismos de un espacio vectorial complejo m-dimensional. Sea $B = \mathbb{C}[ab]$. Entonces $A = B + Ba + bB + bBa$ y así $\dim_{\mathbb{C}} A \leq 4 \dim_{\mathbb{C}} B$. Como $a^2 = 0$ tenemos que $\operatorname{Im} a \subseteq \operatorname{Ker} a$ y por lo tanto $2 \dim_{\mathbb{C}} \operatorname{Im} a \leq m$. Consecuentemente, $\dim_{\mathbb{C}} \operatorname{Im} ab \leq \dim_{\mathbb{C}} \operatorname{Im} a \leq \left\lfloor \frac{m}{2} \right\rfloor$. Entonces el Teorema de Cayley-Hamilton implica que ab satisface una identidad polinómica de grado como mucho $\left\lfloor \frac{m}{2} \right\rfloor + 1$. Luego $\dim_{\mathbb{C}} B \leq \left\lfloor \frac{m}{2} \right\rfloor + 1$ y así $m^2 = \dim_{\mathbb{C}} A \leq 4(\left\lfloor \frac{m}{2} \right\rfloor + 1)$. Consecuentemente $\left(\frac{m}{2}\right)^2 \leq \left\lfloor \frac{m}{2} \right\rfloor + 1$, y por lo tanto $m \leq 2$.

Claramente, ambos $J(R)$ y $J(A)$ son nilpotentes. Como A es una extensión central de R sabemos que $J(R) = J(A) \cap R$. Luego consideramos $R/J(R)$ como un subanillo de $A/J(A)$.

Sea $S = M_n(D)$, con D un anillo de división, un cociente simple de R. Por lo dicho anteriormente S se incluye en un cociente simple $M_m(\mathbb{C})$ de A, con $m \leq 2$. Luego todo conjunto completo de idempotentes ortogonales de S tiene como mucho 2 elementos y por tanto $n \leq 2$. Además, si $n = 2$, entonces $m = 2$ y siendo D el doble centralizador de un idempotente primitivo se tiene que $D \subseteq \mathbb{C}$. Por tanto, en este caso, D es un cuerpo. Por otro lado, si $m = 1$, las imágenes naturales de $\overline{a}$ y $\overline{b}$ en $S = D$ son cero. Luego $S = K\left[\overline{a}, \overline{b}\right] = K$. Esto demuestra el resultado. □

El siguiente Lema se encargará del caso en que ab es nilpotente.

Lema 2.2.3 *Sea $A = M_2(D)$ donde D es un anillo de división y a y b elementos de A tales que $a^2 = b^2 = 0$. Si ab es nilpotente entonces $ab = ba = 0$.*

Demostración. De nuevo, identificamos A con el anillo de endomorfismos de un espacio vectorial V sobre D de dimensión 2. Si $ab \neq 0$ entonces Ker ab = Ker b = Im b e Im ab = Im a = Ker a. Sean $0 \neq v_1 \in$ Im a y $v_2 \in V$ tales que $a(v_2) = v_1$. Entonces V es el espacio vectorial por la izquierda sobre D generado por v_1 y v_2. Además, $(ab)(v_1) = \lambda v_1$ para algún $\lambda \in D$. Como ab es nilpotente, $\lambda = 0$. Luego $(ab)^2 = 0$ y por lo tanto Ker b = Ker ab = Im ab = Im a. Concluimos que $ab = 0$, una contradicción. Por tanto ab es nilpotente y por simetría $ba = 0$. □

En este momento podríamos pasar a demostrar el Teorema 2.2.1 pues como veremos tenemos todos los ingredientes para demostrar la afirmación 1 y la afirmación 2 fue demostrada por Salwa [62]. Sin embargo vamos a dar una demostración ligeramente diferente a la de Salwa que nos servirá para obtener una propiedad que utilizaremos en la Sección 3.3. También utilizaremos el siguiente resultado.

Teorema 2.2.4 (Teorema de Sanov. Teorema 14.2.1 [37]) *Si z y w son dos números complejos tal que $|zw| \geq 4$, entonces las dos matrices siguientes generan un grupo libre de rango 2:*

$$P = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & 0 \\ w & 1 \end{pmatrix}$$

Lema 2.2.5 *Sea $A = M_2(K)$, donde K es un subcuerpo de $\mathbb{C}$ y $a, b \in A$ tales que $a^2 = b^2 = 0$ y ab no es nilpotente. Entonces $\langle 1 + a, 1 + mb \rangle$ es un grupo libre para algún entero positivo m. Si, además, $|tr(ab)| \geq 4$, donde tr denota la traza, entonces $\langle 1 + a, 1 + b \rangle$ es un grupo libre.*

Demostración. De nuevo identificamos A con el anillo de endomorfismos del K-espacio vectorial 2-dimensional K^2. Como ab no es nilpotente, después de un cambio de base en K^2, podemos suponer que

$$ab = \begin{pmatrix} \lambda & 0 \\ 0 & 0 \end{pmatrix}$$

para algún $0 \neq \lambda \in K$. Así, como $Im(a) = Im(ab)$ y $Ker(b) = Ker(ab)$, tenemos que

$$a = \begin{pmatrix} p & r \\ 0 & 0 \end{pmatrix} \quad \text{y} \quad b = \begin{pmatrix} q & 0 \\ s & 0 \end{pmatrix}$$

para algunos $p, q, r, s \in K$. Como a y b son elementos no nulos nilpotentes, obtenemos que $p = 0 = q$ y $r \neq 0$ y $s \neq 0$. Así

$$1 + a = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad 1 + b = \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix}.$$

Luego por el Teorema 2.2.4 $\langle 1+a, 1+mb\rangle$ es un grupo libre para $m = \left\lceil \frac{4}{|rs|} \right\rceil$. Si $|tr(ab)| \geq 4$, entonces $|rs| \geq 4$ y así $m = 1$. □

Ahora vamos a dar la demostración del Teorema 2.2.1.

Demostración del Teorema 2.2.1. Podemos suponer que $R = K[a, b]$. Sea J el radical de Jacobson de R e identificaremos $\overline{R} = R/J$ con una suma directa $\bigoplus_{i=1}^{k} M_{n_i}(D_i)$ de anillos de matrices sobre anillos de división. Por el Lema 2.2.2 $n_i \leq 2$ para todo i y todos los D_i son cuerpos. Para cada $i = 1, 2, \ldots, k$ sea $\rho_i : R \to M_{n_i}(D_i)$ una de las proyecciones.

Si ab es nilpotente entonces $\rho_i(ab)$ es nilpotente para todo i. Por el Lema 2.2.3 $\rho_i(ab) = \rho_i(ba) = 0$ y por tanto $ab, ba \in J$. Como $R = K[a, b]$, los ideales por la izquierda de $\overline{R}$ generados por $a + J$ y $b + J$ son nilpotentes, lo que implica que $a, b \in J$. Como R es artiniano J es nilpotente y ahora es fácil deducir por inducción en el índice de nilpotencia de J que el grupo $\langle 1 + a, 1 + b\rangle$ es nilpotente.

Si ab no es nilpotente entonces $\rho_i(ab)$ no es nilpotente para algún i con $n_i = 2$. Por el Lema 2.2.5 $\langle 1+\rho_i(a), 1+m\rho_i(b)\rangle$ es libre de rango 2 para algún entero positivo m y por tanto $\langle 1 + a, 1 + mb\rangle$ es libre de rango 2. □

Antes de cerrar esta Sección demostraremos la siguiente Proposición que utilizaremos en la demostración del Teorema 2.1.1

Proposición 2.2.6 *Sea A una $\mathbb{Q}$-algebra que es el producto directo de anillos de división y anillos de matrices cuadradas de dimensión 2 sobre subcuerpos de $\mathbb{C}$. Sean $a, b \in A$ tales que $a^2 = b^2 = 0$. Las siguientes propiedades se verifican*

1. *Si ab es nilpotente, entonces $\langle 1 + a, 1 + b\rangle$ es abeliano libre de torsión.*
2. *Si ab no es nilpotente, entonces existe un entero m tal que $\langle 1+a, 1+mb\rangle$ es libre de rango 2. Además si $|\mathrm{tr}(\rho(ab))| \geq 4$, para alguna proyección $\rho : A \to M_2(K)$ sobre una componente simple de A, entonces $\langle 1 + a, 1 + b\rangle$ es libre de rango 2.*

Demostración. Todo es consecuencia inmediata de el Lema 2.2.3 y el Lema 2.2.5 excepto la parte que afirma que $\langle 1+a, 1+b\rangle$ es libre de torsión para el caso abeliano.

Supongamos que $u = (1 + a)^k(1 + b)^l$ es un elemento periódico de orden m en el grupo abeliano $\langle 1 + a, 1 + b\rangle$ (con $k, l \in \mathbb{Z}$). Entonces $1 + kma = 1 - lmb$, es decir $ka = -lb$. Por lo tato $(1 + a)^k = 1 + ka = 1 - lb = (1 + b)^{-l}$ y así $u = 1$. □

2.3. Unidades bicíclicas de grupos diédricos

En esta Sección demostraremos el Teorema 2.1.1. Sean $b_1 = u_{g,x}$ y $b_2 = u_{h,y}$ dos unidades bicíclicas de D_n tales que $\langle y, h\rangle \subseteq \langle x, g\rangle$. Obsérvese que $\mathbb{Q}D_n$ satisface

las condiciones de la Proposición 2.2.6, ya que todas las representaciones complejas irreducibles de D_n tienen grado ≤ 2. Por lo tanto $\langle b_1, b_2\rangle$ es abeliano libre de torsión ó $\langle b_1, b_2^k\rangle$ es libre de rango 2 para algún $k \geq 1$. Tenemos que demostrar que en el segundo caso podemos tomar $k = 1$. Para ello haremos uso una vez más de la Proposición 2.2.6 y solamente tenemos que probar que si b_1 y b_2 no conmutan entonces existe un carácter irreducible χ de grado 2 de D_n tal que $|\chi(\alpha)| \geq 4$, donde $\alpha = (b_1 - 1)(b_2 - 1)$.

Por lo tanto en lo que resta supondremos que b_1 y b_2 no conmutan. Esto implica que g y h no pertenecen a $\langle a\rangle$, luego $\langle x, g\rangle$ es un grupo diédrico. Por lo tanto podemos suponer sin pérdida de generalidad que $D_n = \langle x, g\rangle$. Como $u_{a^jb,a^ib} = u_{a^jb,a^{i-j}}$, sin pérdida de generalidad, podemos suponer que $x, y \in \langle a\rangle$ y cambiando los generadores si fuera necesario, $x = a$ y $g = b$. Resumiendo $b_1 = u_{a,b}$ y $b_2 = u_{a^i,a^jb}$ para algún $1 \leq i, j < n$ y $2i \neq n$.

Los caracteres irreducibles no lineales de D_n son todas la aplicaciones $\chi_k : G \to \mathbb{C}$, con $1 \leq k < \frac{n}{2}$, dadas por

$$\chi_k(a^t) = \xi^{kt} + \xi^{-kt}, \quad \chi_k(a^tb) = 0$$

para todo $0 \leq t < n$, donde ξ denota una raíz n-ésima de la unidad.

Para todo $m \in \mathbb{Z}$ denotamos:

$$\eta_m = \xi^m + \xi^{-m} = 2\cos\frac{2\pi m}{n}, \quad \nu_m = \xi^m - \xi^{-m} = 2\,\mathrm{sen}\,\frac{2\pi m}{n}.$$

Las siguientes fórmulas se verifican fácilmente:

$$\begin{aligned} \eta_n\eta_m &= \eta_{n+m} + \eta_{n-m} \\ \nu_n\nu_m &= \eta_{n+m} - \eta_{n-m} \\ \nu_m\eta_n &= \nu_{m+n} + \nu_{m-n}. \end{aligned}$$

Entonces

$$\begin{aligned} \alpha &= (b_1 - 1)(b_2 - 1) = (1 - b)a(1 + b)(1 - a^jb)a^i(1 + a^jb) \\ &= a^{i+1} - a^{i-1} + a^{-i-1} - a^{1-i} + a^{1-i-j} + a^{i-1-j} - a^{1+i-j} - a^{-1-i-j} + \\ &\quad (a^{1-i} + a^{i-1} - a^{1+i} - a^{-1-i} + a^{1+i+j} + a^{-1-i+j} - a^{-1+i+j} - a^{1-i+j})b \end{aligned}$$

y así

$$\begin{aligned} \chi_k(\alpha) &= \eta_{(i+1)k} - \eta_{(i-1)k} + \eta_{(-1-i)k} - \eta_{(1-i)k} + \\ &\quad \eta_{(1-i-j)k} + \eta_{(i-1-j)k} - \eta_{(1+i-j)k} - \eta_{(-1-i-j)k} \\ &= 2\nu_k\nu_{ik} + \eta_{-jk}(\nu_{(1-i)k} - \nu_{(1+i)k}) = \nu_k\nu_{ik}(2 - \eta_{jk}) \\ &= 8\,\mathrm{sen}\,\tfrac{2\pi k}{n}\,\mathrm{sen}\,\tfrac{2\pi ik}{n}(1 - \cos\tfrac{2\pi jk}{n}) = 16\,\mathrm{sen}\,\tfrac{2\pi k}{n}\,\mathrm{sen}\,\tfrac{2\pi ik}{n}\,\mathrm{sen}^2\,\tfrac{\pi jk}{n}. \end{aligned}$$

La existencia de un carácter con la propiedad requerida se sigue del siguiente Lema. El resto de esta sección se ocupa de su demostración. Desafortunadamente la demostración es más larga de lo que nos gustaría.

Nos gustaría agradecer aquí algunas útiles conversaciones con Víctor Jiménez sobre esta demostración.

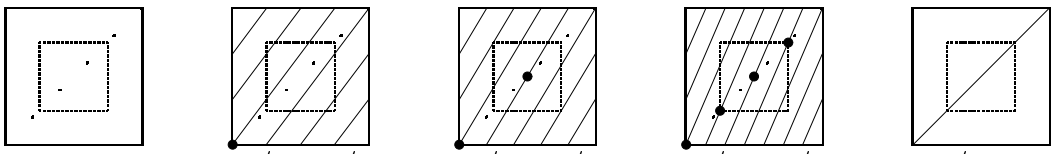
Lema 2.3.1 *Si i, j, n son enteros positivos tales que $1 \leq i, j < n$, $n \geq 3$ y $(n, i, j) \neq (6, 3, 1)$ entonces existe un entero k tal que*

$$\left| \operatorname{sen} \frac{2\pi k}{n} \operatorname{sen} \frac{\pi i k}{n} \operatorname{sen}^2 \frac{\pi j k}{n} \right| \geq \frac{1}{4}. \tag{2.1}$$

Demostración. Para todo número real a sean $s_a = \frac{2\pi a}{n}$ y $f_a : \mathbb{R} \to \mathbb{R}/2\pi\mathbb{Z} = S$ la aplicación definida por $f_a(x) = s_a x + 2\pi\mathbb{Z}$.

Sean i, j, n números enteros satisfaciendo las condiciones del Lema. Sin pérdida de generalidad podemos suponer que $i, j \leq \frac{n}{2}$, luego $s_i, s_j \leq \pi$. Sea $f = f_{i,j} : [0, n) \to T = S^2$ definida por $f(x) = (f_i(x), f_j(x))$. La imagen de f es una espiral en el toro T.

Identificamos S con $[0, 2\pi)$ y T con el cuadrado $[0, 2\pi)^2$, de manera que consideramos f_a como una aplicación $\mathbb{R} \to [0, 2\pi)$. Denotemos por D la diagonal de T y $V = \left[\frac{\pi}{2}, \frac{3\pi}{2}\right]^2$.



El primero de los dibujos anteriores representa T (el cuadrado grande), D (la linea de puntos) y V (el cuadrado pequeño). Los otros dibujos incluyen la imagen de f para distintos valores de j/i. Hemos marcado con puntos gordos los cortes de la imagen de f con la diagonal. Si $i = j$ (el último dibujo) todos los puntos de la diagonal son puntos gordos.

Recuérdese que $\lfloor x \rfloor$ (resp. $\lceil x \rceil$) denota el mayor (resp. menor) entero más pequeño (resp. más grande) que x.

Sean

$$W = \left[\frac{n}{8}, \frac{3n}{8}\right], \quad W_1 = \left[\left\lceil \frac{n}{8} \right\rceil, \left\lfloor \frac{3n}{8} \right\rfloor\right], \quad X = f^{-1}(D)$$

y consideremos las siguientes condiciones

(1) Existen $k_1, k_2 \in \mathbb{Z}$ tales que $|\operatorname{sen} f_i(k_1) \operatorname{sen} f_i(k_1/2) \operatorname{sen}^2 f_j(k_1/2)| \geq \frac{1}{4}$ y $|\operatorname{sen} f_i(k_1) \operatorname{sen}^2 f_i(k_1/2) \operatorname{sen} f_j(k_1/2)| \geq \frac{1}{4}$.

(2) Existen $k_1, k_2 \in \mathbb{Z} \cap W$ tales que $|\operatorname{sen} f_i(k_1/2) \operatorname{sen}^2 f_j(k_1/2)| \geq \frac{\sqrt{2}}{4}$ y $|\operatorname{sen}^2 f_i(k_2/2) \operatorname{sen} f_j(k_2/2)| \geq \frac{\sqrt{2}}{4}$.

(3) $f(\mathbb{Z} \cap W) \cap V \neq \emptyset$.

(4) $f(W_1) \cap D \cap V \neq \emptyset$.

La condición (1) es equivalente a la afirmación del Lema. Esta condición es introducida para obtener simetría en los papeles de i y j. Claramente (3) implica (2) y (2) implica (1). Demostremos ahora que (4) implica (3). Sea $t \in W_1$ tal que $f(t) \in V \cap D$. Entonces existe un entero l tal que $l \leq t \leq l+1$ y $l, l+1 \in W_1 \subseteq W$. Supongamos que $i \leq j$. Como $s_j \leq \pi$ y $\frac{\pi}{2} \leq f_j(t) \leq \frac{3\pi}{2}$, entonces

$$\frac{\pi}{2} \leq f_j(l) \leq f_i(l) \leq f_i(t) \leq \frac{3\pi}{2}$$

ó

$$\frac{\pi}{2} \leq f_i(t) \leq f_i(l+1) \leq f_j(l+1) \leq \frac{3\pi}{2}.$$

Luego (3) se verifica.

Ahora procedemos por reducción al absurdo. Supongamos que el Lema no es cierto y por lo tanto que no se verifican las condiciones (1) a (4). Por lo tanto desde ahora trabajaremos bajo las siguientes suposiciones:

(C1) Para todo $k \in \mathbb{Z}$, $|\operatorname{sen} f_1(k) \operatorname{sen} f_i(k/2) \operatorname{sen}^2 f_j(k/2)| < \frac{1}{4}$, o, para todo $k \in \mathbb{Z}$, $|\operatorname{sen} f_1(k) \operatorname{sen}^2 f_i(k/2) \operatorname{sen} f_j(k/2)| < \frac{1}{4}$.

(C2) Para todo $k \in \mathbb{Z}$, $|\operatorname{sen} f_i(k/2) \operatorname{sen}^2 f_j(k/2)| < \frac{\sqrt{2}}{4}$, o para todo $k \in \mathbb{Z}$, $|\operatorname{sen}^2 f_i(k/2) \operatorname{sen} f_j(k/2)| < \frac{\sqrt{2}}{4}$.

(C3) $f(\mathbb{Z} \cap W) \cap V = \emptyset$.

(C4) $f(W_1) \cap D \cap V = \emptyset$ o equivalentemente $W_1 \cap X \cap f^{-1}(V) \neq \emptyset$.

Una búsqueda exhaustiva con ordenador muestra que la única terna de enteros positivos (n, i, j) con $n \leq 200$ y $i, j \leq \frac{n}{2}$ para los que no hay un entero k satisfaciendo (2.1) es $(n, i, j) = (6, 3, 1)$; precisamente el caso excluido en el enunciado del Lema. Por lo tanto $n > 200$. Esto implica que

$$\left\lfloor \frac{n}{8} \right\rfloor \leq \frac{n}{8} + \frac{7}{8} < \frac{n}{8} + \frac{7}{8}\frac{n}{200} = \frac{207n}{1600}$$

y

$$\left\lfloor \frac{3n}{8} \right\rfloor \geq \frac{3n}{8} - \frac{7}{8} > \frac{3n}{8} - \frac{7}{8}\frac{n}{200} = \frac{593n}{1600},$$

es decir

$$[\frac{207n}{1600}, \frac{593n}{1600}] \subseteq W_1. \tag{2.2}$$

Nótese que debido a la condición (C4) y al hecho de que $s_i, s_j \leq \pi$ también se deduce fácilmente que $i \neq j$. Además, debido a la simetría de los papeles representados por i y j, también podemos suponer que $i < j$.

Introducimos la siguiente notación:

$$\begin{aligned} m &= \gcd(i,j) = |f^{-1}(0,0)| \\ v &= \frac{j-i}{m} = |D \cap \text{ Im } f| \\ \alpha &= \frac{n}{mv} \\ \theta &= f_i(\alpha)(= f_j(\alpha)). \end{aligned}$$

Entonces

$$\begin{aligned} X &= \{k\alpha : k = 0, 1, \ldots, mv-1\} \text{ y} \\ f(X) &= D \cap \text{Im } f = \{(\frac{2\pi k}{v}, \frac{2\pi k}{v}) : k = 0, 1, \ldots, v-1\} \text{ (los puntos gordos).} \end{aligned}$$

Está claro que $f(X)$ es un subgrupo aditivo cíclico de D de orden v y (θ, θ) es un generador de $f(X)$.

Como $f(X) \cap V = \text{Im } f \cap V \cap D$, la condición (C4) implica que

(C5) Si I es un intervalo tal que $f(I) = \text{Im } f$ entonces $f(X) \cap V \subseteq f((I \setminus W_1) \cap X)$.

Como $\alpha = \frac{n}{j-i} > 2$, todo intervalo de longitud ≤ 2 contiene como mucho un elemento de X y por lo tanto la condición (C4) implica que

$$\left|\left[\frac{n}{8}, \left\lceil\frac{n}{8}\right\rceil\right] \cap X\right| \leq 1, \quad \left|\left[\left\lfloor\frac{3n}{8}\right\rfloor, \frac{3n}{8}\right] \cap X\right| \leq 1 \tag{2.3}$$

y así $|W \cap X \cap f^{-1}(V)| \leq 2$.

Consideramos ahora los siguientes casos que se excluyen mutuamente: (1) $v \neq 1$ y $mv \neq 2$, (2) $v = 1$ y $m \geq 3$ y (3) $mv \leq 2$.

Caso 1: $v \neq 1$ y $mv \neq 2$.

Primero demostraremos que $m \leq 4$. Obsérvese que

$$|f(X) \cap V| = \begin{cases} \frac{v}{2} + 1 & \text{si} \quad v \equiv 0 \bmod 4 \\ \frac{v}{2} & \text{si} \quad v \equiv 2 \bmod 4 \\ \frac{v+1}{2} & \text{si} \quad v \equiv 3 \bmod 4 \\ \frac{v-1}{2} & \text{si} \quad v \equiv 1 \bmod 4 \end{cases} \tag{2.4}$$

que es diferente de 0. Sea I el intervalo centrado en $\frac{n}{4}$ y de longitud $\frac{n}{m}$. Como $f(I) = \operatorname{Im} f$, la condición (C5) implica que I no está contenido en W_1 y esto implica que $m \leq 4$.

En segundo lugar demostramos que $m \neq 4$. Supongamos lo contrario, esto es supongamos que $v \neq 1$ y $m = 4$. Como W tiene longitud $\frac{n}{m} = \frac{n}{4}$, obtenemos que $f(W) = \operatorname{Im} f$ y por (C5) tenemos que $f(X) \cap V \subseteq f((W \setminus W_1) \cap X)$. Luego $|f(X) \cap V| \leq 2$, por (2.3). Como por hipótesis $v \neq 1$, obtenemos fácilmente de (2.4) que $v = 2, 3$ ó $v = 5$. Si $v = 3$ ó $v = 5$ entonces $X \cap W = \{\frac{2n}{12}, \frac{3n}{12}, \frac{4n}{12}\}$ ó $X \cap W = \{\frac{3n}{20}, \frac{4n}{20}, \frac{5n}{20}, \frac{6n}{20}, \frac{7n}{20}\}$ respectivamente. De (2.2) deducimos que $X \cap W \subseteq W_1$ y así $f(X) \cap V = \emptyset$, una contradicción. Luego $v = 2$ y por lo tanto $f(\frac{n}{8}) = (\pi, \pi) = f(\frac{3n}{8})$. Por la condición (C3) n no es un múltiplo de 8. Debido a (C3) sabemos que $f(\lceil \frac{n}{8} \rceil) \notin V$ luego $f_j(\lceil \frac{n}{8} \rceil) > \frac{3\pi}{2}$. Así

$$\frac{\pi}{2} < f_j(\left\lceil \frac{n}{8} \right\rceil) - f_j(\frac{n}{8}) = s_j\left(\lceil n/8 \rceil - n/8\right) \leq \pi \left(\left\lceil \frac{n}{8} \right\rceil - \frac{n}{8}\right)$$

y por lo tanto $n \equiv q \bmod 8$ con $q = 1, 2$ ó 3. Esto implica que para $k = \lfloor \frac{n}{8} \rfloor$ tenemos que

$$\frac{5\pi}{8} \leq \pi - \frac{q\pi}{8} = f_j(k) < f_i(k) < \pi$$

y

$$\frac{\pi}{4} > f_1(k) = \frac{2\pi \frac{n-q}{8}}{n} = \frac{\pi}{4} - \frac{\pi q}{4n} \geq \frac{\pi}{4} - \frac{3\pi}{800} = \frac{197\pi}{800}.$$

Consecuentemente,

$$\left| \operatorname{sen} f_1(k) \ \operatorname{sen} \frac{f_i(k)}{2} \ \operatorname{sen}^2 \frac{f_j(k)}{2} \right| \geq \operatorname{sen} \frac{197\pi}{800} \ \operatorname{sen}^3 \frac{5\pi}{8} \geq \frac{1}{4}$$

y

$$\left| \operatorname{sen} f_1(k) \ \operatorname{sen}^2 \frac{f_i(k)}{2} \ \operatorname{sen} \frac{f_j(k)}{2} \right| \geq \operatorname{sen} \frac{197\pi}{800} \ \operatorname{sen}^3 \frac{5\pi}{8} \geq \frac{1}{4}$$

en contradicción con (C1).

En tercer lugar demostramos que $m \neq 3$. Supongamos lo contrario, esto es, supongamos que $m = 3$. Sea $I = \left[0, \frac{n}{3}\right]$. Entonces $f(X) \cap V \subseteq f(\left[0, \lceil \frac{n}{8} \rceil\right] \cap X)$, por (C5). Obsérvese que $\left[0, \frac{n}{8}\right] \cap X = \{\frac{kn}{3v} \mid 1 \leq k \leq \frac{3v}{8}\}$ tiene $\lfloor \frac{3v}{8} \rfloor$ elementos. Así (2.3) implica que

$$|f(X) \cap V| \leq |X \cap (0, \left\lceil \frac{n}{8} \right\rceil)| \ \leq \ \left\lfloor \frac{3v}{8} \right\rfloor + 1 \tag{2.5}$$

Un análisis de las desigualdades (2.4) y (2.5) nos lleva a concluir que $v = 2, 3, 5, 6$ ó 9 y en todos los casos $|f(X) \cap V| > \lfloor \frac{3v}{8} \rfloor$. Concluimos que $X \cap \left[\frac{n}{8}, \lceil \frac{n}{8} \rceil\right]$ tiene un único elemento. Este elemento es $\frac{n}{6}$ si $v = 2$, $\frac{2n}{9}$ si $v = 3$, $\frac{2n}{15}$ si $v = 5$, $\frac{3n}{18}$ si $v = 6$

y $\frac{4n}{27}$ si $v = 9$. El número más pequeño listado anteriormente es $\frac{2n}{15}$ y así de (2.2) tenemos que

$$\frac{2n}{15} \leq \left\lceil \frac{n}{8} \right\rceil < \frac{207n}{1600},$$

una contradicción.

Concluimos que $m \leq 2$, de donde se deduce que $f(\frac{n}{4}) \neq (0,0)$. Si mv fuera múltiplo de 4, $f(\frac{n}{4})$ pertenecería a $f(W_1) \cap D$ y como $f(\frac{n}{4}) \neq (0,0)$ necesariamente $f(\frac{n}{4})$ pertenecería a $f(W_1) \cap V \cap D$ en contra de $(C4)$. Por tanto mv no es múltiplo de 4.

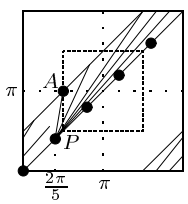
Consideremos las aplicaciones $g : [0,n) \to \mathbb{R}$ y $\bar{g} : [0,n) \to T$ dadas por $g(t) = \frac{\theta}{\alpha}t$ y $\bar{g}(t) = (g(t) + 2\pi\mathbb{Z}, g(t) + 2\pi\mathbb{Z})$. La imagen de $\bar{g}$ es D y $\bar{g}(t) = f(t)$ para todo $t \in X$. Por la condición (C4), tenemos que

$$\bar{g}(X \cap W_1) \cap V = \emptyset. \tag{2.6}$$

Supongamos que $\frac{\pi}{2} \leq \theta \leq \frac{3\pi}{2}$. Entonces, por la condición (C4), $\alpha = \frac{n}{mv} \notin W_1$ y como $mv > 2$, $\alpha < \left\lceil \frac{n}{8} \right\rceil$. Como 4 no divide a mv tenemos que $mv \geq 9$. La restricción hecha sobre θ fácilmente nos conduce a que si $W_1 \cap X$ tiene al menos tres elementos, entonces $W_1 \cap X \cap f^{-1}(V) \neq \emptyset$, contradiciendo (C4). Luego tenemos que $|W_1 \cap X| \leq 2$. Así la longitud del intervalo W_1 es como mucho 2α y como mínimo $\frac{n}{4} - 2$. Por lo tanto $\frac{2n}{9} \geq 2\alpha \geq \frac{n}{4} - 2$ y esto implica que $n \leq 72$, una contradicción.

Sólo queda tratar con la situación $\theta < \frac{\pi}{2}$ ó $\theta > \frac{3\pi}{2}$. Trataremos $\theta < \frac{\pi}{2}$ (para el otro caso se procede de manera similar). En tal caso, claramente $v \geq 4$. Como 4 no divide a mv se sigue que $v \geq 5$ y $v \neq 8$. Si $v = 6$, entonces $\frac{n}{3} \in W_1 \cap X$ y $\bar{g}(\frac{n}{3}) \in V$; si $v = 7$ y $m = 1$ entonces $\frac{2n}{7} \in W_1 \cap X$ y $\bar{g}(\frac{2n}{7}) \in V$; y si $v = 7$ y $m = 2$ entonces $\frac{n}{7} \in W_1 \cap X$ y $\bar{g}(\frac{n}{7}) \in V$. Estos tres casos no llevan a contradicción con (2.6) por lo tanto $v = 5$ ó $v \geq 9$.

Supongamos primero que $v = 5$. Si $m = 2$, entonces $2\alpha = \frac{n}{5} \in W_1 \cap X$ y $\bar{g}(2\alpha) \in V$, de nuevo una contradicción con (2.6). Luego $m = 1$ y $g(\alpha) = \frac{2\pi}{5}$. Por la condición (C3) tenemos que $f(\mathbb{Z} \cap I) \cap V = \emptyset$, donde $I = \left[\frac{n}{5}, \frac{n}{4}\right]$. Además, para todo $x \in I$, $f_i(x) \leq f_j(x) \leq f_i(x) + \frac{\pi}{2}$, esto es $f(I)$ está en la banda entre la diagonal y la paralela de la diagonal que pasa por el punto $A = (\frac{\pi}{2}, \pi)$. (Nótese que esta última tienen una continuación en la esquina inferior derecha tal y como muestra la siguiente figura.)



Los puntos sobre la diagonal representan los elementos de $f(X)$ y $f(\alpha) = (\frac{2\pi}{5}, \frac{2\pi}{5})$ está etiquetado con la letra P. Las líneas que salen de P representan varias posibilidades para $f(I)$. Todas ellas salen de P y acaban en la linea que es paralela a la diagonal que pasa por A. La longitud del intervalo $f_i(I)$ es al menos $\frac{\pi}{10}$, y la igualdad se verifica si y sólo si $i = 1$. Si $i = 1$ entonces $f\left(\frac{n}{4}\right) = A$ y $f(I)$ es el segmento que une P con A. Entonces $f\left(\left\lceil \frac{n}{4} \right\rceil\right) \in V$ contradiciendo (C3). Por lo tanto $i \neq 1$ y así $f(I)$ interseca el interior de V y de hecho $f\left[\frac{n}{5}, \frac{9n}{40}\right]$ interseca V. Esto es porque la longitud de $f_i\left[\frac{n}{5}, \frac{9n}{40}\right]$ es $\frac{\pi i}{20} \geq \frac{\pi}{10}$, y por lo tanto existe $t \in \left[\frac{n}{5}, \frac{9n}{40}\right]$ con $f_i(t) = f_i\left(\frac{n}{5}\right) + \frac{\pi}{10} = \frac{\pi}{2}$ y para tal t tenemos que $f(t) \in V$ (véase la figura). Sea t el menor elemento de I tal que $f(t) \in V$ y sea $k = \lfloor t \rfloor$. Entonces $k + 1 \in I$ y así $f(k + 1) \notin V$. Esto implica que $f_i(k + 1) > \pi$ (véase la figura anterior) y por lo tanto $\frac{\pi}{2} < f_i(k+1) - f_i(k)$, de manera que la pendiente de f_i es mayor que $\frac{\pi}{2}$. Luego

$$\frac{\pi}{2} = \frac{2\pi}{5} + \frac{\pi}{10} \leq f_i(\lfloor \alpha \rfloor + 1) \leq f_j(\lfloor \alpha \rfloor + 1) \leq \frac{3\pi}{2}$$

por lo tanto $f(\lfloor \alpha \rfloor + 1) \in V$, una contradicción con (C3).

Finalmente, supongamos que $v \geq 9$ y recordemos que estamos suponiendo que $\theta \leq \frac{\pi}{2}$. Sea l el primer entero no negativo tal que $g(l\alpha) \geq \pi/2$ y p el menor entero tal que $g((l+p)\alpha) > 3\pi/2$. Nótese que la primera desigualdad implica que $(l-1)\alpha < \frac{n}{4}$. Como $\alpha \leq \frac{n}{9}$ tenemos que por (2.2) $l\alpha \leq \frac{n}{3} < \left\lfloor \frac{3n}{8} \right\rfloor$. Como $\theta < \pi/2$, tenemos que $l, p \geq 2$.

Aseguramos que $p = 2$. Supongamos que $p \geq 3$. Sea $\beta = (l + p - 1)\alpha$. Entonces $\overline{g}(\beta) \in V$ y por la condición (2.6), $\beta \notin W_1$. Como por suposición, $p \geq 3$ y además $g(l) < \frac{\pi}{2}$ y $g((l + p)\alpha) > \frac{3\pi}{2}$ se sigue que $g(\beta) > \frac{3\pi}{2} - \frac{\pi}{3} = \frac{7\pi}{6}$. Así que la longitud $g[0, \beta]$ es al menos $\frac{7\pi}{6}$. Si $\beta \leq \left\lceil \frac{n}{8} \right\rceil$, entonces la longitud de $g(W_1)$ es al menos

$$\frac{7\pi}{6} \frac{\left\lfloor \frac{3n}{8} \right\rfloor - \left\lceil \frac{n}{8} \right\rceil}{\left\lceil \frac{n}{8} \right\rceil} \geq \frac{7\pi}{3} \frac{n-6}{n+7} \geq 2\pi.$$

Esto implica que $\bar{g}(W_1 \cap X) \cap V \neq \emptyset$, contradiciendo (2.6). Luego $\beta > \left\lceil \frac{n}{8} \right\rceil$ y como además $\beta \notin W_1$, deducimos que $\beta > \left\lfloor \frac{3n}{8} \right\rfloor$. Sea k el mayor entero no negativo tal que $(l + k)\alpha \leq \left\lfloor \frac{3n}{8} \right\rfloor$ (recuérdese que $l\alpha < \left\lfloor \frac{3n}{8} \right\rfloor$). Así $k < p - 1$. Como $f((l + k)\alpha) \in V$ de (2.6) tenemos que $(l + k)\alpha \notin W_1$ y de aquí deducimos que $(l + k)\alpha < \left\lceil \frac{n}{8} \right\rceil$. Consecuentemente,

$$\left\lfloor \frac{3n}{8} \right\rfloor < (l + k + 1)\alpha \leq 2(l + k)\alpha \leq 2\left\lceil \frac{n}{8} \right\rceil \leq \frac{n+7}{4} \leq \left\lfloor \frac{3n}{8} \right\rfloor$$

una contradicción.

Luego tenemos que $p = 2$. Consecuentemente, $\frac{\pi}{2} + 3\theta > \frac{3\pi}{2}$ y así $\theta > \frac{\pi}{3}$. Luego, $g(2\alpha) > \frac{2\pi}{3} > \frac{\pi}{2}$. De este modo $l = 2$ y $\bar{g}(3\alpha) \in V$ pues $\theta < \frac{\pi}{2}$. Por lo tanto $3\alpha \notin W_1$. Como $3\alpha \leq \frac{n}{3}$ tenemos que $3\alpha < \left\lceil \frac{n}{8} \right\rceil$. Como también $g(4\alpha) = 4\theta > \frac{3\pi}{2}$,

$g(3\alpha) = 3\theta \geq \frac{9\pi}{8}$ y por lo tanto $g(W_1)$ es al menos

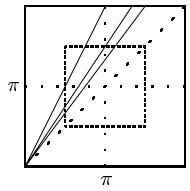
$$\frac{9\pi}{8}\frac{\lfloor\frac{3n}{8}\rfloor - \lceil\frac{n}{8}\rceil}{\lceil\frac{n}{8}\rceil} \geq \frac{9\pi}{4}\frac{n-6}{n+7} \geq 2\pi.$$

consecuentemente, $\bar{g}(W_1 \cap X) \cap V \neq \emptyset$, de nuevo una contradicción.

Esto termina la demostración del Caso 1. Nos vemos en la lamentable obligación de avisar que éste era el caso fácil.

Caso 2: $v = 1$ y $m \geq 3$.

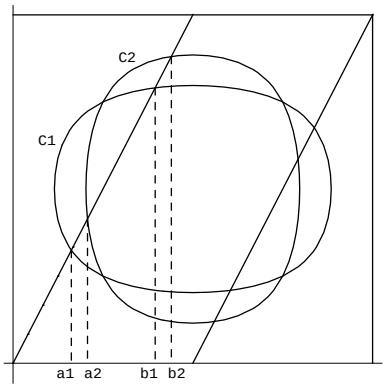
Sea $\lambda = \frac{i}{m} = \frac{j}{m} - 1$, un entero positivo. La pendiente de f es $\frac{j}{i} = 1 + \frac{1}{\lambda}$. La figura siguiente muestra la imagen $\left[0, \frac{n}{j}\right]$ mediante f para $\lambda = 1, 2$ y 3. Cuanto mayor sea λ más cercana estará esta imagen a la diagonal D.



Supongamos que $m \geq 4$. Sea t_0 el mayor elemento de $\left[0, \frac{n}{4}\right] \cap X$ y t_1 el elemento siguiente de X. Nótese que $t_1 - t_0 = \frac{n}{m} \leq \frac{n}{4}$ y así $\frac{t_0+t_1}{2} = t_0 + \frac{t_1-t_0}{2} \leq \frac{3n}{8}$. Claramente $t_0 = \lfloor\frac{m}{4}\rfloor \frac{n}{m}$. Si $m \geq 6$ entonces $t_0 \geq \frac{m-3}{4}\frac{n}{m} \geq \frac{n}{8}$ y si $m = 4$ ó 5, entonces $t_0 = \frac{n}{m} \geq \frac{n}{5}$. Por lo tanto, el intervalo $I = \left[t_0, \frac{t_0+t_1}{2}\right]$ está contenido en W. Debido a la condición (C3) tenemos que $f(I \cap \mathbb{Z}) \cap V = \emptyset$. Sea $k = \lfloor t_0 \rfloor + 1 \in W$. Como $i, j \leq \frac{n}{2}$, $\alpha \geq 2$ y por lo tanto la longitud del I es mayor o igual que 1 tenemos que $k \in W$.Entonces $0 < f_j(k) \leq \pi$ y así $f_i(k) < \frac{\pi}{2}$ (la figura anterior ayuda aquí). Sea p el menor entero no negativo tal que $f_i(k+p) \geq \frac{\pi}{2}$. Como $\pi \in f_i(I)$ (pués al menos medio círculo está cubierto por $f_i(I)$), tenemos que $k + p \in I \cap \mathbb{Z}$ y así $f_j(k+p) > \frac{3\pi}{2}$.

Supongamos que $\lambda \neq 1$, es decir, de la posibles líneas representando $f\left[0, \frac{n}{j}\right]$ en la figura anterior, excluimos la que está más a la izquierda. Entonces una mirada a la figura muestra que de $f_j(k+p) > \frac{3\pi}{2}$ se deduce que $f_i(k+p) > \pi$. Luego la pendiente s_i de f_i es mayor que $\frac{\pi}{2}$. De esto se sigue que $p = 1$. Luego $f_j(k+1) > \frac{3\pi}{2}$. Como $s_j \leq \pi$ tenemos que $f_j(k) > \frac{\pi}{2}$. Un argumento similar hacia atrás muestra que $\pi \leq f_j(\lceil t_0 \rceil - 1) < \frac{3\pi}{2}$. Consecuentemente, $|f_j(\lfloor t_0 \rfloor + 1) - f_j(\lceil t_0 \rceil - 1)| > \pi$. Usando de nuevo que $s_j \leq \pi$ tenemos que la longitud del intervalo $[\lceil t_0 \rceil - 1, \lfloor t_0 \rfloor + 1]$ es mayor que 1 y así t_0 es un entero. Por lo tanto $\frac{\pi}{2} < f_i(k+1) - f_i(k) = f_i(t_0+1) - f_i(t_0) = f_i(k) < \frac{\pi}{2}$, una contradicción.

Luego $\lambda = 1$ y así $j = 2i$ y $m = i$. La siguiente figura representa la imagen de f y las curvas C_1 y C_2 definidas por las ecuaciones $\operatorname{sen}(x/2)\operatorname{sen}^2(y/2) = \frac{\sqrt{2}}{4}$ y $\operatorname{sen}^2(x/2)\operatorname{sen}(y/2) = \frac{\sqrt{2}}{4}$ respectivamente.



Si (x, y) está en la región R_1 limitada por la curva C_1 entonces $\operatorname{sen}(x/2)\operatorname{sen}^2(y/2) \geq \frac{\sqrt{2}}{4}$ y si (x, y) está en la región R_2 limitada por C_2 entonces $\operatorname{sen}^2(x/2)\operatorname{sen}(y/2) \geq \frac{\sqrt{2}}{4}$. Sean a_i y b_i las primeras coordenadas de los puntos de intersección de la primera parte de la imagen de f con C_i $(i = 1, 2)$. Debido a la condición (C2), no existen enteros k_1 y k_2 en el intervalo W tales que $f(k_i) \in R_i$ para ambos $i = 1, 2$. Como $I \subseteq W$ y $f(I)$ cubre el tramo de la izquierda de la imagen de f se sigue fácilmente que $s_i > \text{mín}(b_1 - a_1, b_2 - a_2)$. Calculando estas intersecciones obtenemos que

$$a_1 \leq 1{,}019, \quad a_2 \leq 1{,}302, \quad b_1 \geq 2{,}484, \quad b_2 \geq 2{,}766.$$

Luego $s_i > 1{,}464$ y así $\frac{i}{n} = \frac{S}{2\pi} \geq 0{,}233$. Como $n > 200$ tenemos que $i > 46$ y de esta manera tenemos que $\alpha = \frac{n}{m} = \frac{n}{i} < \frac{n}{46}$. Se sigue que $\frac{n}{4} - \frac{n}{46} < t_0 < t_1 < \frac{n}{4} + \frac{n}{46}$. Consecuentemente, para todo $t \in [t_0, t_1]$ tenemos que $\operatorname{sen}\frac{2\pi t}{n} \geq \operatorname{sen}\frac{21\pi}{46} > 0{,}9$. Sea C_1' la curva definida por $\operatorname{sen}(x/2)\operatorname{sen}^2(y/2) = \frac{1}{4\cdot(0{,}9)}$ y C_2' la curva definida por $\operatorname{sen}^2(x/2)\operatorname{sen}(y/2) = \frac{1}{4\cdot(0{,}9)}$. Sea a_i' y b_i' las primeras componentes de los puntos de intersección de C_i' con la primera parte de la imagen de f. Entonces

$$a_1' \leq 0{,}912, \quad a_2' \leq 1{,}165, \quad b_1' \geq 2{,}573, \quad b_2' \geq 2{,}854.$$

Debido a la condición (C1), obtenemos de la misma manera que antes que $s_j > 2\,\text{mín}(b_1' - a_1', b_2' - a_2') \geq 3{,}316 > \pi$, una contradicción.

Luego hemos demostrado que $m = 3$. Sea $t_0 = \left\lceil \frac{n}{3} \right\rceil$ y $k = t_0 - 1$. De forma análoga a la situación anterior (esto es, para $m \geq 4$), podemos llegar a contradicción argumentando hacia atrás en el intervalo $\left[\frac{n}{6}, \frac{n}{3}\right]$.

Caso 3: $mv \leq 2$.

Este es el caso más difícil pues no podemos apoyarnos como en los casos anteriores en algún $t \in W$ tal que $f(t)$ tenga alguna propiedad útil, por ejemplo $f(t) \in D$ ó $f(t) = (0, 0)$. En efecto los únicos valores de $t \in [0, n]$ para los que sucede una de estas dos cosas son $t = 0$ y $t = \frac{n}{2}$, ambos lejos de W. Vamos a evitar esta dificultad apoyándonos en el punto t_0 que es igual a $\frac{n}{4}$ si $mv = 1$ e igual a $\frac{n}{8}$ si $mv = 2$

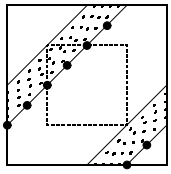
Sea $I = [t_0, 2t_0] \cap W$ entonces

$$f(t_0) = \begin{cases} \left(0, \frac{\pi}{2}\right), \left(\frac{\pi}{2}, \pi\right), \left(\pi, \frac{3\pi}{2}\right) \text{ o } \left(\frac{3\pi}{2}, 0\right) & \text{si } v = 1 \\ \left(\frac{\pi}{4}, \frac{3\pi}{4}\right), \left(\frac{3\pi}{4}, \frac{5\pi}{4}\right), \left(\frac{5\pi}{4}, \frac{7\pi}{4}\right) \text{ o } \left(7\frac{\pi}{4}, \frac{\pi}{4}\right) & \text{si } v = 2 \end{cases}$$

Para todo $t \in I$, tenemos que

$$\frac{\pi}{2} \leq f_j(t) - f_i(t) = \frac{2\pi t}{\alpha} \leq \pi,$$

es decir, $f(I)$ está en la parte sombreada de la siguiente figura donde los valores posibles para $f(t_0)$ han sido representados por círculos en negrita.



Además la pendiente s_{j-i} de la función $f_j - f_i$ es $\frac{2\pi(j-i)}{n} = \frac{2vm\pi}{n} < \frac{\pi}{50}$ (debido a la suposición $n > 200$).

Los posibles valores de m y $f(t_0)$ nos conducen a 12 casos diferentes. Usando argumentos similares se demuestra que cada uno de estos casos nos llevan a contradicción, y así acabamos la demostración. Es crucial en todos estos argumentos que ocurre en "un poco" después del instante t_0. En realidad los argumentos en los 12 casos son muy similares y tediosos Ilustraremos el método para $m = 2$ y $f(t_0) = (0, \frac{\pi}{2}) = O$, por lo tanto $v = 1$. El lector que haya llegado a este punto de la demostración no tendrá dificultad en variar ligeramente los argumentos que damos a continuación para este caso de manera que sirvan para los otros 11 casos.

Sea $k = \lceil t_0 \rceil \leq t_o + \frac{7}{8}$. Como $s_i \leq \pi$ y $s_{j-i} \leq \frac{\pi}{50}$ se sigue que

$$0 \leq f_i(k) \leq \frac{7\pi}{8}$$

y

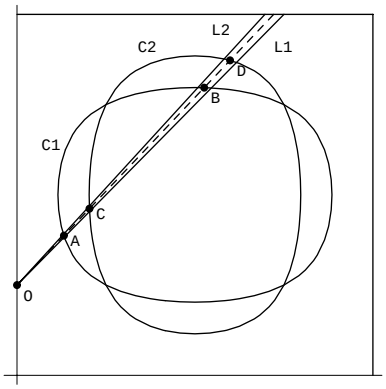
$$\frac{\pi}{2} = f_j(t_0) - f_i(t_0) \leq f_j(k) - f_i(k) = (f_j - f_i)(t_0) + (f_j - f_i)(k - t_0) \leq \frac{\pi}{2} + \frac{\pi}{50} = \frac{13\pi}{25}.$$

Luego $\frac{\pi}{2} \leq f_j(k) \leq \frac{7\pi}{8} + \frac{13\pi}{25} < \frac{3\pi}{2}$. Así, por la condición (C3) obtenemos que $f_i(k) < \frac{\pi}{2}$. Sea l el primer entero mayor que t_0 tal que $f_i(l) \geq \frac{\pi}{2}$. Aseguramos que $f_i(l) \geq \frac{3\pi}{4}$. Esto es fácil si $l \geq \frac{3n}{16}$, por que $m = 2$ divide a i y entonces $f_i(l) \geq \frac{2\pi i}{n}\frac{3n}{16} \geq \frac{3\pi}{4}$, tal y como deseábamos. Luego supongamos que $l < \frac{3n}{16}$ y $f_i(l) < \frac{3\pi}{4}$. Entonces $f_j(l) = (f_j - f_i)(l) + f_i(l) < \frac{4\pi}{n}\frac{3n}{16} + \frac{3\pi}{4} = \frac{3\pi}{2}$. En cualquier caso

esto nos lleva a contradicción con la condición (C3). Esto demuestra lo asegurado $f_i(l) \geq \frac{3\pi}{4}$. Como $f_i(l-1) < \frac{\pi}{2}$ y $f_i(l) \geq \frac{3\pi}{4}$ se sigue que $s_i \geq \frac{\pi}{4}$, y así obtenemos que $l \leq k+2$. Si la pendiente de la imagen de f es S, entonces

$$\begin{aligned} 1 &< S = \tfrac{(f_j(l)-f_j(t_0))}{(f_i(l)-f_i(t_0))} = 1 + \tfrac{(f_j(l)-f_j(t_0))-(f_i(l)-f_i(t_0))}{(f_i(l)-f_i(t_0))} = 1 + \tfrac{s_{j-i}(l-t_0)}{f_i(l)} \\ &< 1 + \tfrac{\frac{\pi}{50}(2+\frac{7}{8})}{\frac{3\pi}{4}} = \tfrac{323}{300} = S_{\text{máx}}. \end{aligned}$$

Sean a y b los dos primeros elementos de I tales que $A = f(a) = (A_1, A_2)$ y $B = f(b) = (B_1, B_2)$ pertenecen a la curva C_1 con ecuación $\operatorname{sen}(x/2)\operatorname{sen}^2(y/2) = \frac{\sqrt{2}}{4}$, y sean c y d los dos primeros elementos de I tales que $C = f(c) = (C_1, C_2)$ y $D = f(d) = (D_1, D_2)$ pertenecen a la curva C_2 con ecuación $\operatorname{sen}^2(x/2)\operatorname{sen}(y/2) = \frac{\sqrt{2}}{4}$. La figura siguiente representa las curvas C_1 and C_2 y las líneas L_1 y L_2 que pasan por O de pendientes 1 y S_{max} respectivamente.



La imagen $f([t_0, t_0+\epsilon])$ de un intervalo $[t_0, t_0+\epsilon]$ por f cae en la región entre L_1 y L_2. Calculando la intersección de las rectas L_1 y L_2 con C_1 y C_2 se deduce que

$$\begin{aligned} 0{,}82 < \;& A_1 \;< 0{,}84 \\ 1{,}27 < \;& C_1 \;< 1{,}29 \\ 3{,}19 < \;& B_1 \;< 3{,}44 \\ 3{,}65 < \;& D_1 \;< 3{,}88 \end{aligned}$$

La condición (C2) implica que $f_i(l-1) < A_1$ y $B_1 < f_i(l)$, ó $f_i(l-1) < C_1$ y $D_1 < f_i(l)$. Luego $l - 1 - t_0 = \frac{(l-1)-t_0}{l-(l-1)} \leq \text{máx}\{\frac{A_1}{B_1-A_1}, \frac{C_1}{D_1-C_1}\} \leq 0{,}6$. En particular, $(l-1) - t_0 < 1$. Como también $l, k \in \mathbb{Z}$ y $t_0 \leq k \leq l-1$ obtenemos que $l = k+1$ y $\lceil t_0 \rceil - t_0 = k - t_0 < 0{,}6$, así que $n \not\equiv 1, 2, 3 \bmod 8$.

Argumentando de forma análoga en el intervalo $\left[\frac{5n}{8}, \frac{6n}{8}\right]$ (nótese que $f(\frac{5n}{8}) = 5f(t_0) = O$) deducimos que $5n \not\equiv 1, 2, 3 \bmod 8$, así que $n \not\equiv 5, 7 \bmod 8$. Si $n \equiv 0 \bmod 8$ entonces $f(l) \in V$ contradiciendo (C3). Concluimos que $n \equiv 4 \bmod 8$ o $n \equiv 6 \bmod 8$.

La condición (C2) implica que $f_i(k) < A_1$ y $f_i(k+1) > B_1$, ó $f_i(k) < C_1$ y $f_i(k+1) > D_1$. Por lo tanto $s_i > \text{mín}(B_1 - A_1, D_1 - C_1) \geq 2{,}35$.

Supongamos que $n \equiv 4 \bmod 8$. Entonces $f_i(k) = s_i/2 > 2{,}35/2 > A_1$ y así $f_i(k) < C_1$ y $f_i(k+1) > D_1$. Lo primero implica que $s_i < 2C_1 < 2{,}58$ y lo segundo que $s_i > \frac{2D_1}{3} > 2{,}43$. Por lo tanto, tenemos que

$$2\pi + \frac{\pi}{2} < \frac{7 \cdot 2{,}43}{2} < f_i(k+3) = \frac{7s_i}{2} < \frac{7 \cdot 2{,}58}{2} < 2\pi + \frac{3\pi}{2}$$

y

$$2\pi + \tfrac{\pi}{2} < \tfrac{7\cdot 2{,}43}{2} + \tfrac{\pi}{2} < f_i(k+3) + \tfrac{\pi}{2} < f_j(k+3) < f_i(k+3) + \tfrac{\pi}{2} + \tfrac{7\pi}{2}\tfrac{\pi}{50} <$$

$$\tfrac{7\cdot 2{,}58}{2} + \tfrac{\pi}{2} + \tfrac{7}{2}\tfrac{\pi}{50} < 2\pi + \tfrac{3\pi}{2}.$$

Luego $f(k+3) \in V$ lo que nos lleva a contradicción con (C3).

Así $n \equiv 6 \bmod 8$. Entonces $5s_i/4 = f_i(k+1) > B_1 > 3{,}19$, luego $s_i > 2{,}55$. Sea $h = \left\lceil \frac{n}{4} \right\rceil = \frac{n+2}{4}$. Entonces $\frac{\pi}{2} < f_1(h) = \frac{\pi(n+2)}{2n} < \frac{\pi}{2} + \frac{\pi}{200} = \frac{102\pi}{200}$, $1{,}27 < s_i/2 = f_i(h) < \frac{\pi}{2}$ y $\pi < f_j(h) \leq f_i(h) + \pi + \frac{\pi}{100}$, luego

$$\text{mín}\{|\operatorname{sen} f_1(h) \operatorname{sen} f_i(h/2) \operatorname{sen}^2 f_{j/2}(h/2)|, |\operatorname{sen} f_1(h) \operatorname{sen}^2 f_i(h/2) \operatorname{sen} f_{j/2}(h/2)|\} \geq$$

$$\operatorname{sen} \tfrac{102\pi}{200} \operatorname{sen}^2 \tfrac{1{,}27}{2} \operatorname{sen} \tfrac{(1{,}27 + 101\pi/100)}{2} > \tfrac{1}{4},$$

lo que nos lleva a contradicción con (C1). □

2.4. Puntos libres y unidades bicíclicas

De las secciones 2 y 3 de este capítulo esta claro que el problema de obtener grupos libres generados por dos unidades bicíclicas se puede reducir a menudo a determinar cuando un grupo generado por dos matrices dos por dos es un grupo libre. En particular, con la notación de la Proposición 2.2.6, para asegurar que el grupo generado por $G = \langle 1+a, 1+b \rangle$ es libre de rango 2 es suficiente demostrar que existe un homomorfismo $\rho : A \to M_2(\mathbb{C})$ tal que las dos matrices $\rho(a)$ y $\rho(b)$ generan un grupo libre de rango 2. Identificando $M_2(K)$ con el anillo de endomorfismos de K^2 y después de un cambio de variable, si $\rho(ab)$ no es nilpotente, después de un cambio de base en K^2 podemos suponer que

$$\rho(a) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \text{ y } \rho(b) = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$$

generan un grupo libre, donde $2\lambda = \operatorname{tr}(\rho(ab)) \in \mathbb{C}$ (ver la demostración del Lema 2.2.5). Si este es el caso se dice que λ es un punto libre [2]. Hasta ahora nosotros

hemos usado el Teorema de Sanov (Teorema 14.2.1 [37]) y que es equivalente al Teorema 2.2.4, que afirma que un número complejo de módulo por lo menos 2 es un punto libre. El problema de decidir cuando un número complejo es un punto libre es un tema bastante activo de investigación. Para muchos números complejos se ha determinado si son puntos libres o no y muchos artículos se han escrito sobre este tema. A modo de ejemplo se sabe que λ es un punto libre en cada uno de los siguientes casos:

(1) $\lambda \in \mathbb{C}$ está fuera de los círculos unidad centrados en $-1, 0$ y 1 [9].

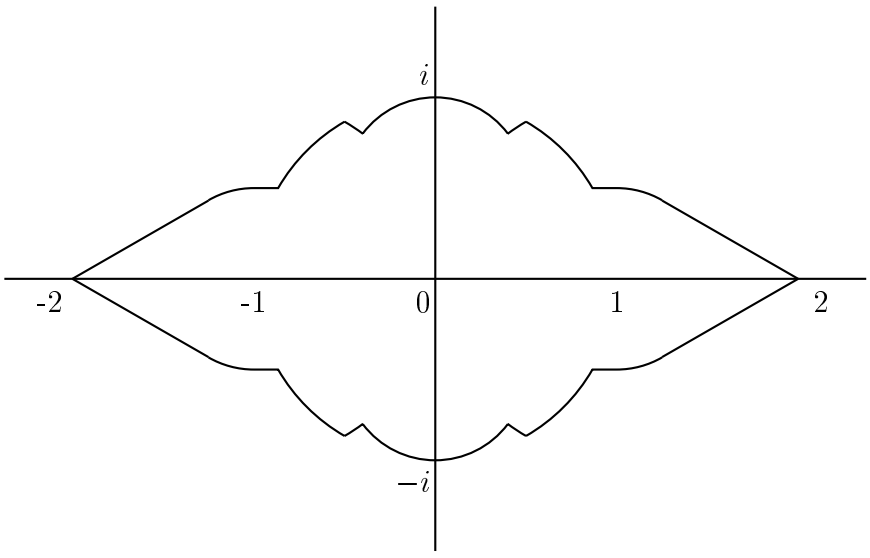
(2) $\lambda \in \mathbb{C}$ está fuera del círculo abierto de radio $\frac{1}{2}$ y centrado en $\frac{i}{2}$ y $\frac{-i}{2}$ y fuera del círculo unidad centrado en -1 y 1 [44].

(3) $\lambda \in \mathbb{C}$ está fuera de la envolvente convexa que contiene el círculo unidad centrado en el origen y los puntos ± 2 [44].

(4) $\lambda \in \mathbb{C}$ satisface $|\lambda - 1| > \frac{1}{2}$ y $1 \leq |Re(\lambda)| < \frac{5}{4}$ [22].

(5) $\lambda \in \mathbb{C}$ está fuera del círculo unidad y $|Im(\lambda)| \geq \frac{1}{2}$ [23].

Además, es bien conocido que si z es libre entonces $\overline{z}$ y $-z$ también lo son. Todos estos resultados se pueden resumir diciendo que son puntos libres todos los puntos que están en el exterior de la siguiente figura.



Recientemente Bamberg [3] ha dado una familia F de polinomios tal que un número complejo es punto libre si y sólo si es raíz de un elemento de F. En cualquier caso es muy difícil comprobar si un número complejo en particular es raíz de uno de los polinomios dados. En particular no conocemos si $\sqrt{3}$ es un punto libre. Ahora ponemos de manifiesto que una respuesta a esto último es necesaria para saber si el

grupo generado por dos unidades bicíclicas que no conmuten es libre para un grupo diédrico arbitrario, es decir para eliminar la hipótesis $\langle y, h\rangle \subseteq \langle x, g\rangle$ del Teorema 2.1.1.

Sean b_1, b_2 dos unidades bicíclicas del mismo tipo en $\mathbb{Z}D_n$ y supongamos que $b_1 b_2 \neq b_2 b_1$. De nuevo es fácil de ver que podemos suponer que $b_1 = \beta_{a^t,b}$ y $b_2 = \beta_{a^i,a^j b}$. Si $x = (b_1 - 1)(b_2 - 1)$, entonces (con la notación de la sección anterior)

$$\chi_k(x) = 16 \operatorname{sen} \frac{2\pi tk}{n} \operatorname{sen} \frac{2\pi ik}{n} \operatorname{sen}^2 \frac{\pi jk}{n}.$$

En general no es verdad que exista un k tal que $\chi_k(x) \geq 4$. Por ejemplo, si $n = 12$, $t = j = 2$ y $i = 3$, entonces $\chi_k(x) = 0$ si $k = 2, 3, 4$ y $|\chi_k(x)| = 2\sqrt{3} < 4$ si $k = 1, 5$. Miremos a las representaciones. La descomposición de Wedderburn de $\mathbb{Q}D_{12}$ es bien conocida:

$$\mathbb{Q}D_{12} = 4\mathbb{Q} \oplus 3M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\sqrt{3})).$$

Tomando una base adecuada podemos hacer las siguientes identificaciones:

$$b_1 = (1, 1, 1, 1, A, A, 1, C) \quad \text{y} \quad b_2 = (1, 1, 1, 1, 1, B, D),$$

donde $A, B \in M_2(\mathbb{Q})$ no son la matriz identidad y

$$C = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad D = \begin{pmatrix} 1 & 0 \\ \sqrt{3} & 1 \end{pmatrix}.$$

Luego $\langle b_1, b_2\rangle$ es libre si y sólo si no existen enteros no nulos $h_1, \ldots, h_m$ y $k_1, \ldots, k_m$ tales que

$$h_1 + \ldots + h_m = k_1 + \ldots + k_m = 0 \quad \text{y} \quad C^{h_1} D^{k_1} C^{h_2} D^{k_2} \ldots C^{h_m} D^{k_m} = I.$$

En particular si $\sqrt{3}$ es un punto libre entonces $\langle b_1, b_2\rangle$ es libre.

De hecho el caso anterior parece ser el único caso problemático para grupos diédricos. Una búsqueda mediante ordenador para $n \leq 200$ muestra que si n no es un múltiplo de 12 entonces para todo $1 \leq t, i, j < n$ existe un k tal que $|\chi_k(x)| \geq 4$. Más aún, si $n = 12m$ entonces los únicos valores de (t, i, j) para los que $|\chi_k(x)| < 4$ para todo valor de k son

$$(2, 3, 2)m, \quad (3, 2, 2)m, \quad (4, 3, 2)m \quad \text{and} \quad (3, 4, 2)m.$$

Después de una reducción apropiada se puede demostrar que todos los casos se reducen a $n = 12$ y $(t, i, j) = (2, 3, 2)$. Éste es precisamente el ejemplo con el que nosotros tratábamos antes. Esto parece ser un indicio de que para todo par de unidades bicíclicas b_1 y b_2 del mismo tipo que no conmutan en $\mathbb{Z}D_n$ tenemos que $\langle b_1, b_2^2\rangle$ es un grupo libre y si $\sqrt{3}$ es un punto libre entonces $\langle b_1, b_2\rangle$ siempre es libre.

Acabamos esta sección haciendo una observación sobre el grupo generado por dos unidades bicíclicas de diferente tipo. Sean $b_1 = u_{a,b}$ y $b_2 = v_{a^i,a^jb}$. Entonces para todo carácter complejo irreducible χ_k de D_n tenemos que

$$\chi_k(x) = 16 \operatorname{sen} \frac{2\pi k}{n} \operatorname{sen} \frac{2\pi ik}{n} \cos^2 \frac{\pi jk}{n}.$$

En cualquier caso, para esa fórmula no hay análogo al Lemma 2.3.1. De hecho, para $n = 3$, es decir para D_3, hay pares de unidades bicíclicas que tienen traza "mala". Por ejemplo, si $b_1 = u_{b,a}$ y $b_2 = v_{ab,a}$, entonces

$$\chi_1(x) = 16 \operatorname{sen} \frac{2\pi}{3} \operatorname{sen} \frac{2\pi}{3} \cos^2 \frac{\pi}{3} = 3.$$

Esto implica que $\langle b_1, b_2 \rangle$ no es libre. De hecho, como se menciona en [12] el grupo $\langle b_1, b_2 \rangle$ contiene la unidad trivial $a \in D_3$.

Capítulo 3

Productos directos de grupos libres en $\mathcal{U}(\mathbb{Z}G)$

3.1. Introducción

El Problema 17 planteado por S. K. Sehgal [65], propone dar una presentación por generadores y relaciones de $\mathcal{U}(\mathbb{Z}G)$ para algunos grupos finitos G. Este problema es difícil de resolver para un grupo finito en general. La unidades cíclicas de Bass y las unidades bicíclicas generan un subgrupo de índice finito en $\mathcal{U}(\mathbb{Z}G)$ para muchos grupos. Son pocos los grupos para los que se conoce una presentación de $\mathcal{U}(\mathbb{Z}G)$ o de un subgrupo de índice finito suyo. Repasemos algunos de estos pocos casos.

Denotemos por $\mathcal{U}_1(\mathbb{Z}G)$ las unidades de aumento 1.

Los primeros resultados son debidos a Higman.

Teorema 3.1.1 (Teorema 2.9 (Higman)[65]) *Si A es un grupo finito abeliano, entonces $\mathcal{U}_1(\mathbb{Z}A) = A \times F$ donde F es un grupo libre abeliano cuyo rango viene determinado en términos de la estructura de A.*

Teorema 3.1.2 (Teorema 2.7 (Higman)[65]) *Para un grupo finito G, $\mathcal{U}(\mathbb{Z}G) = \pm G$ si y sólo si G es abeliano de exponente $2, 3, 4, 6$ ó $G = E \times Q_8$ donde E es un 2-grupo abeliano elemental.*

Para los grupos finitos G no considerados en los Teoremas de Higman, el siguiente resultado de Hartley y Pickel muestra como aparecen los grupos libres no abelianos en $\mathcal{U}(\mathbb{Z}G)$.

Teorema 3.1.3 (Teorema 5.1 (Hartley-Pickel)) *Sea G un grupo finito no abeliano. Entonces $\mathcal{U}(\mathbb{Z}G)$ contiene un subgrupo libre no abeliano si y sólo si G no es un 2-grupo Hamiltoniano, es decir, G no es isomorfo a $Q_8 \times E$, donde E es un 2-grupo abeliano elemental.*

Para algunos grupos G un grupo libre no abeliano representa un papel relevante.

Teorema 3.1.4 ([33]) *Sea $D_3 = \langle a, b | a^3 = b^2 = 1 bab = a^{-1} \rangle$ el grupo diédrico de orden 6. Entonces $\mathcal{U}_1(\mathbb{Z}D_3)$ es el producto semidirecto $V \rtimes D_3$, donde V es un grupo libre de rango 3 con generadores:*

$v_1 = 1 + (a - ba)(1 - a) = u_{b,a}$

$v_2 = 1 + (a - ba^2)(1 - a) = u_{ba,a}$

$v_3 = 1 + (a - b)a(1 - a) = u_{ba^2,a}$

En particular V esta generado por unidades bicíclicas.

Teorema 3.1.5 (Teorema 3.2 [65]) *Sea $D_4 = \langle a, b | a^4 = b^2 = 1 bab = a^{-1} \rangle$ el grupo diédrico de orden 8. Entonces $\mathcal{U}_1(\mathbb{Z}D_4)$ es un producto semidirecto $V \rtimes D_4$, donde V es un grupo libre de rango 3 con generadores:*

$v_1 = 1 + (b + a)(1 - a^2) = u_{ba,b}^{-1}$,

$v_2 = 1 + (ab - a)(1 - a^2) = u_{a^2b,ab}^{-1}$ *y*

$v_3 = 1 + (-b + a)(1 - a^2) = u_{ab,b}$.

En particular V esta generado por unidades bicíclicas.

Teorema 3.1.6 ([48]) *Q_{12} tiene un complemento normal en $\mathcal{U}_1(\mathbb{Z}Q_{12})$ que es un grupo libre de rango 5.*

Por desgracia un único grupo libre no suele ser suficiente para obtener un subgrupo de índice finito en $\mathcal{U}(\mathbb{Z}G)$ como muestra el siguiente teorema.

Teorema 3.1.7 (Jespers [24]) *Los únicos grupos finitos no abelianos G para los que $\mathcal{U}(\mathbb{Z}G)$ contiene un subgrupo libre de índice finito son:*

$$D_3,\ D_4,\ Q_{12} \quad y \quad \mathcal{P} = \langle a, b | a^4 = 1, b^4 = 1, aba^{-1}b^{-1} = a^2 \rangle.$$

Un ejemplo más en el que conocemos la estructura de $\mathcal{U}(\mathbb{Z}G)$ es el siguiente.

Teorema 3.1.8 ([34]) *Q_{16} tiene un complemento normal en $\mathcal{U}_1(\mathbb{Z}Q_{16})$ que es el producto directo de un grupo cíclico infinito y un grupo libre no abeliano de rango 9.*

Uno de los ingredientes importantes en la demostración del Teorema de Hartley-Pickel (Teorema 3.1.3) es el Teorema de Sanov (Teorema 2.2.4) que muestra que los subgrupos libres no abelianos de $\mathcal{U}(\mathbb{Z}G)$ se pueden encontrar en órdenes de las componentes simples del álgebra de grupo $\mathbb{Q}G$. Por esta razón no sólo es fácil encontrar grupos libres no abelianos sino productos directos de estos. Siguiendo esta idea en una serie de artículos ([32], [42] y [35]) Jespers, Leal y del Río caracterizaron los grupos finitos para los que $\mathcal{U}(\mathbb{Z}G)$ tiene un subgrupo de índice finito que es el producto directo de grupos libres, encontrando muchos más grupos que en el Teorema 3.1.7 de Jespers.

Teorema 3.1.9 (Jespers-del Río [35]) *Las siguientes condiciones son equivalentes para un grupo finito G:*

1. $\mathcal{U}(\mathbb{Z}G)$ contiene un subgrupo de índice finito que es el producto directo (finito) de grupos libres (finitamente generados).

2. Todo cociente simple no conmutativo de $\mathbb{Q}G$ es isomorfo a $M_2(\mathbb{Q})$, $\left(\frac{-1,-3}{\mathbb{Q}}\right)$ ó $\mathbb{H}(K)$ con $K = \mathbb{Q}, \mathbb{Q}(\sqrt{2})$ ó $\mathbb{Q}(\sqrt{3})$.

3. G es abeliano o isomorfo a $H \times C_2^k$ donde H es uno de los siguientes grupos:

(a) $\langle x, y \mid x^4 = y^4 = [x^2, y] = [x, y^2] = [x, [x, y]] = [y, [x, y]] = 1\rangle$,

(b) $\langle x, y_1, \ldots, y_n \mid x^4 = y_i^2 = [y_i, y_j] = [x^2, y_i] = [[x, y_i], y_j] = [[x, y_i], x] = 1\rangle$,

(c) $\langle x, y_1, \ldots, y_n \mid x^4 = y_i^4 = y_i^2[x, y_i] = [y_i, y_j] = [x^2, y_i] = [y_i^2, x] = 1\rangle$,

(d) $\langle x, y_1, \ldots, y_n \mid x^2 = y_i^2 = [y_i, y_j] = [[x, y_i], y_j] = [x, y_i]^2 = 1\rangle$,

(e) $\langle x, y_1, \ldots, y_n \mid x^2 = y_i^4 = y_i^2[x, y_i] = [y_i, y_j] = [[x, y_i], x] = 1\rangle$,

(f) $\langle x, y_1, \ldots, y_n \mid x^4 = y_i^4 = x^2y_1^2 = y_i^2[x, y_i] = [y_i, y_j] = [y_i^2, x] = 1\rangle$,

(g) $\langle x, y_1, \ldots, y_n \mid x^4 = x^2y_i^4 = y_i^2[x, y_i] = [y_i, y_j] = 1\rangle$,

(h) $U \rtimes_\phi \langle x\rangle$ *donde* U *es un 3-grupo abeliano elemental,* x *tiene orden* 2 *ó* 4 *y* $\phi(x) = \mathrm{inv}$ *donde* $\mathrm{inv} : G \to G$ *es la aplicación dada por* $g \mapsto g^{-1}$.

(i) $U \rtimes_\phi Q_8$ *donde* U *es un 3-grupo abeliano elemental,* $Q_8 = \langle x, y\rangle$ *y* $\phi(x) = \phi(y) = \mathrm{inv}$, *donde* $\mathrm{inv} : G \to G$ *es la aplicación dada por* $g \mapsto g^{-1}$.

El objetivo de este capítulo es concretar el Teorema 3.1.9 en un subgrupo con la estructura deseada, es decir, encontrar un subgrupo concreto $F = \prod_{i=1}^n F_i$ de índice finito en $\mathcal{U}(\mathbb{Z}G)$, tal que F_i es libre y óptimo en el sentido de que el índice de F en $\mathcal{U}(\mathbb{Z}G)$ sea mínimo entre todos los posibles subgrupos de $\mathcal{U}(\mathbb{Z}G)$ con esta estructura. El caso en que G es abeliano ya fue resuelto por Higman (Teorema 3.1.2), por lo que supondremos que $G = H \times Z$, donde H es un grupo de uno de los tipos $(a) - (i)$

y $Z = C_2^k$. Hay una manera natural de obtener tales subgrupos si no imponemos la condición de optimalidad. Por el Teorema 3.1.9, para todo idempotente central primitivo e de $\mathbb{Q}G$, una de las siguientes condiciones se verifica:

(A) $\mathbb{Q}Ge$ es isomorfo a $\mathbb{Q}$, una extensión imaginaria de $\mathbb{Q}$ o un álgebra de cuaterniones totalmente definida sobre $\mathbb{Q}$;

(B) $\mathbb{Q}Ge$ es un álgebra de cuaterniones totalmente definida sobre una extensión real cuadrática de $\mathbb{Q}$;

(C) $\mathbb{Q}Ge$ es isomorfo a $M_2(\mathbb{Q})$.

Sean A, B y C los conjuntos de idempotentes centrales primitivos de $\mathbb{Q}G$ de tipo (A), (B) y (C) respectivamente e $I = A \cup B \cup C$. Para todo $e \in I$ sea $\mathcal{O}_e$ un orden en $\mathbb{Q}Ge$. Entonces $\mathcal{U}(\mathcal{O}_e)$ es finito si $e \in A$. Si $e \in B$, el Lema 1.2.5 nos asegura que $\mathcal{U}(\mathcal{O}_e)$ es virtualmente cíclico infinito. Finalmente la siguiente Proposición junto con la Proposición 1.2.1 nos asegura que $\mathcal{U}(\mathcal{O}_e)$ es virtualmente libre no abeliano si $e \in C$.

Proposición 3.1.10 *El grupo $GL_2(\mathbb{Z})$ es virtualmente libre no abeliano.*

Demostración. Basta considerar $\Gamma(n)$ para cualquier $n \geq 3$ (véase la Proposición 1.3.2). □

Como $\mathcal{O} = \prod_{e \in I} \mathcal{O}_e$ y $\mathbb{Z}G$ son dos órdenes en $\mathbb{Q}G$, por la Proposición 1.2.1 tenemos que $\mathcal{U}(\mathcal{O}) \cap \mathcal{U}(\mathbb{Z}G)$ tiene índice finito en ambos. Por lo tanto $\mathcal{U}(\mathbb{Z}G) \cap (1 + \mathbb{Q}Ge)$ contiene un subgrupo de índice finito F_e que es trivial si $e \in A$, cíclico infinito si $e \in B$ y libre no abeliano si $e \in C$. Entonces $\prod_{e \in I} F_e$ es un subgrupo de índice finito de $\mathcal{U}(\mathbb{Z}G)$ con la estructura deseada.

Si queremos saber más sobre la estructura de $\mathcal{U}(\mathbb{Z}G)$ deberíamos calcular el rango de F_e para cada $e \in C$. Por supuesto que esto depende de la elección de F_e ya que el rango de un subgrupo de índice finito de un grupo libre no abeliano no es un invariante. En nuestro primer resultado mostramos que salvo para dos grupos (D_3 y D_4) podemos elegir F_e lo más grande posible, es decir, $F_e = \mathcal{U}(\mathbb{Z}G) \cap (1 + \mathbb{Q}Ge)$ y además todos los F_e tienen el mismo rango.

Teorema 3.1.11 *Sea $G = H \times Z$, donde Z es un 2-grupo elemental y H de uno de los tipos $(a) - (i)$ del Teorema 3.1.9. Sean B y C los conjuntos de idempotentes centrales primitivos de tipo (B) y (C) respectivamente. Sean $f_B = \sum_{f \in B} f$ y $F_0 = \mathcal{U}(\mathbb{Z}G) \cap (1 + \mathbb{Q}Gf_B)$ y para cada $e \in C$ sea $F_e = \mathcal{U}(\mathbb{Z}G) \cap (1 + \mathbb{Q}Ge)$. Entonces*

1. $F = F_0 \times \prod_{e \in C} F_e$ *tiene índice finito en* $\mathcal{U}(\mathbb{Z}G)$.

2. *Si* $G \ncong D_3, D_4$, *entonces para todo* $e \in C$

$$F_e = \mathcal{U}(\mathbb{Z}G) \cap (1 + \mathbb{Q}Ge)$$

es libre no abeliano y todos los F_e*'s tienen el mismo rango.*

3. F_0 *es libre abeliano de rango* $|B|$.

Probaremos el Teorema 3.1.11 en la Sección 3.2. Además calcularemos el rango de F_0 y de todos los F_e's para todos los grupos. Más aún, todo F_e es isomorfo a un subgrupo del grupo modular $\mathrm{PSL}_2(\mathbb{Z})$, el cual calcularemos en cada caso. Si tenemos en cuenta que existen métodos poderosos para obtener generadores de subgrupos de $\mathrm{PSL}_2(\mathbb{Z})$ (Reidemeister-Schreier) y de subgrupos de anillos de enteros, podemos concluir que tenemos un método para calcular generadores de F. Claro que esto es teórico pues los cálculos en grupos concretos son tremendos.

Así el grupo $F = F_0 \times \prod_{e \in C} F_e$ del Teorema 3.1.11 tiene las propiedades deseadas. Sin embargo esto no da información sobre como de grande es el grupo construido, o mejor dicho, como de pequeño es el índice de este grupo en $\mathcal{U}(\mathbb{Z}G)$, o sea, sobre la optimalidad del subgrupo construido. Sorprendentemente lo que vamos a demostrar es que esta construcción que en principio podría resultar simple, nos da un subgrupo óptimo en casi todos los casos y en aquellos casos en los que falla basta con "bajar un poco". De hecho los únicos únicos grupos para los que esto no es cierto son D_3, D_4, Q_{12} y Q_{16}, precisamente los de los Teoremas 3.1.4, 3.1.5, 3.1.6 y 3.1.8. Como no podemos pedir nada mejor que los resultados de estos teoremas no nos molestaremos en estudiarlos. En la Sección 3.3 demostramos que el grupo F del Teorema 3.1.11 es el mejor posible. Explícitamente demostramos el siguiente Teorema:

Teorema 3.1.12 *Sean* $G = H \times Z$ *y* $F = F_0 \times \prod_{e \in C} F_e$ *como en el Teorema 3.1.11. Si* $E = E_0 \times \prod_{j \in J} E_j$ *es un subgrupo de índice finito en* $\mathcal{U}(\mathbb{Z}G)$, *donde* E_0 *es libre abeliano y* E_j *es libre no abeliano para todo* j. *Entonces*

1. $r(E_0) = |B|$ *y* $|C| = |J|$.

   Además, si G *no es isomorfo a* D_3, D_4, Q_{12} *ni a* Q_{16} *entonces*

2. $[\mathcal{U}(\mathbb{Z}G) : F] \leq [\mathcal{U}(\mathbb{Z}G) : E]$ *y*

3. $r(E_j) \geq r(F_e)$ *para todo* $e \in C$ *y* $j \in J$.

Obsérvese que los grupos excepcionales D_3, D_4, Q_{12} y Q_{16} pertenecen a la lista de grupos que estamos considerando con los siguientes parámetros: $k = 0$ y $n = 1$ para todos ellos; D_4 es del tipo (d) ó (e), D_3 y Q_{12} son de tipo (h) con x de orden 2 y 4 respectivamente y finalmente Q_{16} es de tipo (g).

Estos cuatro grupos fueron estudiados respectivamente por Jespers y Leal [28] (véase el Teorema 3.1.5), Jespers y Parmenter [33] (véase el Teorema 3.1.4), Parmenter [48] (véase el Teorema 3.1.6) y de nuevo por Jesper y Parmenter [34] (véase el Teorema 3.1.8).

Todos los resultados de este Capítulo aparecieron en el artículo [55].

3.2. Grandes Subgrupos

En esta sección vamos a demostrar el Teorema 3.1.11. De hecho vamos a obtener más información ya que daremos además el rango de cada uno de los grupos libres F_e para cada idempotente central primitivo e del tipo (C) y un subgrupo de $\mathrm{PSL}_2(\mathbb{Z})$ isomorfo a F_e. Además vamos a obtener el rango del grupo libre abeliano F_0.

La afirmación (1) del Teorema 3.1.11 se sigue del párrafo anterior al Teorema 3.1.11.

A lo largo de toda la sección $G = H \times Z$ donde H es un grupo de uno de los tipos $(a) - (i)$ del Teorema 3.1.9 y $Z = C_2^k$ para algún entero k. Demostraremos los apartados (2) y (3) del Teorema 3.1.11 mediante una serie de Proposiciones que distinguen los diferentes casos. Las demostraciones son muy similares y obviaremos repeticiones tediosas. El esquema de las Proposiciones y sus demostraciones es el siguiente:

- Identificaremos los idempotentes centrales primitivos de $\mathbb{Q}G(1-\widehat{G'})$ y dentro de estos identificamos el tipo de cada uno de ellos. Obsérvese que los idempotentes centrales primitivos de $\mathbb{Q}G\widehat{G'}$ son precisamente aquellos para los que $\mathbb{Q}Ge$ es un cuerpo y por lo tanto son de tipo (A).
- Para cada idempotente central primitivo e de tipo (B) ó (C) obtendremos una base y un isomorfismo con una de las álgebras simples del apartado 2 del Teorema 3.1.9.
- Para cada idempotente central primitivo e de tipo (C) obtendremos un isomorfismo de F_e con un subgrupo de $\mathrm{PSL}_2(\mathbb{Z})$ y utilizaremos esto, junto con el Teorema de Nielsen-Schreier para obtener el rango de F_e.
- Mostraremos que F_0 está incluido en el centro de $\mathbb{Z}Gf_B$ y es libre de torsión, de donde se deduce el apartado 3 del Teorema 3.1.11 y calculamos el rango de F_0 contando el número de idempotentes de tipo (B).

Recordamos el enunciado del Teorema de Nielsen-Schreier.

Teorema 3.2.1 (Teorema de Nielsen-Schreier. Teorema 6.1.1 [60]) *Sea H un subgrupo de índice i de un grupo libre de rango r, entonces H es libre de rango $1 + i(r-1)$.*

También utilizaremos el siguiente lema que calcula cual es el grupo de las unidades de determinados órdenes en las álgebras de cuaterniones que aparecen en 2 del Teorema 3.1.9.

Lema 3.2.2 *1. Sea $A = \mathbb{H}(R)$ donde $R = \mathbb{Z}[\sqrt{n}]$ siendo n un entero positivo. Entonces las unidades de A son de la forma $u, u\mathbf{i}, u\mathbf{j}$ ó $u\mathbf{k}$ donde u es una unidad de R.*

2. Sea $A = \mathbb{Z}[\mathbf{i}, \frac{1+\mathbf{j}}{2}]$ el subanillo de $\left(\frac{-1,-3}{\mathbb{Q}}\right)$ generado por $\mathbf{i}$ y $\frac{1+\mathbf{j}}{2}$. Entonces las unidades de A son $\pm 1, \pm\mathbf{i}, \pm\frac{\mathbf{i}+\mathbf{ij}}{2}, \pm\frac{1-\mathbf{j}}{2}, \pm\frac{1+\mathbf{j}}{2}$ y $\frac{\mathbf{i}-\mathbf{ij}}{2}$ (véase [48]).

3. Sea n un entro congruente con -1 módulo 4. Sea $R = \mathbb{Z}[\mathbf{i}, \mathbf{j}, \frac{1+\sqrt{n}\mathbf{i}}{2}]$ el subanillo de $\mathbb{H}(\mathbb{Q}(\sqrt{n}))$. Entonces las unidades de R son de la forma v ó $v\mathbf{j}$ donde v es una unidad de $\mathbb{Z}[\mathbf{i}, \frac{1+\sqrt{n}\mathbf{i}}{2}]$.

Demostración. Demostraremos 1 con detalle para el caso en que $R = \mathbb{Z}[\sqrt{n}]$ y daremos una indicación para la demostración de 3, ya que el resto de las demostraciones se sigue por argumentos similares.

1. Podemos suponer sin pérdida de generalidad que n es libre de cuadrados y mayor que 1.

Sea $u = u_1 + u_2\mathbf{i} + u_3\mathbf{j} + u_4\mathbf{k} \in \mathcal{U}(A)$ con $u_i = x_i + y_i\sqrt{n}$ y $x_i, y_i \in \mathbb{Z}$. Entonces la norma reducida de u visto como elemento de A es una unidad en $\mathbb{Z}[\sqrt{n}]$, es decir, $a = N_A(u) = \sum_{i=1}^4 u_i^2 = \sum_{i=1}^4 (x_i^2 + ny_i^2) + 2\sqrt{n}\sum_{i=1}^4 x_i y_i \in \mathcal{U}(\mathbb{Z}[\sqrt{n}])$. Por lo tanto la norma de a, vista en la extensión cuadrática $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{n})$, es igual a ± 1. Esta norma vale

$$\begin{aligned} N_{\mathbb{Q}(\sqrt{n})/\mathbb{Q}}(a) &= (\textstyle\sum_{i=1}^4 x_i^2 + n\sum_{i=1}^4 y_i^2)^2 - 4n(\sum_{i=1}^4 x_i y_i)^2 \\ &= \textstyle\sum_{i=1}^4 x_i^4 + n^2\sum_{i=1}^4 y_i^4 + 2\sum_{i<j} x_i^2 x_j^2 + 2n^2\sum_{i<j} y_i^2 y_j^2 + \\ &\quad 2n\textstyle\sum_{i=1}^4 x_i^2 y_i^2 + 2n\sum_{i<j}(x_i^2 y_j^2 + y_i^2 x_j^2) - 4n\sum_{i=1}^4 x_i^2 y_i^2 - 8n\sum_{i<j} x_i y_i x_j y_j \\ &= \textstyle\sum_{i=1}^4 (x_i^2 - ny_i^2)^2 + 2\sum_{i<j}(x_i x_j - ny_i y_j)^2 + 2n\sum_{i<j}(x_i y_j - y_i x_j)^2 \\ &= \textstyle\sum_{i=1}^4 N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(u_i)^2 + 2\sum_{i<j}(x_i x_j - ny_i y_j)^2 + 2n\sum_{i<j}(x_i y_j - y_i x_j)^2. \end{aligned}$$

Luego $N_{\mathbb{Q}(\sqrt{n})/\mathbb{Q}}(a) = 1$ y deducimos que $N_{\mathbb{Q}(\sqrt{n})/\mathbb{Q}}(u_i) = 1$ para un $i = 1, 2, 3, 4$ y $N_{\mathbb{Q}(\sqrt{n})/\mathbb{Q}}(u_j) = 0$ para todo $j \neq i$ y con esto acabamos la demostración de 1.

3. Sea $w = \frac{1+\sqrt{n}\mathbf{i}}{2}$. Entonces se verifican las siguientes relaciones

$$\begin{aligned} x^2 &= x - \tfrac{n+1}{4} \in R \\ \mathbf{i}w &= \mathbf{i}w \in R \\ \mathbf{j}w &= \mathbf{j} - w\mathbf{j} \in R \\ \mathbf{k}w &= \mathbf{k} - w\mathbf{k} \in R \end{aligned}$$

Luego el conjunto de combinaciones lineales de $1, \mathbf{i}, \mathbf{j}, \mathbf{k}, w, w\mathbf{i}, w\mathbf{j}, w\mathbf{k}$ con coeficientes enteros forman un orden R en $\mathbb{H}(\mathbb{Q}(\sqrt{n}))$.

Los elementos de R son de la forma $u = \frac{1}{2}[u_1+u_2\mathbf{i}+u_3\mathbf{j}+u_4\mathbf{k}]$ con $u_i \in \mathbb{Z}[\sqrt{n}]$ para $i = 1, 2, 3, 4$ y $u_1+u_2\sqrt{n} \in 2\mathbb{Z}[\sqrt{n}]$, $u_3+u_4\sqrt{n} \in 2\mathbb{Z}[\sqrt{n}]$. Si $N : \mathbb{H}(\mathbb{Q}(\sqrt{n})) \to \mathbb{Q}(\sqrt{n})$ es la norma reducida, entonces $N(R)$ está incluido en un orden de $\mathbb{Q}(\sqrt{n})$, luego está incluido en el anillo de enteros de $\mathbb{Q}(\sqrt{n})$ que , como $n \equiv -1 \bmod 4$ es $\mathbb{Z}[\sqrt{n}]$. Sea $u = \frac{1}{2}[u_1 + u_2\mathbf{i} + u_3\mathbf{j} + u_4\mathbf{k}] \in \mathcal{U}(R)$ con $u_i = x_i + y_i\sqrt{n}$ y $x_i, y_i \in \mathbb{Z}$. Entonces la norma reducida de u es una unidad en $\mathbb{Z}[\sqrt{n}]$, es decir, $a = N(u) = \frac{1}{4}\sum_{i=1}^{4} u_i^2 = \sum_{i=1}^{4}(x_i^2 + ny_i^2) + 2\sqrt{n}\sum_{i=1}^{4} x_iy_i \in \mathcal{U}(\mathbb{Z}[\sqrt{n}])$. Por lo tanto la norma de a, vista en la extensión cuadrática $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{n})$, es igual a ± 1. Repitiendo los cálculos de la demostración de 1 vemos que esta norma vale

$$\frac{1}{16}[\sum_{i=1}^{4} N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(u_i)^2 + 2\sum_{i<j}(x_ix_j - ny_iy_j)^2 + 2n\sum_{i<j}(x_iy_j - y_ix_j)^2].$$

Luego $N_{\mathbb{Q}(\sqrt{n})/\mathbb{Q}}(a) = 1$ de donde deducimos que

$$\sum_{i=1}^{4} N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(u_i) + 2\sum_{i<j}(x_ix_j - ny_iy_j)^2 + 2n\sum_{i<j}(x_iy_j - y_ix_j)^2 = 16.$$

La demostración se acaba con un largo pero directo análisis de casos en que los ingredientes principales son las siguientes propiedades,

$$n \equiv -1 \bmod 4$$

y

$$x_1 - y_1 \equiv x_1 - y_1 \equiv x_1 - y_1 \equiv x_1 - y_1 \equiv 0 \bmod 2$$

□

Ahora pasamos a introducir la notación que utilizaremos en el desarrollo de la sección.

3.2.1. Notación

Si H es un grupo de uno de los tipos $(b) - (f)$, entonces para cada $i = 1, 2, \ldots, n$ pondremos

$$t_i = [x, y_i] = xy_ix^{-1}y_i^{-1}.$$

Sin embargo si H es del tipo (g) entonces

$$t_i = [x, y_i]\langle x^2\rangle \in H/\langle x^2\rangle.$$

Además en este caso denotaremos por $\pi : G \to G/\langle x^2\rangle$ a la proyección.

Claramente

$$G' = H' = \begin{cases} \langle [x,y] \rangle \cong C_2 & \text{si } H \text{ es de tipo (a);} \\ \langle t_1, t_2, \ldots, t_n \rangle \cong C_2^n & \text{si } H \text{ es del tipo (b)-(f);} \\ \pi^{-1}(\langle t_1, t_2, \ldots, t_n \rangle) \cong C_4 \times C_2^{n-1} & \text{si } H \text{ es del tipo (g);} \\ U \cong C_3^n & \text{si } H \text{ es del tipo (h);} \\ U \times \langle x^2 \rangle \cong C_3^n \times C_2 & \text{si } H \text{ es del tipo (i).} \end{cases}$$

Si X es un grupo denotamos por $X^* = \mathrm{Hom}(X, \mathcal{U}(\mathbb{Z}))$, y si $\varphi : X \to \mathbb{Z}$ es una aplicación denotaremos por $\widehat{X}_\varphi = \frac{1}{|X|} \sum_{x \in X} \varphi(x) x$. Obsérvese que $\widehat{X} = \widehat{X}_\psi$ donde $\psi(x) = 1$ para todo $x \in X$. Si $x \in X$ y $\psi \in \langle x \rangle^*$ pondremos $\widehat{x}_\psi$ en lugar de $\widehat{\langle x \rangle}_\psi$.

En las siguientes proposiciones tendremos:

- $\psi \in Z^*$.
- S un subgrupo maximal de:
  - H' si H es de uno de los tipos $(b) - (f)$;
  - H' que contiene a $\langle x^2 \rangle$ si H es de tipo (g);
  - U si H es de uno de los tipos (h) ó (i).
- χ un elemento de:
  - $\langle x^2, y^2 \rangle^*$ si H es del tipo (a);
  - $\langle x^2 \rangle^*$ si H es de uno de los tipos $(b) - (h)$;
  - $\langle xy \rangle^*$ si H es de tipo (i) y $Q_8 = \langle x, y \rangle$.
- $\phi : H' \to H$ la aplicación dada por $\phi(t_1^{i_1} t_2^{i_2} \cdots t_n^{i_n}) = y_1^{i_1} y_2^{i_2} \cdots y_n^{i_n}$ si H es de uno de los tipos $(a) - (f)$.
- $\varrho : H'/\langle x^2 \rangle \to H$ la aplicación dada por $\varrho(t_1^{i_1} t_2^{i_2} \cdots t_n^{i_n}) = y_1^{i_1} y_2^{i_2} \cdots y_n^{i_n}$ si H es de tipo (g).
- Para todo $a, b \in \mathbb{Z}$ definimos

$$\Lambda^a(b) = \mathrm{SL}_2(\mathbb{Z}) \cap \left[1 + b \begin{pmatrix} \mathbb{Z} & a\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{pmatrix} \right] \text{ y}$$

$$\Lambda_a(b) = \mathrm{SL}_2(\mathbb{Z}) \cap \left[1 + b \begin{pmatrix} a\mathbb{Z} & \mathbb{Z} \\ a\mathbb{Z} & a\mathbb{Z} \end{pmatrix} \right].$$

3.2.2. Tipos $(b)-(f)$

En esta subsección demostraremos el Teorema 3.1.11 para los casos en que H es de uno de los tipos $(b)-(f)$.

Proposición 3.2.3 *Supongamos que H es de uno de los tipos $(b)-(f)$. Entonces:*

1. *Los idempotentes centrales primitivos de $\mathbb{Q}G(1-\widehat{G'})$ son los elementos de la forma*
$$e = e_{S,\chi,\varphi,\psi} = \widehat{x^2}_{\chi}(\widehat{S}-\widehat{G'})\widehat{\phi(S)}_{\varphi}\widehat{Z}_{\psi}$$
donde S,χ,φ,ψ y ϕ son tal y como se explican en la notación de la Subsección 3.2.1 y además si H es del tipo (f), χ es trivial si y sólo si $t_1 \in S$.

2. *Si χ no es trivial y H no es de tipo (b) entonces $Ge \cong Q_8$ y $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q})$, por tanto e es de tipo (A),*

3. *en caso contrario $Ge \cong D_4$ y $\mathbb{Q}Ge \cong M_2(\mathbb{Q})$, es decir e es de tipo (C).*

4. *Si e es un idempotente central primitivo de tipo (C) entonces:*

   a) $F_e \cong \begin{cases} \Lambda^2(2^{2n+k}) & \text{si } H \text{ es de tipo } (b)-(c). \\ \Lambda^2(2^{2n+k-1}) & \text{si } H \text{ es de tipo } (d)-(f). \end{cases}$

   b) Si $G \ncong D_4$ entonces F_e es libre y
$$r(F_e) = \begin{cases} 1+2^{6n+3(k-1)} & \text{si } H \text{ es de tipo } (b)-(c), \\ 1+2^{6n+3(k-2)} & \text{si } H \text{ es de tipo } (d)-(f). \end{cases}$$

Demostración. La afirmación 1 es consecuencia de 2 y 3 y de que la suma de los idempotentes $e_{S,\chi,\varphi,\psi}$ es $1-\widehat{G'}$. Esto último se obtiene con un cálculo sencillo. Sea $H_S = \langle x^2, G', \phi(S), Z\rangle$. Entonces H_S es un subgrupo normal de índice 4 en G y si $t \in H' \setminus S$, entonces $\{e, xe, ye = \phi(t)e, xye\}$ es una base de $\mathbb{Q}Ge$ y se verifican las siguientes relaciones:

- $yexe = -xeye$.
- $x^2e = y^2e = -e$, si se verifican las condiciones de 2, con lo que en tal caso $Ge \cong Q_8$ y $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q})$.
- $\pm e = x^2e \neq y^2e = \pm e$ si se verifican las condiciones de 3, con lo que en tal caso $Ge \cong D_4$ y $(1+x)e$ es un divisor de cero de $\mathbb{Q}Ge$. Como la dimensión de $\mathbb{Q}Ge$ sobre $\mathbb{Q}$ es 4, $\mathbb{Q}Ge \cong M_2(\mathbb{Q})$.

Esto demuestra 2 y 3.

Supongamos que e es de tipo (C) y denotemos $a = xe$ y $b = ye$ o viceversa de forma que $a^4 = b^2 = e$. Entonces los elementos

$$\begin{array}{ll} e_{11} = \frac{(e+b)}{2}e, & e_{12} = \frac{(ab-a)}{2}e, \\ e_{21} = \frac{(ab+a)}{2}e, & e_{22} = \frac{(e-b)}{2}e, \end{array}$$

forman una base de matrices elementales, es decir $e_{ij}e_{kl} = \delta_{jk}e_{il}$ para todo i, j, k, l y $e_{11} + e_{22} = e$.

Esto implica que existe un único isomorfismo $\rho : \mathbb{Q}Ge \to M_2(\mathbb{Q})$ que asocia

$$e_{11} \sim \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ e_{12} \sim \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ e_{21} \sim \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ y } e_{22} \sim \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

y se verifican las siguientes relaciones:

$$\begin{array}{c} e = e_{11} + e_{22} \\ a = e_{21} - e_{12} \\ b = e_{11} - e_{22} \\ ab = e_{12} + e_{21} \end{array}$$

Por lo tanto la aplicación $\rho : \mathbb{Q}Ge \to M_2(\mathbb{Q})$ dada por

$$\rho(\alpha_0 e + \alpha_1 a + \alpha_2 b + \alpha_3 ab) = \begin{pmatrix} \alpha_0 + \alpha_2 & \alpha_3 - \alpha_1 \\ \alpha_1 + \alpha_3 & \alpha_0 - \alpha_2 \end{pmatrix}$$

es un isomorfismo de $\mathbb{Q}$-álgebras. Con el fin de obtener una mejor representación matricial componemos ρ con el automorfismo interno inducido por $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Entonces tenemos un isomorfismo $\mathbb{Q}Ge \cong M_2(\mathbb{Q})$ que asocia el elemento $\alpha_0 e + \alpha_1 a + \alpha_2 b + \alpha_3 ab$ con

$$\begin{pmatrix} \alpha_0 + \alpha_2 - \alpha_1 - \alpha_3 & 2(\alpha_2 - \alpha_1) \\ \alpha_1 + \alpha_3 & \alpha_0 + \alpha_1 - \alpha_2 + \alpha_3 \end{pmatrix}$$

que pasaremos a llamar ρ olvidándonos del viejo ρ.

Todo elemento $\alpha \in \mathbb{Z}G$ se puede escribir como

$$\alpha = \beta_0 + \beta_1 x + \beta_2 y + \beta_3 xy$$

donde $\beta_i \in \mathbb{Z}G$ y $sop(\beta_i) \subseteq H_S$. Además si $h \in H_S$, entonces $he = \pm 1$ y por lo tanto $\alpha e = \alpha_0 e + \alpha_1 a + \alpha_2 b + \alpha_3 ab$ para algún $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}$ y $\omega(\alpha) = \sum_{i=0}^{3} \omega(\beta_i) \equiv \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 \bmod 2$, donde ω denota la aplicación aumento.

Si $\alpha \in F_e = \mathcal{U}(\mathbb{Z}G) \cap (1 + \mathbb{Q}Ge)$ tenemos que $\alpha = \alpha e + (1 - e) = 1 + (\alpha - 1)e$. Por el párrafo anterior podemos escribir $\alpha = 1 + \alpha_0 e + \alpha_1 a + \alpha_2 b + \alpha_3 ab$ con $\alpha_i \in \mathbb{Z}$ y $\omega(\alpha) \equiv \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 \bmod 2$. Como $\alpha \in \mathbb{Z}G$ tenemos que $\alpha_i e \in \mathbb{Z}G$ para

todo i y considerando el coeficiente del 1 en este elemento tenemos que $2^{2n+k} \mid \alpha_i$ ó $2^{2n+k-1} \mid \alpha_i$ dependiendo de que H sea de uno de los tipos $(b)-(c)$ ó $(d)-(f)$ respectivamente. A partir de ahora nos referimos al caso en que H sea de los tipos (b) ó (c) en el texto básico y al caso en que H sea de los tipos $(d)-(f)$ en el texto entre paréntesis. Sea $\gamma_i = \alpha_i/2^{2n+k}$ (respectivamente $\gamma_i = \alpha_i/2^{2n+k-1}$). Entonces $\alpha = 1+2^{2n+k}(\gamma_0+\gamma_1 x+\gamma_2 y+\gamma_3 xy)e$ (resp. $\alpha = 1+2^{2n+k-1}(\gamma_0+\gamma_1 x+\gamma_2 y+\gamma_3 xy)e$), luego

$$\rho(\alpha) = 1 + 2^{2n+k}\begin{pmatrix} \gamma_0-\gamma_1+\gamma_2-\gamma_3 & 2(\gamma_2-\gamma_1) \\ \gamma_1+\gamma_3 & \gamma_0+\gamma_1-\gamma_2+\gamma_3 \end{pmatrix}$$

(resp.

$$\rho(\alpha) = 1 + 2^{2n+k-1}\begin{pmatrix} \gamma_0-\gamma_1+\gamma_2-\gamma_3 & 2(\gamma_2-\gamma_1) \\ \gamma_1+\gamma_3 & \gamma_0+\gamma_1-\gamma_2+\gamma_3 \end{pmatrix}).$$

Por lo tanto $\rho(\alpha) = 1 + 2^{2n+k}\begin{pmatrix} a & 2b \\ c & d \end{pmatrix}$ (resp. $\rho(\alpha) = 1 + 2^{2n+k-1}\begin{pmatrix} a & 2b \\ c & d \end{pmatrix}$) con $a \equiv d \bmod 2$. El determinante de $\rho(\alpha)$ tiene que ser una unidad de $\mathbb{Z}$, pero del hecho de que $a \equiv d \bmod 2$ deducimos que este determinante es 1. Luego $\rho(F_e) \subseteq \Lambda^2(2^{2n+k})$ (resp. $\rho(F_e) \subseteq \Lambda^2(2^{2n+k-1})$). Veamos que en efecto se da la igualdad. Para ver esto basta observar que si $A = \begin{pmatrix} 1+2^{2n+k}a & 2^{2n+k+1}b \\ 2^{2n+k}c & 1+2^{2n+k}d \end{pmatrix} \in \Lambda^2(2^{2n+k})$ (resp. $A = \begin{pmatrix} 1+2^{2n+k-1}a & 2^{2n+k}b \\ 2^{2n+k-1}c & 1+2^{2n+k-1}d \end{pmatrix} \in \Lambda^2(2^{2n+k-1})$) el siguiente sistema

$$\begin{aligned} \gamma_0-\gamma_1+\gamma_2-\gamma_3 &= a \\ \gamma_2-\gamma_1 &= b \\ \gamma_1+\gamma_3 &= c \\ \gamma_0+\gamma_1-\gamma_2+\gamma_3 &= d \end{aligned}$$

tiene soluciones enteras. Más concretamente el sistema es equivalente a

$$\begin{aligned} \gamma_0-\gamma_1+\gamma_2-\gamma_3 &= a \\ \gamma_2-\gamma_1 &= b \\ \gamma_2+\gamma_3 &= b+c \\ \gamma_3 &= \tfrac{a+d+2b}{2} \end{aligned}$$

cuyas soluciones son enteras ya que $a \equiv d \bmod 2$ por ser $\det(A) = 1$.

Además $\Lambda^2(2^{2n+k})$ (resp. $\Lambda^2(2^{2n+k-1})$) es un subgrupo de índice 2 de $\Gamma(2^{2n+k})$ (resp. $\Gamma(2^{2n+k-1})$) y por el Teorema 1.3.1 $\Gamma(2^{2n+k}) \simeq \widehat{\Gamma(2^{2n+k})}$ (resp. $\Gamma(2^{2n+k-1}) \simeq \widehat{\Gamma(2^{2n+k-1})}$) es un subgrupo de índice $2^{6n+3k-4}$ (resp. $2^{6n+3k-7}$) de $\widehat{\Gamma(2)}$. Como este último grupo es libre de rango 2, por el Teorema 3.2.1, $\Lambda^2(2^{2n+k})$ (resp.$\Lambda^2(2^{2n+k-1})$) es libre de rango $1+2^{6n+3(k-1)}$ (resp. $1+2^{6n+3(k-2)}$). Obsérvese que $\Lambda^2(2^m) \subseteq \Gamma(2^m)$ y que $\Gamma(2^m)$ es libre para $m > 1$. Por tanto el único caso en que $\rho(F_e)$ pudiera ser no libre sería para H de tipo $(d)-(f)$ con $2n+k-1 = 0$, es decir $k = 0$ y $n = 1$. Los casos en (d) y (e) con estos valores de k y n corresponden a $G \cong D_4$. El caso (f)

con estos valores corresponde a Q_8. Pero $\mathbb{Q}Q_8$ no tiene idempotentes de tipo (C) y esto termina la demostración de 4. $\square$

Obsérvese que D_4 es de tipo (d) y (e) con $n = 1$ y $k = 0$. Utilizaremos la presentación (e). Entonces I tiene un único elemento $e = 1 - \widehat{y_1^2} \in C$. Por la Proposición 3.2.3, $F_e \cong \Lambda^2(2)$ que no es libre pues $-I \in \Lambda^2(2)$. Para encontrar un subgrupo libre de índice finito basta bajar un poco. En efecto $\Lambda^2(2)$ contiene un subgrupo libre de índice 2, a saber el formado por las matrices de $\mathrm{SL}_2(\mathbb{Z})$ de la forma $1+2\begin{pmatrix} 2a & 2b \\ c & 2d \end{pmatrix}$ (véase la demostración del Lema 3.3.2). De aquí se deduce que F_e contiene un subgrupo libre de índice 2 que es precisamente el grupo V del Teorema 3.1.5.

3.2.3. Tipo (a)

La demostración de la siguiente proposición es análoga a la de la Proposición 3.2.3 y por tanto la obviaremos para evitar repeticiones.

Proposición 3.2.4 *Supongamos que H es de tipo (a). Entonces:*

1. *Los idempotentes centrales primitivos de $\mathbb{Q}G(1 - \widehat{G'})$ son de la forma $e = \widehat{\langle x^2, y^2\rangle}_\chi(1 - \widehat{G'})\widehat{Z}_\psi$, donde $\chi \in \langle x^2, y^2\rangle^*$ y $\psi \in Z^*$.*
2. *Si $\chi(x^2) = \chi(y^2) = -1$ entonces $Ge \cong Q_8$ y $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q})$, luego e es de tipo (A),*
3. *en caso contrario $Ge \cong D_4$ y $\mathbb{Q}Ge \cong M_2(\mathbb{Q})$, luego e es de tipo (C).*
4. *Si e es un idempotente central primitivo de $\mathbb{Q}G$ de tipo (C), $F_e \cong \Lambda^2(2^{k+3})$ que es libre y su rango es $1 + 2^{3k+7}$.*

3.2.4. Tipo (g)

El caso en que H es de tipo (g) presenta la novedad respecto a los tipos $(a)-(f)$ de que $\mathbb{Q}G$ tiene idempotentes centrales primitivos de tipo (B). Por tanto éste es el primer grupo que nos encontramos en el que $F_0 \neq 1$ lo que nos lleva a tener que desarrollar nuevos argumentos para su cálculo.

Definimos

$$K = \langle y_1^2y_2^2, \ldots, y_1^2y_n^2, Z\rangle = \langle y_1^{2i_1}y_2^{2i_2}\ldots y_n^{2i_n} : \sum_{t=1}^{n} i_t \equiv 0 \bmod 2\rangle \times Z.$$

Para todo $\xi \in K^*$ y todo $2 \leq i \leq n$, sea $\xi_i = \xi(y_1^2y_i^2)$,

$$K(\xi) = \langle y_1^{\xi_2}y_2, \ldots, y_1^{\xi_n}y_n, Z\rangle$$

y

$$T_\xi = \{y_1^{\sum_{j=2}^n \xi_j i_j} y_2^{i_2} \dots y_n^{i_n} : 0 \leq i_j \leq 1\}.$$

Entonces T_ξ es un transversal de $\langle x^2, K(\xi)\rangle$ módulo K. Para cada $\xi \in K^*$ y $\tau \in K(\xi)^*$ definimos $\rho_{\xi,\tau}(kt) = \tau(k)\xi(t)$ para todo $k \in K$ y $t \in T_\xi$, de forma que $\rho_{\xi,\tau}$ está definido en $\langle x^2, K(\xi)\rangle$.

Proposición 3.2.5 *Supongamos que H es de tipo (g). Entonces:*

1. *$\mathbb{Q}G(1-\widehat{G'})$ no tiene idempotentes centrales primitivos de tipo (A).*
2. *Los idempotentes centrales primitivos de $\mathbb{Q}G$ de tipo (C) son de la forma*

$$e = e_{S,\varphi,\psi} = (\widehat{S} - \widehat{G'})\widehat{\varrho\pi(S)_\varphi}\widehat{Z_\psi}$$

donde S y ϱ son tal y como se explican en la notación de la Subsección 3.2.1, $\pi : G \to G/\langle x^2\rangle$ es la proyección y $\varphi : \phi \circ \pi(S) \to \mathcal{U}(\mathbb{Z})$ es una aplicación tal que $\varphi \circ \phi \in (S/\langle x^2\rangle)^*$.

3. *Si e es un idempotente central primitivo de $\mathbb{Q}G$ de tipo (C), $F_e \simeq \Lambda^2(2^{2n+k})$ que es libre de rango $1 + 2^{6n+3(k-1)}$.*
4. *Los idempotentes centrales primitivos de $\mathbb{Q}G$ de tipo (B) son de la forma*

$$f = f_{\xi,\tau} = (1-\widehat{x^2})\widehat{K(\xi)}_{\rho_{\xi,\tau}}$$

con $\xi \in K^*$ y $\tau \in K(\xi)^*$ tal que $K \subseteq \operatorname{Ker}\tau$.

5. *$f_B = 1 - \widehat{x^2}$ y si $F_0 = \mathcal{U}(\mathbb{Z}G) \cap (1 + \mathbb{Q}Gf_B)$, entonces F_0 está incluido en el centro de $\mathbb{Q}G$ y es libre abeliano de rango 2^{2n+k-2}.*

Demostración. Las demostraciones de $1, 2$ y 3 se siguen de argumentos similares a los utilizados en la Proposición 3.2.3.

4. Que $f = f_{\xi,\tau}$ es un idempotente central es obvio. Mostraremos que es primitivo identificando $\mathbb{Q}Gf$ con $\mathbb{H}(\mathbb{Q}(\sqrt{2}))$ que es un anillo de división. En efecto,

$$Gf_{\xi,\chi} = \langle a = xf, b = y_1 f \mid a^2 = b^4, b^8 = 1, aba^{-1} = b^{-1}\rangle \simeq Q_{16}$$

y $\mathcal{B} = \{f, b, b^2, b^3, a, ab, ab^2, ab^3\}$ es una base de $\mathbb{Q}Gf$ sobre $\mathbb{Q}$ y $b^4 = a^2 = -1$ y $ab = -b^3a$. El centro de $\mathbb{Q}Gf$ es $K = \mathbb{Q}(c)$ donde $c = b(1-b^2)$ satisface que $c^2 = 2$. Por lo tanto existe un homomorfismo de algebras $\eta : \mathbb{Q}Gf \to \mathbb{H}(K)$ tal que $\eta(a) = \mathbf{i}$ y $\eta(b) = \frac{\sqrt{2}(1+\mathbf{j})}{2}$. Así el homomorfismo η definido por

$$\begin{aligned}\eta(\textstyle\sum_{g\in\mathcal{B}} \alpha_g g) \;=\; & \alpha_f + \tfrac{\sqrt{2}}{2}(\alpha_b - \alpha_{b^3}) + (\alpha_a + \tfrac{\sqrt{2}}{2}(\alpha_{ab} - \alpha_{ab^3}))\mathbf{i} + \\ & (\alpha_{b^2} + \tfrac{\sqrt{2}}{2}(\alpha_b + \alpha_{b^3}))\mathbf{j} + (\alpha_{ab^2} + \tfrac{\sqrt{2}}{2}(\alpha_{ab} + \alpha_{ab^3}))\mathbf{k}\end{aligned}$$

es un isomorfismo de anillos.

5. Si $\alpha \in F_0$ entonces $\alpha - 1 \in \Delta(G, \langle x^2 \rangle)$ y así $(\alpha - 1)f_B \equiv 0 \bmod 2$, en $\mathbb{Z}Gf_B$. Por lo tanto, si $f \in B$, entonces $(\alpha - 1)f \equiv 0 \bmod 2$, en $\mathbb{Z}Gf$ y

$$\begin{aligned}\eta(\alpha) &= 1 + \alpha_f + \tfrac{\sqrt{2}}{2}(\alpha_b - \alpha_{b^3}) + (\alpha_a + \tfrac{\sqrt{2}}{2}(\alpha_{ab} - \alpha_{ab^3}))\mathbf{i} + \\ &\quad (\alpha_{b^2} + \tfrac{\sqrt{2}}{2}(\alpha_b + \alpha_{b^3}))\mathbf{j} + (\alpha_{ab^2} + \tfrac{\sqrt{2}}{2}(\alpha_{ab} + \alpha_{ab^3}))\mathbf{k}\end{aligned}$$

es una unidad de $\mathbb{H}(\mathbb{Z}[\sqrt{2}])$. Como todas las unidades de $\mathbb{H}(\mathbb{Z}[\sqrt{2}])$ son de la forma u, ui, uj ó uk, donde $u \in \mathcal{U}(\mathbb{Z}[\sqrt{2}])$ (Lema 3.2.2), y el coeficiente de 1 en la expresión de $\eta(\alpha)$ no es 0 por ser α_f par, se deduce fácilmente que $\eta(\alpha) \in \mathbb{Z}[\sqrt{2}]$ y por lo tanto α es central. Entonces tenemos que existe una inclusión de $F_0 f$ en $\mathbb{Q}Gf$ para todo $f \in B$. Por lo tanto F_0 está incluido en el centro de $\mathbb{Q}G$. Además de lo demostrado anteriormente y por los comentarios previos al Teorema 3.1.11 tenemos que F_0 es libre abeliano y que su rango coincide con el cardinal del conjunto B que es fácilmente calculable y vale 2^{2n+k-2}. □

3.2.5. Tipo (h)

Los dos casos que nos quedan por analizar corresponden a los grupos no nilpotentes.

Si H es de tipo (h) entonces $B = \emptyset$ y la demostración es similar al caso en que H es de tipo $(a) - (f)$, con la diferencia que los idempotentes centrales primitivos se construyen de forma diferente y que si e es un idempotente central primitivo de tipo (C), entonces $Ge \cong D_3$ ó D_6 y el isomorfismo $\mathbb{Q}Ge \cong M_2(\mathbb{Q})$ tiene un aspecto diferente de lo que se siguen expresiones de F_e en términos de subgrupos de $\mathrm{GL}_2(\mathbb{Z})$ bien distintos.

Proposición 3.2.6 *Supongamos que H es del tipo (h). Entonces*

1. *Los idempotentes centrales primitivos de $\mathbb{Q}G(1 - \widehat{G'})$ son los elementos de la forma*
$$e = e_{S,\chi,\psi} = \widehat{x^2}\chi(\widehat{S} - \widehat{U})\widehat{Z}_\psi$$
donde S, χ y ψ son tal y como se explica en la notación.

2. *Si $e = e_{S,\chi,\psi}$ y χ no es trivial (y por tanto el orden de x es 4), entonces tenemos que $Ge \cong Q_{12}$ y $\mathbb{Q}Ge \cong \left(\frac{-1,-3}{\mathbb{Q}}\right)$; por tanto e es de tipo (A).*

3. *Si $e = e_{S,\chi,\psi}$ y χ es trivial, entonces*
$$Ge \cong \begin{cases} D_3 & \text{si } \psi \text{ es trivial y} \\ D_6 = D_3 \times C_2 & \text{en otro caso,} \end{cases}$$
y $\mathbb{Q}Ge \cong M_2(\mathbb{Q})$ y por tanto e es de tipo (C).

4. *Si e es un idempotente central primitivo de $\mathbb{Q}G$ de tipo (C) y G no es isomorfo a D_3 entonces:*

   a) $F_e = \begin{cases} \Lambda_3(2^k 3^{n-1}) & \text{si el orden de } x \text{ es 2;} \\ \Lambda_3(2^{k+1}3^{n-1}) & \text{si el orden de } x \text{ es 4;} \end{cases}$

   b) *Si G no es isomorfo a D_3 entonces F_e es libre y*

$$r(F_e) = \begin{cases} 1 + 2 \cdot 3^{3n-4} & \text{si } k = 0 \text{ y el orden de } x \text{ es 2;} \\ 1 + 2^{3k-1}3^{3(n-1)} & \text{si } k \neq 0 \text{ y el orden de } x \text{ es 2;} \\ 1 + 2^{3k+2}3^{3(n-1)} & \text{si el orden de } x \text{ es 4.} \end{cases}$$

Demostración. La afirmación 1 se obtiene como en las demostraciones anteriores como consecuencia de 2 y 3 y de que la suma de los idempotentes $e_{S,\chi,\psi}$ es $1 - \widehat{G'}$.

Sea $e = e_{S,\chi,\psi}$ y $u \in U \setminus S$. Entonces $H_S = \langle x^2, S, Z\rangle$ es un subgrupo normal de G y $\{1, u, u^2, x, xu, xu^2\}$ es una transversal por la derecha de G módulo H_S. Además $he = \pm e$ para todo $h \in H_S$ y $(1 + u + u^2)e = 0$. Deducimos que $\{e, a = ue, b = xe, ab = uexe\}$ es una base de $\mathbb{Q}Ge$ y se verifican las siguientes relaciones:

- Si χ no es trivial, es decir, si se verifican las condiciones de 2, y llamamos $g = x^2ue$ y $h = xe$, entonces $g^3 = h^2$, $hgh^{-1} = g^{-1}$ y por lo tanto $Q_{12} = \langle g, h\rangle = Ge$. Además como $\{e, a, b, ab\}$ es una base de $\mathbb{Q}Ge$, también la forman $\mathbf{1} = e$, $\mathbf{i} = b$, $\mathbf{j} = -b - 2ba$ y $\mathbf{k} = \mathbf{ij}$ que verifican las relaciones $\mathbf{i}^2 = -1$, $\mathbf{j}^2 = -3$ y $\mathbf{ij} = -\mathbf{ji}$. Por tanto $\mathbb{Q}Ge \cong \left(\frac{-1,-3}{\mathbb{Q}}\right)$.

- Si χ es trivial entonces $(1+x)e$ es un divisor de cero de $\mathbb{Q}Ge$. Como la dimensión de $\mathbb{Q}Ge$ sobre $\mathbb{Q}$ es 4, $\mathbb{Q}Ge \cong M_2(\mathbb{Q})$. Tenemos dos opciones dependiendo de que ψ sea o no sea trivial:

  - Si ψ es trivial tenemos que $a^3 = e$, $b^2 = e$ y $bab^{-1} = a^{-1}$, por lo tanto $Ge \cong D_3$.
  - Si ψ no es trivial, entonces $\widehat{Z}_\psi = (\widehat{Z_1} - \widehat{Z})$ donde Z_1 es el núcleo de ψ que es un subgrupo maximal de Z. Sea ahora $z \in Z \setminus Z_1$ y pongamos $c = ze$. Entonces tenemos que $a^3 = 1$, $b^2 = 1$, $bab^{-1} = a^{-1}$, $ac = ca$, $bc = cb$ y $c^2 = 1$, por lo tanto $Ge \cong D_6 = D_3 \times C_2$.

Esto demuestra 2 y 3.

Supongamos ahora que e es de tipo (C). Entonces los siguientes elementos

$$\begin{aligned} e_{11} &= \tfrac{(1+b)}{2}e, & e_{12} &= \tfrac{(1+b)}{2}(2a+1)e, \\ e_{21} &= \tfrac{-1}{3}\tfrac{(1-b)}{2}(2a+1)e, & e_{22} &= \tfrac{(1-b)}{2}e, \end{aligned}$$

forman una base de matrices elementales, es decir $e_{ij}e_{kl} = \delta_{jk}e_{il}$ para todo i, j, k, l y $e_{11} + e_{22} = e$.

Esto implica que existe un único isomorfismo $\mathbb{Q}Ge \cong_\rho M_2(\mathbb{Q})$ que asocia $e_{11} \sim \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $e_{12} \sim \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $e_{21} \sim \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ y $e_{22} \sim \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Además $\{e, a, b, ab\}$ es una base de $\mathbb{Q}Ge$ sobre $\mathbb{Q}$, y se verifican las siguientes relaciones:

$$\begin{aligned} 1-a &= (1-a)e = \tfrac{1}{2}(3e_{11} - e_{12} + 3e_{21} + 3e_{22}) \\ a(1-a) &= a(1-a)e = e_{12} - 3e_{21} \\ b(1-a) &= b(1-a)e = \tfrac{1}{2}(3e_{11} - e_{22} - 3e_{21} - 3e_{22}) \\ ba(1-a) &= ba(1-a)e = e_{12} + 3e_{21} \end{aligned}$$

Por lo tanto el isomorfismo ρ asocia el elemento $(\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ba)(1-a)$ con la matriz

$$\begin{pmatrix} \frac{3}{2}(\beta_0 + \beta_2) & \frac{-1}{2}\beta_0 + \beta_1 - \frac{1}{2}\beta_2 + \beta_3 \\ \frac{3}{2}\beta_0 - 3\beta_1 - \frac{3}{2}\beta_2 + 3\beta_3 & \frac{3}{2}(\beta_0 - \beta_2) \end{pmatrix}.$$

Con el fin de obtener una mejor representación matricial componemos con el automorfismo interno inducido por $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ y después con el inducido por $\begin{pmatrix} 2 & 0 \\ -3 & 1 \end{pmatrix}$. Seguimos llamando ρ al nuevo isomorfismo entre $\mathbb{Q}Ge$ y $M_2(\mathbb{Q})$. Entonces tenemos que el elemento $(\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ba)(1-a)$ está asociado con la matriz

$$\begin{pmatrix} 3(\beta_0 - \beta_1 - \beta_2) & -\beta_0 + 2\beta_1 + 2\beta_2 - \beta_3 \\ 3(\beta_0 - 2\beta_1 - \beta_2 - \beta_3) & 3(\beta_1 + \beta_2) \end{pmatrix}.$$

Todo elemento $\alpha \in \mathbb{Z}G$ se puede escribir como

$$\alpha = \alpha_0 + \alpha_1 u + \alpha_2 x + \alpha_3 ux$$

donde $\alpha_i \in \mathbb{Z}G$ y $sop(\alpha_i) \subseteq H_S$. Además si $h \in H_S$, entonces $he = \pm 1$. Si $\alpha \in F_e = \mathcal{U}(\mathbb{Z}G) \cap (1 + \mathbb{Q}Ge)$ tenemos que $\alpha = \alpha e + (1-e) = 1 + (\alpha - 1)e$ luego $\alpha - 1 \in \Delta(G, \langle u \rangle)e = \mathbb{Z}G(1-a)e$ de donde deducimos que

$$\alpha = 1 + (\alpha - 1)e = 1 + (\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ba)(1-a)e$$

con $\beta_i \in \mathbb{Z}$. Como $(1 + u + u^2)e = 0$ se verifica que $a^2 = -1 - a$ y por tanto $(\alpha - 1)e = (\beta_0 - \beta_1 + (2\beta_1 - \beta_0)a + (\beta_2 + 2\beta_3)b + (\beta_3 - \beta_2)ba)e$. Por otro lado el denominador de e es $2^k 3^n$ si el orden de x es 2 y $2^{k+1}3^n$ si el orden de x es 4. A partir de ahora nos referimos al caso en que el orden de x es 2 en el texto básico y al caso en que el orden de x es 4 en el texto entre paréntesis. Como $\alpha \in \mathbb{Z}$ tenemos que $2^k 3^n$ ($2^{k+1}3^n$) divide a $\beta_0 - \beta_1$, $2\beta_1 - \beta_0$, $\beta_2 + 2\beta_3$ y $\beta_3 - \beta_2$, de donde deducimos que $2^k 3^{n-1}$ ($2^{k+1}3^{n-1}$) divide a β_i para $i = 0, 1, 2$ y 3. Pongamos $\gamma_0 = \frac{\beta_0}{2^k 3^{n-1}}$ ($\gamma_0 = \frac{\beta_0}{2^{k+1}3^{n-1}}$), $\gamma_1 = \frac{\beta_1}{2^k 3^{n-1}}$ ($\gamma_1 = \frac{\beta_1}{2^{k+1}3^{n-1}}$), $\gamma_2 = \frac{\beta_2}{2^k 3^{n-1}}$ ($\gamma_2 = \frac{\beta_2}{2^{k+1}3^{n-1}}$) y $\gamma_3 = \frac{\beta_3}{2^k 3^{n-1}}$ ($\gamma_3 = \frac{\beta_3}{2^{k+1}3^{n-1}}$). Así

$$\rho(\alpha) = 1 + 2^k 3^{n-1} \begin{pmatrix} 3(\gamma_0 - \gamma_1 - \gamma_2) & -\gamma_0 + 2\gamma_1 + 2\gamma_2 - \gamma_3 \\ 3(\gamma_0 - 2\gamma_1 - \gamma_2 - \gamma_3) & 3(\gamma_1 + \gamma_2) \end{pmatrix}$$

$$(\rho(\alpha) = 1 + 2^{k+1}3^{n-1}\begin{pmatrix} 3(\gamma_0-\gamma_1-\gamma_2) & -\gamma_0+2\gamma_1+2\gamma_2-\gamma_3 \\ 3(\gamma_0-2\gamma_1-\gamma_2-\gamma_3) & 3(\gamma_1+\gamma_2)\end{pmatrix})$$

luego $\rho(F_e) \subseteq \Lambda_3(2^{k+2}3^{n-1})$ ($\rho(F_e) \subseteq \Lambda_3(2^{k+2}3^{n-1})$). Para demostrar que se da la igualdad procedemos como en casos anteriores. Basta observar que si

$$A = \begin{pmatrix} 1+2^k3^na & 2^k3^{n-1}b \\ 2^k3^nc & 1+2^k3^nd\end{pmatrix} \in \Lambda_3(2^k3^{n-1})$$

$$(A = \begin{pmatrix} 1+2^{k+1}3^na & 2^{k+1}3^{n-1}b \\ 2^{k+1}3^nc & 1+2^{k+1}3^nd\end{pmatrix} \in \Lambda_3(2^{k+1}3^{n-1}))$$

el siguiente sistema

$$\begin{gathered}\gamma_0-\gamma_1-\gamma_2 = a \\ -\gamma_0+2\gamma_1+2\gamma_2-\gamma_3 = b \\ \gamma_0-2\gamma_1-\gamma_2-\gamma_3 = c \\ \gamma_1+\gamma_2 = d\end{gathered}$$

tiene soluciones enteras. Más concretamente el sistema es equivalente a

$$\begin{gathered}\gamma_0-\gamma_1-\gamma_2 = a \\ \gamma_1+\gamma_2-\gamma_3 = a+b \\ \gamma_2-2\gamma_3 = b+c \\ \gamma_3 = d-b\end{gathered}$$

cuyas soluciones son enteras. Luego $\rho(F_e) = \Lambda_3(2^k3^{n-1})$ ($\rho(F_e) = \Lambda_3(2^{k+1}3^{n-1})$). Si $G \cong D_3$ entonces $n = 1$, $k = 0$ y el orden de x es 2. Por tanto $F_e \cong \Lambda_3(1)$ que no es libre pues contiene el elemento $\begin{pmatrix} -2 & -3 \\ 3 & 1\end{pmatrix}$ que tiene orden 3. En caso contrario o bien $k \geq 1$ con lo que $\rho(F_e) = \Lambda_3(2)$ o bien el orden de x es 4 ó $n > 1$ con lo que $\rho(F_e) = \Gamma(3)$. Como tanto $\Gamma(3)$ como $\Lambda_3(2)$ son libres deducimos que $\rho(F_e)$ es libre y por tanto también lo es F_e. Veamos ahora cual es el rango de F_e para $G \ncong D_3$. Si $k = 0$ como $G \ncong D_3$ tenemos que $n \geq 2$ y por lo tanto $\Gamma(3^n)$ es un subgrupo de índice 3 de $\Lambda_3(3^{n-1})$. Por otro lado $\Gamma(3^n)$ tiene índice $3^{3(n-1)}$ en $\Gamma(3)$, siendo este último un grupo libre de rango 3. Luego por el Teorema 3.2.1 el rango de $\Lambda_3(3^{n-1})$ vale $1+2\cdot 3^{3n-4}$. Si $k \neq 0$ entonces argumentos similares muestran que $\Lambda_3(2^k3^{n-1})$ ($\Lambda_3(2^{k+1}3^{n-1})$) es un subgrupo libre de $\widehat{\Gamma}(2)$ de rango $1+2^{3k-1}3^{3(n-1)}$ ($1+2^{3k+2}3^{3(n-1)}$). □

En la demostración de la Proposición 3.2.6 hemos visto la razón de la exclusión de D_3. Para este grupo sólo hay un idempotente de tipo C: $e = 1-\widehat{a}$ y F_e no es libre aunque si que contiene un subgrupo libre, a saber $V = (1+\Delta(G)\Delta(G,G'))\cap\mathcal{U}(\mathbb{Z}G)$, de hecho V es precisamente el complemento normal de D_3 que aparece en el Teorema 3.1.4.

3.2.6. Tipo (i)

Sólo nos queda considerar el caso en que H es de tipo (i). Éste y el caso en que H es de tipo (g) son los dos únicos casos en que $\mathbb{Q}G$ tiene idempotentes centrales primitivos de tipo (B), y por tanto son los únicos casos en que $F_0 \neq 1$. La demostración en el caso en que H es de tipo (i) son como en el que H es de tipo (g), con diferencias del mismo estilo a las explicadas para el tipo (h) con respecto a los tipos $(a)-(f)$.

Proposición 3.2.7 *Supongamos que H es de tipo (i). Entonces:*

1. *Los idempotentes centrales primitivos de $\mathbb{Q}G(1-\widehat{G'})$ de tipo (A) son de la forma*
$$e = (1-\widehat{x^2})\widehat{U}\widehat{Z}_\psi$$
donde ψ es tal y como se explica en la notación de la Subsección 3.2.1. Además $Ge = Q_8$ y por tanto $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q})$.

2. *Los idempotentes centrales primitivos de $\mathbb{Q}G$ de tipo (C) son de la forma*
$$e = e_{S,\chi,\psi} = \widehat{x^2}(\widehat{S}-\widehat{U})\widehat{xy}_\chi\widehat{Z_\psi}$$
donde S, χ y ψ son tal y como se explican en la notación de la Subsección 3.2.1.

3. *Si e es un idempotente central primitivo de $\mathbb{Q}G$ de tipo (C), $F_e \simeq \Lambda_3(2^{k+2}3^{n-1})$ que es libre de rango $1+2^{3k+5}3^{3(n-1)}$.*

4. *Los idempotentes centrales primitivos de tipo (B) son de la forma*
$$f = f_{S,\psi} = (1-\widehat{x^2})(\widehat{S}-\widehat{U})\widehat{Z}_\psi$$
donde S y ψ son tal y como se explica en la notación de la Subsección 3.2.1.

5. *$f_B = (1-\widehat{x^2})(1-\widehat{U})$ y si $F_0 = \mathcal{U}(\mathbb{Z}G)\cap(1+\mathbb{Q}Gf_B)$, entonces F_0 está incluido en el centro de $\mathbb{Q}G$ y es libre abeliano de rango $1+2^{k-1}(3^n-1)$.*

Demostración.

1. Sean $e = (1-\widehat{x^2})\widehat{U}\widehat{Z}_\psi$ y $H_S = \langle x^2, U, Z\rangle$. Entonces H_S es un subgrupo normal de G y $\{1,x,y,xy\}$ es un transversal de G módulo H_S. Además $he = \pm e$ para todo $h \in H_S$; $\{e, xe, ye, xye\}$ es una base de $\mathbb{Q}Ge$ y se verifica que $x^2e = y^2e = -e$, con lo que en tal caso $Ge \cong Q_8$ y $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q})$, lo que demuestra la afirmación 1.

2. Sean $e = e_{S,\chi,\psi} = \widehat{x^2}(\widehat{S} - \widehat{U})\widehat{xy}_\chi \widehat{Z}_\psi$ y $u \in U \setminus S$. Entonces $H_S = \langle xy, x^2, S, Z\rangle$ es un subgrupo normal de G y $\{1, u, u^2, x, xu, xu^2\}$ es un transversal por la derecha de G módulo H_S. Además $he = \pm e$ para todo $h \in H_S$, $(1+u+u^2)e = 0$ y $\{e, a = ue, b = xe, ab = uexe\}$ es una base de $\mathbb{Q}Ge$ y se verifican las siguientes relaciones: $\pm e = x^2 e \neq y^2 e = \pm e$ con lo que en tal caso $Ge \cong D_8$ y $\mathbb{Q}Ge \cong M_2(\mathbb{Q})$.

3. La demostración de 3 es análoga a la de la Proposición 3.2.6 y no la escribiremos para evitar repeticiones.

4. Que $f = f_{S,\psi}$ es un idempotente central es obvio. Mostraremos que es primitivo identificando $\mathbb{Q}Gf$ con $\mathbb{H}(\mathbb{Q}(\sqrt{3}))$ que es un álgebra simple. En efecto, sean $X = xf$, $Y = yf$ y $W = wf$, donde $w \in U \setminus S$. Entonces $X^2 = Y^2 = -e$, $1 + W + W^2 = 0$, $xW = W^2X$, $YW = W^2Y$ y $XYW = WXY$. Entonces el centro de $\mathbb{Q}Gf$ es $K = \mathbb{Q}(a)$ donde $a = XY(1 + 2W)$ satisface que $a^2 = 3$ y $\{f, X, Y, XY\}$ es una base de $\mathbb{Q}Gf$ sobre K. Por tanto existe un homomorfismo de algebras $\lambda : \mathbb{Q}Gf \to \mathbb{H}(K)$ tal que $\lambda(X) = \mathbf{j}$, $\lambda(Y) = \mathbf{K}$ y $\lambda(W) = \frac{-1+\sqrt{3}\mathbf{i}}{2}$. Luego $\mathcal{B} = \{f, X, Y, W, XY, WX, WY, WXY\}\}$ es una $\mathbb{Q}$-base de $\mathbb{Q}Gf$. Así el homomorfismo λ dado por

$$\begin{aligned}\lambda(\textstyle\sum_{g\in\mathcal{B}} \alpha_g g) \;=\; & \tfrac{1}{2}[2\alpha_f - \alpha_W - \sqrt{3}\alpha_{WXY} + (2\alpha_{XY} - \alpha_{WXY} + \sqrt{3}\alpha_W)\mathbf{i} \\ & (2\alpha_X - \alpha_{WX} - \sqrt{3}\alpha_{WY})\mathbf{j} + (2\alpha_Y - \alpha_{WY} + \sqrt{3}\alpha_{WX})\mathbf{k}]\end{aligned}$$

es un isomorfismo de anillos.

5. La demostración de 5 es análoga a la de la Proposición 3.2.5 y no la escribiremos para evitar repeticiones.

□

Los dos únicos grupos para los que $F_0 \neq 1$, o lo que es lo mismo, que poseen idempotentes centrales primitivos de tipo (B), son aquellos en los que H es de tipo (g) e (i). En las demostraciones de las Proposiciones 3.2.5 y 3.2.7 hemos obtenido isomorfismos entre $\mathbb{Q}Gf$ y $\mathbb{H}(\mathbb{Q}(\sqrt{d}))$ con $d = 2$ ó 3 para cada idempotente central primitivo f de $\mathbb{Q}G$ de tipo (B). Estos isomorfismos nos serán de utilidad en la siguiente sección por lo que los incluiremos en un lema para uso futuro.

Lema 3.2.8 *1. Supongamos que H es de tipo (g). Sea f un idempotente central primitivo de $\mathbb{Q}G$ de tipo (B). Entonces $\mathcal{B} = \{f, b, b^2, b^3, a, ab, ab^2, ab^3\}$, donde $a = xf$ y $b = y_1 f$, es una base entera de $\mathbb{Z}Gf$ y la aplicación $\eta : \mathbb{Q}Gf \to \mathbb{H}(\mathbb{Q}[\sqrt{2}])$ dada por*

$$\begin{aligned}\eta(\textstyle\sum_{g\in\mathcal{B}} \alpha_g g) \;=\; & \alpha_f + \tfrac{\sqrt{2}}{2}(\alpha_b - \alpha_{b^3}) + (\alpha_a + \tfrac{\sqrt{2}}{2}(\alpha_{ab} - \alpha_{ab^3}))\mathbf{i} + \\ & (\alpha_{b^2} + \tfrac{\sqrt{2}}{2}(\alpha_b + \alpha_{b^3}))\mathbf{j} + (\alpha_{ab^2} + \tfrac{\sqrt{2}}{2}(\alpha_{ab} + \alpha_{ab^3}))\mathbf{k}\end{aligned}$$

es un isomorfismo de anillos.

2. *Supongamos que H es de tipo (i). Sea f un idempotente central primitivo de $\mathbb{Q}G$ de tipo (B). Entonces $\mathcal{B} = \{f, X, Y, XY, W, WX, WY, WXY\}$, donde $X = xf$, $Y = yf$ y $W = wf$ y $w \in U \setminus S$, es una base entera de $\mathbb{Z}Gf$ y la aplicación $\lambda : \mathbb{Q}Gf \to \mathbb{H}(\mathbb{Q}[\sqrt{3}])$ dada por*

$$\begin{aligned}\lambda(\textstyle\sum_{g\in\mathcal{B}} \alpha_g g) &= \tfrac{1}{2}[2\alpha_f - \alpha_W - \sqrt{3}\alpha_{WXY} + (2\alpha_{XY} - \alpha_{WXY} + \sqrt{3}\alpha_W)\mathbf{i} \\ &\quad (2\alpha_X - \alpha_{WX} - \sqrt{3}\alpha_{WY})\mathbf{j} + (2\alpha_Y - \alpha_{WY} + \sqrt{3}\alpha_{WX})\mathbf{k}]\end{aligned}$$

es un isomorfismo de anillos.

3.3. Optimalidad

En esta sección demostraremos el Teorema 3.1.12.

Si N es un subgrupo normal de G, denotaremos por $\Delta(G, N)$ a $\Delta_{\mathbb{Z}}(G, N)$ y por $\Delta(G)$ a $\Delta(G, G)$ (véase la Sección 1.4).

Ingredientes importantes en nuestra demostración son el Lema 30,6 y el Teorema 31,3 de [65]. Estos dos resultados juntos nos proporcionan el siguiente teorema.

Teorema 3.3.1 *Sea A un subgrupo abeliano normal de G tal que G/A es abeliano y tiene exponente 2, 3, 4 ó 6. Entonces $\mathcal{U}(\mathbb{Z}G) = \pm V \rtimes G$ donde $V = \mathcal{U}(\mathbb{Z}G) \cap (1 + \Delta(G)\Delta(G, A))$ y V es libre de torsión.*

A lo largo de toda la sección G es uno de los grupos no abelianos del Teorema 3.1.9 y $V = \mathcal{U}(\mathbb{Z}G) \cap (1 + \Delta(G)\Delta(G, G'))$. Obsérvese que G satisface las condiciones del Teorema 3.3.1 para $A = G'$, y por lo tanto V es un complemento normal libre de torsión de las unidades triviales de $\mathcal{U}(\mathbb{Z}G)$. Es bien conocido que V es libre no abeliano si $G = D_4$ ó $G = D_3$ (de hecho V es el grupo de los Teoremas 3.1.4 y 3.1.5).

Para demostrar el Teorema 3.1.12 necesitamos varios lemas técnicos.

Lema 3.3.2 *Para todo $e \in C$, Ve es libre de torsión.*

Demostración. Sea $v \in V = \mathcal{U}(\mathbb{Z}G) \cap (1 + \Delta(G)\Delta(G, G'))$ y $e \in C$ un idempotente central primitivo. Supongamos primero que H es de uno de los tipos $(a) - (g)$. Entonces como $\Delta(G, G')$ es el ideal de $\mathbb{Z}G$ generado por los elementos de la forma $1-g$ con $g \in G'$, utilizando la expresión que se ha obtenidopara e en las Proposiciones 3.2.3, 3.2.4 y 3.2.5 es fácil ver que $ve = e + 2\alpha e$ con $\omega(\alpha) = 0$, donde ω denota el homomorfismo de aumento. Entonces por las Proposiciones 3.2.3, 3.2.4 y 3.2.5 de la Sección 3.2 tenemos que la representación matricial de ve es

$$\begin{pmatrix} 1 + 2(\alpha_0 + \alpha_2 - \alpha_1 - \alpha_3) & 4(\alpha_2 - \alpha_1) \\ 2(\alpha_1 + \alpha_3) & 1 + 2(\alpha_0 + \alpha_1 - \alpha_2 + \alpha_3) \end{pmatrix}$$

donde $\alpha_0+\alpha_2+\alpha_1+\alpha_3 \equiv \omega(\alpha) = 0 \bmod 2$. Por lo tanto la representación matricial de ve pertenece a $(1+2\begin{pmatrix} 2\mathbb{Z} & 2\mathbb{Z} \\ \mathbb{Z} & 2\mathbb{Z} \end{pmatrix}) \cap \mathrm{SL}_2(\mathbb{Z}) = X$. Como $-I \notin X$, X es isomorfo a su imagen en $\widehat{\Gamma}(2)$ y éste es libre y por tanto libre de torsión. De aquí deducimos que ve tiene orden infinito

Si H es de tipo (h) ó (i), entonces se razona de forma similar salvo que en este caso $ve = e+(\beta_0 e+\beta_1 a+\beta_2 b+\beta_3 ba)(1-a)e$ con $\beta_i \in \mathbb{Z}$, $\beta_0+\beta_1+\beta_2+\beta_3 \equiv 0 \bmod 3$ y a, b como en las Proposiciones 3.2.6 y 3.2.7. Entonces la representación matricial de ve es

$$\begin{pmatrix} 3(\beta_0-\beta_1-\beta_2) & -\beta_0+2\beta_1+2\beta_2-\beta_3 \\ 3(\beta_0-2\beta_1-\beta_2-\beta_3) & 3(\beta_1+\beta_2) \end{pmatrix}$$

que pertenece $\Gamma(3)$ que es libre y por lo tanto libre de torsión. □

Definamos ahora

$$\widetilde{F}_0 = \{u \in \mathcal{U}(\mathbb{Z}G) : ue = e \text{ para todo } e \in C\}$$

y para todo $e \in C$, sea

$$\widetilde{F}_e = \{u \in \mathcal{U}(\mathbb{Z}G) : uf = f \text{ para todo } f \in C \setminus \{e\}\}.$$

Obviamente $\widetilde{F}_0 = \widetilde{F}_{e_1} \cap \widetilde{F}_{e_2}$ para todo par de idempotentes distintos e_1 y e_2 en C. Está claro que $F_0 \subseteq \widetilde{F}_0$ y para cada $e \in C$, $F_e \subseteq \widetilde{F}_e$. El punto crucial en la demostración consiste en demostrar que $\widetilde{F}_e \cap V \subseteq F_0 \times F_e$ y $\widetilde{F}_0 \cap V \subseteq F_0$ y en que si $E = E_0 \times \prod_{j\in J} E_j$ como en el Teorema 3.1.12, entonces $E_0 \subseteq \widetilde{F}_0$ y podemos suponer que $J = C$ y $E_j \subseteq \widetilde{F}_j$ para cada $j \in J$.

Lema 3.3.3 *Si f es un idempotente central primitivo de $\mathbb{Q}G$, tal que $\mathbb{Q}Gf$ es conmutativo o isomorfo a $\mathbb{H}(\mathbb{Q})$, entonces $Vf = f$.*

Demostración. En efecto, si $\mathbb{Q}Gf$ es conmutativo, entonces $f(1-\widehat{G'}) = 0$ y la afirmación es evidente. Si $\mathbb{Q}Gf \simeq \mathbb{H}(\mathbb{Q})$ entonces tal y como vimos en las Proposiciones 3.2.3, 3.2.4 y 3.2.7 se verifica que $Gf \cong Q_8$. Por lo tanto existen elementos $g, h \in G$ tales que $a = gf$ y $b = hf$ verifican $a^2 = -f$, $b^2 = -f$ y $ab = -ba$. Esto implica que existe un único isomorfismo $\mathbb{Q}Ge \cong_\varphi \mathbb{H}(\mathbb{Q})$ que asocia a con $\mathbf{i}$ y b con $\mathbf{j}$. Además $T = \{f, a, b, ab\}$ es una base entera de $\mathbb{Z}Gf$. Debido a cómo son estos idempotentes centrales primitivos f (véanse las Proposiciones 3.2.3, 3.2.4 y 3.2.7), para todo $g \in G'$ se verifica que $gf = \pm f$. Como consecuencia de que $\Delta(G, G')$ es el ideal de $\mathbb{Z}G$ generado por los elementos de la forma $1-g$ con $g \in G'$, tenemos que todo elemento de $\Delta(G)\Delta(G, G')f$ es de la forma $2\alpha f$ para algún $\alpha \in \Delta(G)$. Más aún $\alpha f = \sum_{t\in T} \alpha_t t$, donde $\alpha_t \in \mathbb{Z}W$, siendo W el núcleo de la aplicación canónica $G \to Gf \to Gf/\langle a^2\rangle$. Entonces $\alpha_t f = \beta_t f$ donde $\beta_t \in \mathbb{Z}$ y $\beta_t \equiv \omega(\alpha_t) \bmod 2$ donde $\omega : \mathbb{Z}G \to \mathbb{Z}$ denota el

homomorfismo de aumento. Por lo tanto $\sum_{t\in T}\beta_t \equiv \omega(\alpha) = 0 \bmod 2$. Así, si $u \in V$, entonces $uf = 1+2\sum_{t\in T}\beta_t t$, con $\sum_t \beta_t$ par. Luego $\varphi(uf) = 1+2(\beta_f+\beta_a\mathbf{i}+\beta_b\mathbf{j}+\beta_{ab}\mathbf{k})$ es una unidad en $\mathbb{H}(\mathbb{Z})$. Como las únicas unidades de $\mathbb{H}(\mathbb{Z})$ son ± 1, $\pm i$, $\pm j$ y $\pm ij$ (Lema 3.2.2), concluimos que $u = f$. $\square$

Recordemos que en el enunciado del Teorema 3.1.12 se han excluido los grupos D_3, D_4, Q_{12} y Q_{16}. La exclusión de los grupos D_3 y D_4 ya aparecía en el Teorema 3.1.11 y correspondientemente se reflejaba en las Proposiciones 3.2.6 y 3.2.3 respectivamente. La exclusión del grupo Q_{12} aparece por primera vez en el siguiente lema y la del grupo Q_{16} aparece en el lema posterior.

Lema 3.3.4 *Si $G \ncong Q_{12}$, $e \in C$ y $f \in A$, entonces $(\widetilde{F}_e \cap V)f = f$.*

Demostración. Por el Lema 3.3.3, podemos suponer que $\mathbb{Q}Gf$ no es conmutativo y que $\mathbb{Q}Gf \neq \mathbb{H}(\mathbb{Q})$. Esto junto con la descripción de los idempotentes centrales primitivos de $\mathbb{Q}G$ que aparecen en las proposiciones de la sección anterior, implica que H es de tipo (h) con x de orden 4 y $\mathbb{Q}Gf$ es isomorfo al álgebra de cuaterniones generalizada

$$A = \mathbb{Q}[i, j : i^2 = -1, j^2 = -3, ij = k = -ji] = \left(\frac{-1,-3}{\mathbb{Q}}\right).$$

Por la Proposición 3.2.6

$$e = e_{S,\psi} = \widehat{x^2}(\widehat{S} - \widehat{U})\widehat{Z_\psi}$$

y

$$f = f_{S_1,\psi_1} = (1 - \widehat{x^2})(\widehat{S_1} - \widehat{U})\widehat{Z_{\psi_1}},$$

donde S y S_1 son dos subgrupos maximales de U y $\psi, \psi_1 \in Z^*$. Fijemos $y \in U \setminus S_1$. Entonces $B_1 = \{f, a = xf, b = yf, ab\}$ es una base entera de $\mathbb{Z}Gf$ y existe un isomorfismo $\phi : \mathbb{Q}Gf \to A$ tal que $\phi(a) = \mathbf{i}$ y $\phi(b) = \frac{1+\mathbf{j}}{2}$ (esto lo vimos con detalle en la demostración de la Proposición 3.2.6). Por lo tanto $\phi(\mathbb{Z}Gf)$ es isomorfo a $\mathbb{Z}[\mathbf{i}, \frac{1+\mathbf{j}}{2}]$ visto como subanillo de A.

Sea $u \in V \cap \widetilde{F}_e$. Tenemos que demostrar que $uf = f$.

Supongamos primero que $(S, \psi) \neq (S_1, \psi_1)$. Sea $e' = e_{S_1,\psi_1}$. Entonces $B_2 = \{e', xe', ye', xye'\}$ es una base entera de $\mathbb{Z}Ge'$. Además para un $\alpha \in \mathbb{Z}G$ los coeficientes de αf y $\alpha e'$ en las bases B_1 y B_2 son congruentes módulo 2. Como $u \in \widetilde{F}_e$, tenemos que $(u-1)e' = 0$, y así los coeficientes de $(u-1)f$ en la base B_1 son pares. Por lo tanto $uf = 1 + 2(\sum_{t\in B_1}\alpha_t t)$ es una unidad en $\mathbb{Z}Gf \cong \mathbb{Z}[\mathbf{i}, \frac{1+\mathbf{j}}{2}]$. Por el Lema 3.2.2, $uf = \pm f$. Si $uf = -f$, entonces $(u-1)f = -2f$. Como $u \in V$, tenemos que $u - 1 \in \Delta(G)\Delta(G, G')$. Por otro lado como para un $g \in G'$ se verifica que $(1-g)f = (1-y)\frac{1-x^2}{2}\widehat{S_1}\widehat{Z_{\psi_1}}$ podemos escribir $(u-1)f = (\alpha_0 + \alpha_1 x)\frac{1-x^2}{2}\widehat{S_1}\widehat{Z_{\psi_1}}$ (recuérdese que $\Delta(G, G')$ es el ideal de $\mathbb{Z}G$ generado por los elementos $1-g$ con $g \in G'$) donde $\alpha_0, \alpha_1 \in \mathbb{Z}G$ y sus soportes están incluidos en una transversal fijada

de G módulo $\langle x^2, S_1, Z\rangle$ que contiene el 1. Entonces el coeficiente del 1 en $(u-1)f$ es $\frac{\beta}{2^{k+1}3^{m-1}}$, donde β es el coeficiente del 1 en α_0. Sin embargo el coeficiente de $-2f$ es $-\frac{1}{2^k 3^m}$, lo que nos lleva a contradicción. Luego $uf = f$ tal y como queríamos demostrar.

Supongamos ahora que $S = S_1$. Por el Lema 3.3.3 y el párrafo anterior tenemos que

$$u - 1 = (u-1)(f_{S,\psi} + e_{S,\psi}) = (u-1)(\widehat{S} - \widehat{U})\widehat{Z_\psi} = \sum_{i=0}^{3} \alpha_i x^i (\widehat{S} - \widehat{U})\widehat{Z_\psi}$$

con $\alpha_i = \sum_{j=0}^{2} \alpha_{ij} y^j \in \Delta(\langle y\rangle)$. Entonces $\alpha_{i0} + \alpha_{i1} + \alpha_{i2} = 0$ y por lo tanto el coeficiente de $x^i y^j$ en $u-1$ es

$$\frac{3\alpha_{ij} - \alpha_{i0} - \alpha_{i1} - \alpha_{i2}}{2^k 3^n} = \frac{\alpha_{ij}}{2^k 3^{n-1}} \in \mathbb{Z}.$$

Luego $2^k 3^{n-1} \mid \alpha_{ij}$ y así $uf \in f + 2^k 3^{n-1}\mathbb{Z}Gf$ es una unidad de $\mathbb{Z}Gf$. Si $n > 1$, entonces por el Lema 3.2.2 $uf = f$. Supongamos ahora que $n = 1$. Como estamos suponiendo que $G \ncong Q_{12}$, entonces $k \geq 1$ y otra vez por el Lema 3.2.2 tenemos que $uf = f$. Esto finaliza la demostración del lema. □

Lema 3.3.5 *Si $G \ncong Q_{12}$ y $G \neq Q_{16}$, entonces para todo $e \in C$, $\widetilde{F}_e \cap V \subseteq F_0 \times F_e$ y $\widetilde{F}_0 \cap V \subseteq F_0$.*

Demostración. Sea $e \in C$.

Veamos primero que $\widetilde{F}_0 \cap V \subseteq F_0$. Supongamos que $\widetilde{F}_0 \cap V \not\subseteq F_0$. Entonces existe un idempotente central primitivo $f \in A$ tal que $(\widetilde{F}_0 \cap V)f \neq f$. Del Lema 3.3.3 se tiene que $\mathbb{Q}Gf$ no es conmutativo ni isomorfo a $\mathbb{H}(\mathbb{Q})$. Por tanto $\mathbb{Q}Gf \cong \left(\frac{-1,-3}{\mathbb{Q}}\right)$ con lo que H es de tipo (h) con el orden de x igual a 4. Como $\widetilde{F}_0 = \widetilde{F}_{e_1} \cap \widetilde{F}_{e_2}$, del Lema 3.3.4 se tiene que $|C| = 1$, es decir $G = C_3 \rtimes C_4$, caso que estamos excluyendo. Por lo tanto $\widetilde{F}_0 \cap V \subseteq F_0$.

Demostremos ahora que $\widetilde{F}_e \cap V \subseteq F_0 \times F_e$ para todo $e \in C$. Si H no es ni de tipo (g) ni (i), entonces $B = \emptyset$ y el resultado es consecuencia directa del Lema 3.3.4.

Supongamos que H es de tipo (g) y $G \ncong Q_{16}$, así que $n > 1$ ó $k > 0$. La suma de los elementos de B es $f_B = 1 - \widehat{x^2}$ (véase la Proposición3.2.5). Sin pérdida de generalidad podemos suponer que

$$e = \widehat{R}(\widehat{S} - \widehat{G'})\widehat{Z_\psi}$$

donde $R = \langle y_2, \ldots, y_n\rangle$, $S = \langle y_2^2, \ldots, y_n^2\rangle$ y $\psi \in Z^*$. El soporte de e es $L = \langle y_1^2, y_2, \ldots, y_n\rangle \times Z$ y $T_e = \{1, x, y_1, xy_1\}$ es una transversal de G módulo L.

Sean $u \in \widetilde{F}_e \cap V$ y $\beta = u - 1$. Si $l \in L$, entonces $le = \pm e$. Por lo tanto, $\beta e = \alpha' e$ con $\alpha' \in \mathbb{Z}G$, $sop(\alpha') \subseteq T_e$. Por el Lema 3.3.4 tenemos que $u = 1 + \alpha' e + \beta f_B$. Es suficiente demostrar que $\beta_g - \beta_{gx^2}$ es par para todo $g \in G$ pues esto implica que $\beta f_B \in \mathbb{Z}G$ y así $u = (1 + \alpha' e)(1 + \beta f_B)$ con $1 + \alpha' e \in F_e$ y $1 + \beta f_B \in F_0$.

Sea $g \in G$ y $t \in T_e$ tal que $g \equiv t \bmod L$. Entonces el coeficiente β_g de g en $u - 1$ es

$$\pm \frac{\alpha'_t}{2^{2n+k}} + \frac{\beta_g - \beta_{gx^2}}{2}.$$

Por lo tanto $\alpha'_t = 2^{2n+k-1}\alpha_t$ donde $\alpha_t = \pm(\beta_g + \beta_{gx^2})$ y por tanto $\alpha_t \equiv \beta_g - \beta_{x^2 g} \bmod 2$ si $g \equiv t \bmod L$. Luego es suficiente demostrar que α_t es par para todo $t \in T_e$.

Para conseguir nuestro objetivo consideremos la imagen de uf bajo el isomorfismo $\phi = \phi_f : \mathbb{Q}Gf \simeq \mathbb{H}(\mathbb{Q}(\sqrt{2}))$, dado en el Lema 3.2.8, para todo $f \in B$. Vamos a utilizar la notación de ese lema. Obsérvese que un elemento de B es de la forma $f = f_{\xi,\chi} = (1 - \widehat{x^2})\widehat{K(\xi)_{\rho_{\xi,\chi}}}$ (véase la Proposición 3.2.5). Entonces $\beta f = \sum_{tf \in \mathcal{B}} \gamma_{tf} tf$ donde

$$\gamma_{tf} = \sum_{k \in K(\xi)} \rho_{\xi,\chi}(k)(\beta_{tk} - \beta_{tkx^2})$$

donde $t \in \{1, x, y_1, y_1^2, y_1^3, xy_1, xy_1^2, xy_1^3\}$. Obsérvese que $K(\xi) \cap L$ tiene índice 2 en $K(\xi)$ y por lo tanto el cardinal de $K(\xi) \cap L$ es $2^{2(n-1)+k}$. Como $n > 1$ ó $k > 0$, este cardinal es par. Como si $g \equiv t \bmod L$ tenemos que $\alpha_t \equiv \beta_g - \beta_{gx^2}$ tenemos que si $g_1 \equiv g_2 \bmod L$ entonces $\beta_{g_1} - \beta_{g_1 x^2} \equiv \beta_{g_2} - \beta_{g_2 x^2} \bmod 2$, de donde deducimos que

$$\gamma_{tf} = \sum_{k \in K(\xi) \cap L} \rho_{\xi,\chi}(k)(\beta_{tk} - \beta_{tkx^2}) + \sum_{k \in K(\xi) \setminus L} \rho_{\xi,\chi}(k)(\beta_{tk} - \beta_{tkx^2})$$

es par. Por tanto $\phi(\mathbb{Z}Gf) \subseteq \mathbb{H}(\mathbb{Z}[\sqrt{2}])$. Como toda unidad de $\mathbb{H}(\mathbb{Z}[\sqrt{2}])$ es de la forma u, ui, uj or uk con u una unidad de $\mathbb{Z}[\sqrt{2}]$ (véase Lema 3.2.2) deducimos que

$$\gamma_a = \gamma_{b^2} = \gamma_{ab^2} = \gamma_{ab} = \gamma_{ab^3} = \gamma_b + \gamma_{b^3} = 0$$

ya que $\phi(uf)$ es una unidad de $\mathbb{H}(\mathbb{Z}[\sqrt{2}])$ y si expresamos $\phi(uf)$ es la base $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ donde vemos $\mathbb{H}(\mathbb{Q}(\sqrt{2}))$ como espacio vectorial sobre $\mathbb{Q}(\sqrt{2})$, entonces el coeficiente de 1 es $1 + \gamma_f + \frac{\sqrt{2}}{2}(\gamma_b - \gamma_b^3)$ que no es cero pues γ_f es par (véase Proposición 3.2.5). Escribiendo estas ecuaciones en términos de los β's obtenemos un sistema de ecuaciones lineales

$$\sum_{h \in K(\xi)} \rho_{\xi,\chi}(h)(\beta_{th} - \beta_{thx^2}) = 0,$$

para todo $t = x, y_1^2, xy_1^2, xy_1, xy_1^3$. Fijados $\xi \in K^*$ y $k \in K$ el anterior sistema de ecuaciones lineales se convierte en

$$\sum_{t_1 \in T_\xi} \chi(t_1) \sum_{k \in K} \xi(k)(\beta_{tt_1 k} - \beta_{tt_1 kx^2}) = 0.$$

Pero la matriz $(\chi(t_1))_{t_1\in T_\xi,\chi\in(K(\xi)/K)^*}$ es una matriz de Hadamard, es decir una matriz de 1's y -1's con filas ortogonales. En particular su determinante es distinto de cero y así

$$\sum_{k\in K}\xi(k)(\beta_{tt_1k}-\beta_{tt_1kx^2})=0$$

para todo $\xi\in K^*$ y $t_1\in K$. Usando que la matriz $(\xi(k))_{\xi\in K^*,k\in K}$ es también una matriz de Hadamard, deducimos que $\beta_{tk}-\beta_{tkx^2}=0$ para todo $k\in K(\xi)$. Por lo tanto si g es congruente con y_1^2, x, xy_1, xy_1^2, o xy_1^3 módulo $K(\xi)$ para algún $\xi\in K^*$ entonces $\beta_g-\beta_{gx^2}=0$. En particular $\alpha_1\equiv\beta_{y_1^2}-\beta_{y_1^2x^2}=0 \bmod 2$, $\alpha_x\equiv\beta_x-\beta_{x^3}=0 \bmod 2$ y $\alpha_{xy_1}\equiv\beta_{xy_1}-\beta_{x^3y_1}=0 \bmod 2$. Falta demostrar que α_{y_1} es par. Por un lado tenemos que $y_1y_2\equiv y_1^2 \bmod K(\xi)$, y por otro si seleccionamos $\xi\in K^*$ tal que $\xi(y_1^2y_2^2)=-1$, entonces $y_1^{-1}y_2\in K(\xi)$ y por lo tanto $y_1y_2\equiv y_1^2 \bmod K(\xi)$. Así $\alpha_{y_1}\equiv\beta_{y_1y_2}-\beta_{x^2y_1y_2}=0 \bmod 2$. Esto acaba la demostración para este caso.

Supongamos ahora que H es de tipo (i). Entonces $f_B=(1-\widehat{x^2})(1-\widehat{U})$ y $e=e_{S,\chi,\psi}=\widehat{x^2}(\widehat{S}-\widehat{U})\widehat{xy}_\chi\widehat{Z}_\psi$, donde S es un subgrupo maximal de U, $\chi\in\langle xy\rangle^*$ y $\phi\in Z^*$. Para simplificar un poco la demostración supondremos que χ y ψ son los homomorfismos triviales, es decir $e=(\widehat{S}-\widehat{U})\widehat{xy}\widehat{Z}$. El caso general se demuestra de forma similar.

Sean $v\in\tilde{F}_e\cap V$ y $\beta=v-1$. Entonces $\beta=\beta e+\beta f_B$. Como en la demostración del caso en que H es de tipo (g) bastará demostrar que $\beta f_B\in\mathbb{Z}G$. Como $e,f_B\in\Delta_{\mathbb{Q}}(G,U)$, tenemos que $\beta\in\Delta_{\mathbb{Z}}(G,U)$. Por tanto $\beta f_B=\beta(1-\widehat{x^2})$. Para cada $g\in G$ sea $\delta_g=\beta_g-\beta_{gx^2}$ y $\delta=\sum_{g\in G}\delta_g g$. Entonces $\beta f_B=\frac{\delta}{2}$ y por tanto alcanzaremos nuestro objetivo demostrando que todos los δ_g son pares.

Fijaremos un elemento a de $U\setminus S$. Utilizando que $ge=e$ para todo $g\in\langle xy,S,Z\rangle$ y que $(1+a+a^2)e=0$ es fácil ver que $\beta e=\alpha' e$ para un $\alpha'\in\mathbb{Z}G$ cuyo soporte está incluido en $\{1,x,a,ax\}$. Si $t\in\{1,x\}$ y $l\in\langle xy,S,Z\rangle$, entonces los coeficientes de tl, atl y a^2tl en $2^{k+2}3^n\alpha' e$ son respectivamente $2\alpha'_t-\alpha'_{at}$, $-\alpha'_t+2\alpha'_{at}$ y $-\alpha'_t-\alpha'_{at}$. Por tanto

$$\begin{aligned}2\alpha'_t-\alpha'_{at}+2^{k+1}3^n\delta_{tl} &= 2^{k+2}3^n\beta_{tl}\\ -\alpha'_t+2\alpha'_{at}+2^{k+1}3^n\delta_{atl} &= 2^{k+2}3^n\beta_{atl}\\ -\alpha'_t-\alpha'_{at}+2^{k+1}3^n\delta_{a^2tl} &= 2^{k+2}3^n\beta_{a^2tl}\end{aligned}$$

de donde deducimos que

$$\begin{aligned}2\alpha'_t-\alpha'_{at}+2^{k+1}3^n\delta_{tl} &\equiv\\ -\alpha'_t+2\alpha'_{at}+2^{k+1}3^n\delta_{atl} &\equiv\\ -\alpha'_t-\alpha'_{at}+2^{k+1}3^n\delta_{a^2tl} &\equiv 0 \bmod 2^{k+2}3^n\end{aligned}\qquad(3.1)$$

Luego $2^{k+1}3^n$ divide a $2\alpha'_t-\alpha'_{at}$ y $-\alpha'_t-\alpha'_{at}$ y por tanto también divide a los coeficientes de α'. Pongamos $\alpha=\frac{\alpha'}{2^{k+1}3^n}$. Escribiendo (3.1) en términos de los coeficientes de α tenemos

$$\begin{aligned}2\alpha_t-\alpha_{at}+3\delta_{tl} &\equiv\\ -\alpha_t+2\alpha_{at}+3\delta_{atl} &\equiv\\ -\alpha_t-\alpha_{at}+3\delta_{a^2tl} &\equiv 0 \bmod 6\end{aligned}$$

En particular para cada $t \in \{1, x\}$ y cada $l \in \langle xy, S, Z\rangle$ tenemos

$$\begin{array}{rcll} \delta_{tl} & \equiv & \alpha_{at} & \mod 2, \\ \delta_{atl} & \equiv & \alpha_t & \mod 2, \\ \delta_{a^2tl} & \equiv & \alpha_t + \alpha_{at} & \mod 2 \end{array} \tag{3.2}$$

Podemos por tanto cambiar nuestro objetivo por el de demostrar que los coeficientes de α son todos pares.

Vamos ahora a analizar las proyecciones de β en las componentes simples de la forma $\mathbb{Q}Gf_{S,\psi}$ con $\psi \in Z^*$. Fijemos un $\psi \in Z^*$ y pongamos $f = f_{S,\psi}$. Recordemos (Lema 3.2.8) que tenemos un isomorfismo $\lambda = \lambda_\psi : \mathbb{Q}Gf \to \mathbb{H}(\mathbb{Q}(\sqrt{3}))$. Este isomorfismo se puede caracterizar por las siguientes relaciones

$$\begin{array}{rcl} \lambda(sf) & = & 1, \text{ si } s \in S; \\ \lambda(af) & = & \omega = \frac{1}{2}\left(-1 + \sqrt{3}\mathbf{i}\right); \\ \lambda(xf) & = & \mathbf{j}; \\ \lambda(yf) & = & \mathbf{k}; \\ \lambda(zf) & = & \psi(z), \text{ si } z \in Z. \end{array} \tag{3.3}$$

Para cada $b \in \langle a\rangle$, $t \in \{1, x, y, xy\}$ y $z \in Z$ pongamos

$$\bar{\delta}_{btz} = \sum_{s\in S} \delta_{sbtz}.$$

Utilizando (3.3) obtenemos los coeficientes de $\lambda(\beta f)$ en la base

$$B = \{1, \sqrt{3}, \mathbf{i}, \sqrt{3}\mathbf{i}, \mathbf{j}, \sqrt{3}\mathbf{j}, \mathbf{k}, \sqrt{3}\mathbf{k}\} :$$

$$\begin{aligned} \lambda(\beta f) = \tfrac{1}{2}\textstyle\sum_{z\in Z}[\quad & (2\bar{\delta}_z - \bar{\delta}_{az} - \bar{\delta}_{a^2z} + \sqrt{3}(-\bar{\delta}_{axyz} + \bar{\delta}_{a^2xyz}))+ \\ & (2\bar{\delta}_{xyz} - \bar{\delta}_{axyz} - \bar{\delta}_{a^2xyz} + \sqrt{3}(\bar{\delta}_{az} - \bar{\delta}_{a^2z}))\mathbf{i}+ \\ & (2\bar{\delta}_{xz} - \bar{\delta}_{axz} - \bar{\delta}_{a^2xz} + \sqrt{3}(-\bar{\delta}_{ayz} + \bar{\delta}_{a^2yz}))\mathbf{j}+ \\ & (2\bar{\delta}_{yz} - \bar{\delta}_{ayz} - \bar{\delta}_{a^2yz} + \sqrt{3}(\bar{\delta}_{axz} - \bar{\delta}_{a^2xz}))\mathbf{k}] \end{aligned}$$

Como $v = 1 + \beta$ es una unidad de $\mathbb{Z}G$, entonces $\lambda(vf) = 1 + \lambda(\beta f)$ es una unidad de $\lambda(\mathbb{Z}G) = \mathbb{Z}[\omega, \mathbf{i}, \mathbf{j}]$. Por el Lema 3.2.2, v está en $\mathbb{Z}[\omega, \mathbf{i}]$ o en $\mathbb{Z}[\omega, \mathbf{i}]\mathbf{j}$. Vamos a ver que está en $\mathbb{Z}[\omega, \mathbf{i}]$. En efecto, como $\delta \in \Delta_{\mathbb{Z}}(G, U)$ los coeficientes de 1, $\mathbf{i}$, $\mathbf{j}$ y $\mathbf{k}$ en la expresión de $\lambda(\beta f)$ en la base B son de la forma

$$\sum_{z\in Z} \psi(z)(2\bar{\delta}_{tz} - \bar{\delta}_{atz} - \bar{\delta}_{a^2tz}) \equiv -\sum_{z\in Z} \psi(z) \sum_{u\in U} \delta_{utz} = 0 \mod 3, \tag{3.4}$$

pues $\delta \in \Delta_{\mathbb{Z}}(G, U)$. En particular el coeficiente de 1 en la expresión de $\lambda(vf)$ en la base B es no nulo y deducimos que $\lambda(\beta f) \in \mathbb{Z}[\omega, \mathbf{i}]$.

Concluimos que para cada $\psi \in Z^*$ se verifica

$$\begin{array}{ll} \sum_{z\in Z} \psi(z)(2\bar{\delta}_{xz} - \bar{\delta}_{axz} - \bar{\delta}_{a^2xz}) & = \\ \sum_{z\in Z} \psi(z)(-\bar{\delta}_{ayz} + \bar{\delta}_{a^2yz}) & = \\ \sum_{z\in Z} \psi(z)(2\bar{\delta}_{yz} - \bar{\delta}_{ayz} - \bar{\delta}_{a^2yz}) & = \\ \sum_{z\in Z} \psi(z)(\bar{\delta}_{axz} - \bar{\delta}_{a^2xz}) & = \ 0 \end{array}$$

Teniendo en cuenta que $(\psi(z))_{z\in Z,\psi\in Z^*}$ es una matriz de Hadamard, en particular invertible, deducimos que

$$\begin{array}{rl} 2\bar{\delta}_{xz} - \bar{\delta}_{axz} - \bar{\delta}_{a^2xz} & = \\ -\bar{\delta}_{ayz} + \bar{\delta}_{a^2yz} & = \\ 2\bar{\delta}_{yz} - \bar{\delta}_{ayz} - \bar{\delta}_{a^2yz} & = \\ \bar{\delta}_{axz} - \bar{\delta}_{a^2xz} & = \ 0 \end{array}$$

para todo $z \in Z$. De donde obtenemos las dos siguientes:

$$\begin{array}{rl} \bar{\delta}_{x} - \bar{\delta}_{a^2x} & = \\ \bar{\delta}_{ay} - \bar{\delta}_{a^2y} & = \ 0 \end{array}$$

De (3.2) tenemos que

$$\alpha_x \equiv 3^{n-1}\alpha_x \equiv \sum_{s\in S}(\delta_{sx} - \delta_{sa^2x}) = \bar{\delta}_x - \bar{\delta}_{a^2x} = 0 \bmod 2$$

y

$$\alpha_{ax} \equiv 3^{n-1}\alpha_{ax} \equiv \sum_{s\in S}(\delta_{ay} - \delta_{a^2y}) = \bar{\delta}_{ay} - \bar{\delta}_{a^2y} = 0 \bmod 2.$$

Con esto hemos alcanzado la mitad de nuestro objetivo. Todavía nos queda demostrar que α_1 y α_a son pares.

Como hemos visto en el cálculo de (3.4) los coeficientes de 1 e $\mathbf{i}$ en la expresión de $2\lambda(\beta f)$ en la base B son múltiplos de 3. Además de (3.2) se deduce que estos dos coeficientes son congruentes módulo 2. En resumen, si ponemos $\lambda(vf) = \frac{1}{2}(x_1 + y_1\sqrt{3} + (x_2 + y_2\sqrt{3})\mathbf{i})$, entonces $x_1 \equiv x_2 \bmod 2$ y $1+x_1$ y x_2 son múltiplos de 3. Como además $x_1 \equiv y_2 \bmod 2$, tenemos que todos los x_i e y_i son pares o todos impares.

Supongamos que todos los x_i e y_i son impares. Como $\lambda(vf)$ es una unidad en un orden de $\mathbb{Q}(\sqrt{3},\mathbf{i})$, su norma en la extensión $\mathbb{Q}(\sqrt{3},\mathbf{i})/\mathbb{Q}$ ha de ser ± 1. Esta norma es

$$\frac{1}{16}\left((x_1^2 - 3y_1^2)^2 + (x_2^2 - 3y_2^2)^2 + 2(x_1x_2 - 3y_1y_2)^2 + 6(x_1y_2 - x_2y_1)^2\right)$$

y por tanto

$$(x_1^2 - 3y_1^2)^2 + (x_2^2 - 3y_2^2)^2 + 2(x_1x_2 - 3y_1y_2)^2 + 6(x_1y_2 - x_2y_1)^2 = 16.$$

Como todos los x_i e y_i son impares

$$|x_1^2 - 3y_1^2| = |x_2^2 - 3y_2^2| = 2,$$

luego

$$(x_1x_2 - 3y_1y_2)^2 + 3(x_1y_2 - x_2y_1)^2 = \frac{16-8}{2} = 4.$$

en contra de que x_2 es múltiplo de 3.

Concluimos que $\lambda(vf)$ es una unidad de $\mathbb{Z}[\sqrt{3}, \mathbf{i}]$ y por tanto o bien pertenece a $\mathbb{Z}[\sqrt{3}]$ ó a $\mathbb{Z}[\sqrt{3}]\mathbf{i}$. Pero ya hemos visto que lo segundo no se puede dar pues $1 + x_1$ es múltiplo de 3. Utilizando la expresión de $\lambda(\beta f)$ que hemos obtenido deducimos que

$$\begin{aligned} \textstyle\sum_{z\in Z} \psi(z)(2\bar{\delta}_z - \bar{\delta}_{az} - \bar{\delta}_{a^2z}) &= \\ \textstyle\sum_{z\in Z} \psi(z)(-\bar{\delta}_{axyz} + \bar{\delta}_{a^2xyz}) &= 0 \end{aligned}$$

y volviendo a utilizar que $(\psi(z))_{z\in Z, \psi\in Z^*}$ es una matriz invertible deducimos que

$$\begin{aligned} 2\bar{\delta}_{xyz} - \bar{\delta}_{axyz} - \bar{\delta}_{a^2xyz} &= \\ \bar{\delta}_{az} - \bar{\delta}_{a^2z} &= 0 \end{aligned}$$

y por tanto

$$\begin{aligned} \bar{\delta}_z - \bar{\delta}_{a^2z} &= \\ \bar{\delta}_{axyz} - \bar{\delta}_{a^2xyz} &= 0, \end{aligned}$$

para todo $z \in Z$. Ahora acabamos la demostración utilizando (3.2) una vez más:

$$\alpha_1 \equiv 3^{n-1}\alpha_1 \equiv \sum_{s\in S}(\delta_s - \delta_{sa^2}) = \bar{\delta}_1 - \bar{\delta}_{a^2} = 0 \bmod 2$$

y

$$\alpha_a \equiv 3^{n-1}\alpha_a \equiv \sum_{s\in S}(\delta_{saxy} - \delta_{sa^2xy}) \equiv \bar{\delta}_{axy} - \bar{\delta}_{a^2xy} \equiv 0 \bmod 2.$$

□

Suponemos que el siguiente lema es bien conocido, pero como no conocemos ninguna referencia lo demostramos de todas formas.

Lema 3.3.6 *Si x e y son dos elementos que no conmutan de $M_2(\mathbb{C})$, entonces el centralizador de $\{x, y\}$ en $M_2(\mathbb{C})$ está contenido en el centro de $M_2(\mathbb{C})$.*

Demostración. Sea a un elemento de $M_2(\mathbb{C})$ tal que $ax = xa$ y $ay = ya$. Si x es diagonalizable, existe un $u \in \mathrm{GL}_2(\mathbb{C})$ tal que $uxu^{-1} = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ con $\lambda, \mu \in \mathbb{C}$. Como $xy \neq yx$ necesariamente $\lambda \neq \mu$ y uyu^{-1} no es diagonal. por otro lado $ax = xa$

y por tanto uau^{-1} es diagonal, pongamos $uau^{-1} = \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}$ con $p, q \in \mathbb{C}$. Ahora de que $ay = ya$ e $y$no es diagonal se deduce que $p = q$ y por tanto a es central.

Si x no es diagonalizable entonces existe una matriz invertible $u \in M_2(\mathbb{C})$ tal que $uxu^{-1} = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Como $ax = xa$ entonces uau^{-1} conmuta con $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ y por lo tanto $uau^{-1} = \begin{pmatrix} l & t \\ 0 & l \end{pmatrix}$ para ciertos $l, t \in \mathbb{C}$. Si $t \neq 0$ tenemos que $uyu^{-1} = \begin{pmatrix} d & c \\ 0 & d \end{pmatrix}$ para ciertos $d, c \in \mathbb{C}$ pues $ay = ya$, contradiciendo el hecho de que $xy \neq yx$. Por lo tanto $t = 0$, de donde deducimos que a es central. □

Antes de demostrar el Teorema 3.1.12 necesitamos un lema más.

Lema 3.3.7 *Si E es un subgrupo libre no abeliano de $\mathcal{U}(\mathbb{Z}G)$ entonces existe un $e \in C$ tal que Ee es un subgrupo no abeliano. Además, para todo $e \in C$ tal que Ee no es abeliano se verifica*

$$Cen_{\mathcal{U}(\mathbb{Z}G)}(E)e \subseteq \{\pm e\}$$

donde $Cen_{\mathcal{U}(\mathbb{Z}G)}(E) = \{u \in \mathcal{U}(\mathbb{Z}G) | uh = hu \text{ para todo } h \in E\}$ es el centralizador de E en $\mathcal{U}(\mathbb{Z}G)$.

Demostración. Por ser E un grupo libre no abeliano existen $x, y \in E$ tales que $[x^n, y^n] \neq 1$ para todo $n \geq 1$. Sea $e \in I \setminus C$. Entonces para todo orden $\mathcal{O}$ de $\mathbb{Q}Ge$ el grupo de las unidades del centro de $\mathcal{O}$ tiene índice finito en el grupo de las unidades de $\mathcal{O}$ (Lema 1.2.5). Por tanto existe $n \geq 1$ tal que $[(xe)^n, (ye)^n] = 1$. Por lo tanto existe un $e \in C$ tal que Ee contiene un subgrupo no abeliano. Identificando $\mathbb{Q}Ge$ con $M_2(\mathbb{Q})$ se tiene que si $a \in Cen_{\mathcal{U}(\mathbb{Z}G)}(E)$ entonces por el Lema 3.3.6 ae es un elemento central de un orden de $M_2(\mathbb{Q})$ y por tanto $ae = \pm e$. □

Ya podemos finalmente demostrar el Teorema 3.1.12. Recordemos su enunciado.

Teorema 3.3.8 *Sea $G = H \times Z$ donde Z es un 2-grupo abeliano elemental y H de uno de los tipos $(a) - (i)$ del Teorema 3.1.11. Sean B y C los conjuntos de idempotentes centrales primitivos de $\mathbb{Q}G$ de tipo (B) y (C) respectivamente. Sean $f_B = \sum_{f \in B} f$ y $F_0 = \mathcal{U}(\mathbb{Z}G) \cap (1 + \mathbb{Q}G f_B)$ y para cada $e \in C$ sea $F_e = \mathcal{U}(\mathbb{Z}G) \cap (1 + \mathbb{Q}Ge)$. Sea $F = F_0 \times \prod_{e \in C} F_e$. Si $E = E_0 \times \prod_{j \in J} E_j$ es un subgrupo de índice finito en $\mathcal{U}(\mathbb{Z}G)$, donde E_0 es libre abeliano y E_j es libre no abeliano para todo j; entonces*

1. *$r(E_0) = |B|$ y $|C| = |J|$;*

además, si G no es isomorfo a D_3, D_4, Q_{12} ni a Q_{16} entonces

- $[\mathcal{U}(\mathbb{Z}G) : F] \leq [\mathcal{U}(\mathbb{Z}G) : E]$ *y*
- $r(E_j) \geq r(F_e)$ *para todo* $e \in C$ *y* $j \in J$.

Demostración. Sea $E = E_0 \times \prod_{j \in J} E_j$ un subgrupo de índice finito en $\mathcal{U}(\mathbb{Z}G)$ tal que E_0 es libre abeliano y E_j es libre no abeliano para todo j.

1. Por el Lema 3.3.7, existe una aplicación $\sigma : J \to C$ tal que para todo $j \in J$ existe un $\sigma(j) \in C$ tal que $E_j\sigma(j)$ no es abeliano y $E_0\sigma(j), E_{j_1}\sigma(j) \subseteq \{\pm\sigma(j)\}$, para todo $j_1 \neq j$. Esto implica que σ es inyectiva y que $E_j \cap F_{\sigma(j)}$ contiene un subgrupo de índice finito de $F_{\sigma(j)}$. Sea ahora $e \in C$. Entonces $F_e \cap E$ es un subgrupo de índice finito de F_e y por lo tanto $F_e \cap E$ es libre no abeliano. Así $F_e \cap E_j$ no es abeliano para algún $j \in J$ y entonces $F_e \cap E_{j'} = 1$ para todo $j' \neq j$. Esto implica que el cardinal de C y J coinciden y por tanto σ es una biyección. A partir de ahora identificaremos J y C y consideraremos σ como una igualdad, tal que para cada dos elementos diferentes e y f de C, $E_e e$ no es abeliano y $E_e f = \pm f$.

Entonces $E_0 \cap \widetilde{F}_0$ y F_0 son subgrupos abelianos de índice finito en $\widetilde{F}_0$ y por lo tanto tienen el mismo rango. Como el primero también tiene índice finito en E_0, entonces $r(E_0) = r(F_0) = |B|$.

Supongamos ahora que G no es isomorfo a D_3, D_4, Q_{12} ni Q_{16}.

2. Sea $a \in E_e$. Por el Teorema 3.3.1, $a = vg$ para algún $v \in V$ y una unidad trivial $g \in \pm G$. Para todo $f \in C \setminus \{e\}$, $\pm f = af = vf \cdot gf$ y por lo tanto vf es un elemento de torsión de Vf. Por el Lema 3.3.2, $vf = f$. Combinando este argumento con el Lema 3.3.5 obtenemos

$$E_e \subseteq (\widetilde{F}_e \cap V) \rtimes \pm G \subseteq (F_0 \times F_e) \rtimes \pm G \tag{3.5}$$

y el mismo argumento demuestra que

$$E_0 \subseteq (\widetilde{F}_0 \cap V) \rtimes \pm G \subseteq F_0 \rtimes \pm G. \tag{3.6}$$

En realidad como F_0 y los F_e satisfacen las condiciones exigidas a E_0 y los E_e las dos inclusiones de la derecha en (3.5) y (3.6) son igualdades.

Por lo tanto $E \subseteq F \rtimes (\pm G)$. Como E es libre de torsión $[F \rtimes (\pm G) : E] \geq 2|G|$ y así

$$\begin{aligned}
[\mathcal{U}(\mathbb{Z}G) : E] &= [\mathcal{U}(\mathbb{Z}G) : F \rtimes (\pm G)][F \rtimes (\pm G) : E] \\
&\geq [\mathcal{U}(\mathbb{Z}G) : F \rtimes (\pm G)]\ 2\ |G| \\
&= [\mathcal{U}(\mathbb{Z}G) : F \rtimes (\pm G)][F \rtimes (\pm G) : F] \\
&= [\mathcal{U}(\mathbb{Z}G) : F].
\end{aligned}$$

3. Como todos los F_e tienen el mismo rango (Teorema 3.1.11) basta con demostrar que $r(E_e) \geq r(F_e)$ para un $e \in C$ fijado. Por las Proposiciones 3.2.5 y 3.2.7, F_0 es

central. Utilizando esto y que F_e es libre no abeliano tenemos que $E_e \subseteq (F_0 \times F_e) \rtimes \pm G = F_0 \times (F_e \rtimes \pm G)$. Consideramos la proyección p de E_e en $F_e \rtimes \pm G$. Utilizando que F_0 es central se tiene que p es inyectiva y por tanto $p(E_e)$ es un subgrupo libre de $F_e \rtimes (\pm G)$. Teniendo en cuenta que E es un subgrupo de índice finito en $\mathcal{U}(\mathbb{Z}G)$ y que $E_0 e = E_f e = e$ para todo $f \in C \setminus \{e\}$ tenemos que $p(E_e)$ tiene índice finito en $F_e \rtimes (\pm G)$ y por tanto $F_e \cap p(E_e)$ tiene índice finito en $p(E_e)$ y en F_e. Como

$$\begin{aligned}[F_e \rtimes \pm G : F_e \cap p(E_e)] &= [F_e \rtimes \pm G : F_e][F_e : F_e \cap p(E_e)] \\ &= [F_e \rtimes \pm G : p(E_e)][p(E_e) : F_e \cap p(E_e)].\end{aligned}$$

y

$$[F_e \rtimes \pm G : F_e] = 2|G| \leq [\pm F_e \rtimes G : p(E_e)],$$

por ser $p(E_e)$ libre de torsión, tenemos que

$$[F_e : F_e \cap p(E_e)] \geq [p(E_e) : F_e \cap p(E_e)].$$

Finalmente si $r = r(F_e \cap p(E_e))$ entonces por el Teorema 3.2.1

$$r(F_e) = 1 + \frac{r-1}{[F_e : F_e \cap p(E_e)]} \leq 1 + \frac{r-1}{[p(E_e) : F_e \cap p(E_e)]} = r(p(E_e)) = r(E_e).$$

□

En la sección anterior hemos explicado por que es necesario excluir los grupos D_3 y D_4 de nuestros teoremas, en concreto para estos grupos F_e no es libre pero basta con bajar un poco para obtener un subgrupo libre. Para los grupos Q_{12} y Q_{16} F_e si es libre parta el único elemento e de C. Estos grupos coinciden con los casos en que H es de tipo (h) y (g) respectivamente y $n = 1$ y $k = 0$. Curiosamente el complemento normal V de los Teoremas 3.1.6 y 3.1.8 y nuestro grupo F tienen el mismo rango, en concreto V y F son libres de rango 5 para Q_{12} y son el producto directo de un libre de rango 1 y otro de rango 9 para Q_{16}. Obviamente el grupo V es óptimo por ser un complemento normal en $\mathcal{U}(\mathbb{Z}G)$ del subgrupo formado por las unidades triviales. Aunque nuestros métodos no muestran que el grupo F sea óptimo el hecho de que los rangos coincidan con el de subgrupos óptimos hace sospechar que en realidad también ellos son óptimos y efectivamente, esto es así ya que en ambos casos $V \subseteq F$, y como F es libre de torsión y V tiene un complemento de torsión en $\mathcal{U}(\mathbb{Z}G)$ entonces $V = F$.

Para $Q_{12} = \langle a, b | a^6 = a^3b^2 = bab^{-1}a = 1\rangle$ esto se ve de forma sencilla ya que el complemento normal V de las unidades triviales dado en [48] está formado por las unidades de $\mathbb{Z}G$ de la forma $1 + \alpha(1 - a^2)$ con $\alpha \in \Delta_{\mathbb{Z}}(G)$, que obviamente está contenido en $F = F_e$, donde $e = 1 - \widehat{a^2}$ es el único idempotente central primitivo de $\mathbb{Q}Q_{12}$ de tipo C.

Para $Q_{16} = \langle a, b | a^8 = a^4b^2 = bab^{-1}a = 1\rangle$ hay que trabajar un poco más para obtener la inclusión $V \subseteq F$. El álgebra $\mathbb{Q}Q_{16}$ tiene un idempotente central

primitivo de tipo B, $1-\widehat{a^4}$ y un idempotente central primitivo de tipo C, $\widehat{a^4}-\widehat{a^2}$. El complemento normal V se obtiene de la misma forma, a saber el formado por las unidades de la forma $1+\alpha(1-a^2)$ con $\alpha \in \Delta_{\mathbb{Z}}(G)$. En este caso no es evidente que V esté contenido en $F = F_0 \times F_e$ ya que esté último está formado por las elementos de $\mathbb{Z}G$ de la forma $(1+\alpha(\widehat{a^2}-\widehat{a^4}))(1+\beta\widehat{a^4})$. Sin embargo una detallada lectura de la demostración del Teorema 4 de [34] (que coincide con el Teorema 3.1.8), muestra que $V = V_1 \times V_2$, donde V_1 es cíclico infinito generado por un elemento de la forma $1+\alpha(1-a^4)$ y V_2 es libre de rango 9 generado por elementos de la forma $1+\alpha(1-a^2)(1+a^4)$. Esto muestra que $V_1 \subseteq F_0$ y $V_2 \subseteq F_e$ y por tanto $V \subseteq F$, como queríamos.

Capítulo 4

Grupos finitos de tipo kleiniano

4.1. Introducción

En el Capítulo 3 hemos visto que podemos describir de forma muy satisfactoria un subgrupo de índice finito de $\mathcal{U}(\mathbb{Z}G)$ para algunos grupos finitos G. Lo que tienen de bueno cada uno estos grupos G es que las componentes de la descomposición de Wedderburn de $\mathbb{Q}G$ son "manejables". En concreto las componentes simples son todas cuerpos, algebras de cuaterniones totalmente definidas o isomorfas a $M_2(\mathbb{Q})$. Si elegimos un orden O_i en cada una de las componentes simples S_i $(i = 1, 2, \ldots, n)$ de $\mathbb{Q}G$, entonces el grupo de unidades de $\mathbb{Z}G$ tiene un subgrupo de índice finito que es isomorfo a un producto directo $\prod_{i=1}^{k} H_i$ donde cada H_i es un subgrupo de índice finito del grupo de unidades de O_i. El Teorema de las Unidades de Dirichlet nos proporciona la estructura de H_i si S_i es un cuerpo y, junto con el Lema 1.2.5, también nos proporciona la estructura de H_i si S_i es un álgebra de cuaterniones totalmente definida. Finalmente podemos estudiar la estructura de H_i en el caso en que S_i sea isomorfo a $M_2(\mathbb{Q})$ utilizando diversos métodos. Por ejemplo es bien sabido que $\mathrm{PSL}_2(\mathbb{Z})$ es un producto libre de un grupo cíclico de orden 2 y uno de orden 3 de donde se deduce utilizando el Teorema de Kurosh (Teorema 6.3.1 [60]) que $\mathrm{PSL}_2(\mathbb{Z})$ tiene un subgrupo libre no abeliano de índice finito.

Tanto las demostraciones habituales del Teorema de las Unidades de Dirichlet como las de que $\mathrm{PSL}_2(\mathbb{Z})$ es un producto libre de un grupo cíclico de orden 2 y uno de orden 3 son de tipo geométrico. En ambas se considera el grupo a estudiar actuando en un objeto geométrico. En el caso del Teorema de las Unidades de Dirichlet se incluye el grupo en un espacio euclídeo mediante la aplicación logarítmica y en el caso de $\mathrm{PSL}_2(\mathbb{Z})$ se lo considera actuando en el modelo de Poincaré del espacio hiperbólico

bidimensional $\mathbb{H}^2$ mediante transformaciones de Möbius. Esta forma de estudiar un grupo a partir de su acción en un objeto topológico-geométrico ha sido ampliamente generalizada por múltiples autores como Eichler, Poincaré, Borel, Harish-Chandra, Siegel y otros. Sin embargo, salvo que el objeto geométrico sea muy sencillo, por ejemplo euclídeo como en el Teorema de las Unidades de Dirichlet, o tenga una dimensión pequeña y la acción sea muy controlable, como ocurre con el caso de la acción de $\mathrm{PSL}_2(\mathbb{Z})$ en el plano hiperbólico, es muy difícil explotar esta acción para obtener información precisa sobre el grupo que se está estudiando.

La acción de $\mathrm{PSL}_2(\mathbb{Z})$ en $\mathbb{H}^2$ es, en realidad, la restricción de la acción de $\mathrm{PSL}_2(\mathbb{C})$ por transformaciones de Möbius en la compactificación por un punto $\hat{\mathbb{C}}$ del cuerpo de los números complejos. Esta acción se puede extender a una acción en el espacio hiperbólico tridimensional $\mathbb{H}^3$. De hecho $\mathrm{PSL}_2(\mathbb{C})$ es isomorfo al grupo de isometrías de $\mathbb{H}^3$ que conservan la orientación. Los subgrupos de $\mathrm{PSL}_2(\mathbb{C})$ que actúan discontinuamente en $\mathbb{H}^3$, son exactamente los subgrupos discretos de $\mathrm{PSL}_2(\mathbb{C})$, es decir las proyecciones en $\mathrm{PSL}_2(\mathbb{C})$ de los subgrupos de $\mathrm{SL}_2(\mathbb{C})$ que tienen topología euclídea discreta. Estos grupos reciben el nombre de grupos kleinianos.

El estudio de los grupos kleinianos empieza con un trabajo de Poincaré [52] que proporciona un método para obtener presentaciones de grupos kleinianos a partir de un dominio fundamental. De hecho Poincaré caracteriza cómo son los dominios fundamentales de grupos kleinianos. Bianchi [7] obtuvo un método para obtener dominios fundamentales de los grupos de la forma $\mathrm{PSL}_2(R)$ donde R es el anillo de enteros de una extensión cuadrática imaginaria. Estos grupos son hoy conocidos como grupos de Bianchi. Desde entonces numerosos trabajos se han dedicado al estudio de los grupos kleinianos o al caso particular de los grupos de Bianchi. Algunas referencias básicas son [6], [15], [14].

En este capítulo comenzamos un proyecto de estudio de los grupos finitos G para los que podamos añadir la acción de ciertos grupos discontinuos en el espacio hiperbólico tridimensional para estudiar el grupo de unidades de $\mathbb{Z}G$. Vamos a explicar esto de forma más precisa.

Sea R un orden clásico en un álgebra racional semisimple de dimensión finita A. Sea $A = \prod_{i=1} A_i$ la descomposición de Wedderburn de A y para cada $i = 1, 2, \ldots, n$ sea S_i un orden en A_i. Como consecuencia de la Proposición 1.2.1, el grupo de unidades de cada S_i contiene un subgrupo de índice finito H_i contenido en R de forma que $\prod_{i=1}^{n} H_i$ es un subgrupo de índice finito en el grupo de unidades de R. Por tanto para estudiar la estructura virtual del grupo de unidades de R podemos suponer que A es simple. Sean K el centro de A, S un orden en K y R_1 el grupo de elementos de R de norma reducida 1. Entonces $\mathcal{U}(S) \cap R_1$ es finito y por tanto $\mathcal{U}(R)$ y $\mathcal{U}(S) \times R_1$ comparten un subgrupo de índice finito. Como el Teorema de las Unidades de Dirichlet nos proporciona la estructura de $\mathcal{U}(S)$ la dificultad se encuentra en el estudio de los grupos R_1 para R un orden en un álgebra racional simple de dimensión finita.

Si A es un álgebra de cuaterniones sobre un subcuerpo del cuerpo de los números complejos, entonces A se incluye en $M_2(\mathbb{C})$ de forma natural y además si R es un orden en A entonces R_1 está incluido en $\mathrm{SL}_2(\mathbb{C})$ de forma que R_1 actúa en $\mathbb{H}^3$. Si la imagen de R_1 en $\mathrm{PSL}_2(\mathbb{C})$ es un subgrupo discreto podremos aplicar el método de Poincaré para estudiar R_1. Esto es lo que hizo Bianchi para los grupos que llevan su nombre. Obsérvese que en tal caso lo mismo se verificará para cualquier otro orden en A.

En resumen, tenemos un método teórico para estudiar el grupo de unidades de un orden en un álgebra racional A si las componentes simples de A son todas cuerpos, algebras de cuaterniones totalmente definidas ó álgebras de cuaterniones que tienen un orden R de forma que la imagen de R_1 en $\mathrm{PSL}_2(\mathbb{C})$ es un subgrupo discreto. En realidad las dos primeras son del tercer tipo pues si R es un orden o un álgebra de cuaterniones totalmente definida entonces R_1 es finito y podemos considerar en ambos casos R_1 como un subgrupo discreto de $\mathrm{SL}_2(\mathbb{C})$.

Nuestro objetivo es estudiar los grupos de unidades de $\mathbb{Z}G$ para los grupos finitos G, para los que todas las componentes simples de $\mathbb{Q}G$ contengan un orden R tal que R_1 es un subgrupo discreto de $\mathrm{SL}_2(\mathbb{C})$. Diremos entonces que G es un grupo de tipo kleiniano. En principio el proyecto completo tendría dos partes: La primera clasificar dichos grupos y la segunda aplicar el Método de Poincaré con el fin de obtener un subgrupo de índice finito de $\mathbb{Z}G$ del que podamos dar una estructura precisa. En esta memoria sólo nos vamos a ocupar de la primera parte del proyecto y de hecho sólo vamos a considerar grupos nilpotentes.

Hemos conseguido caracterizar los grupos finitos nilpotentes de tipo kleiniano en términos de la descomposición de Wedderburn del álgebra racional correspondiente (Teorema 4.4.2). El siguiente paso sería obtener la lista de los grupos finitos nilpotentes de tipo kleinianos. Por supuesto que la dificultad está en dar los no abelianos. De momento, sólo hemos conseguido determinar algunos de ellos. Concretamente hemos demostrado que si G es un grupo nilpotente finito no abeliano tal que su subgrupo derivado es central, entonces G es de tipo kleiniano si y sólo si, o bien G es isomorfo a $H \times C_2^k \times C_3^k$ con $k > 1$ y H de uno de los tipos (a)-(f) del Teorema 3.1.9 o bien G es un cociente de $H \times C_4^k$ donde H es uno de los siguientes grupos:

$$
\begin{aligned}
B_2 = \quad & \langle x_1, x_2 | x_i^8 = [x_i, x_j^4] = [x_i, [x_j, x_k]] = 1, i, j, k = 1, 2 \rangle \\
A_{31} = \quad & \langle x_1, x_2, x_3 | x_i^4 = [x_i, x_j^2] = [x_i, [x_j, x_k]] = 1, 1 \leq i, j, k \leq 3 \rangle \\
A_{32} = \quad & \langle x_1, x_2, x_3 | x_1^4 = x_2^4 [x_1, x_2] = x_3^4 [x_1, x_3] = [x_i, x_j^2] = 1, 1 \leq i, j, k \leq 3 \rangle \\
B_{31} = \quad & \langle x_1, x_2, x_3 | x_1^8 = x_k^4 = [x_i, x_j^2] = [x_k, x_l] = [x_i, [x_1, x_k]] = 1, 1 \leq i, j \leq 3, \\
& 2 \leq k, l \leq 3 \rangle \\
B_{32} = \quad & \langle x_1, x_2, x_3 | x_1^8 = x_k^4 [x_1, x_k] = [x_i, x_j^2] = [x_k, x_l] = [x_i, [x_1, x_k]] = 1, \\
& 1 \leq i, j \leq 3, 2 \leq k, l \leq 3 \rangle
\end{aligned}
$$

Por otro lado si G es un grupo finito nilpotente de tipo kleiniano cuyo subgrupo derivado no es central, entonces G es un 2-grupo.

Los grupos nilpotentes de tipo kleiniano que quedan por determinar son todos 2-grupos y tenemos alguna información sobre ellos pero todavía no hemos podido clasificarlos todos.

4.2. Grupos discretos

Sea G un grupo de homeomorfismos de un espacio métrico X. se dice que G es un grupo discontinuo si la intersección de cada compacto de X con cada órbita de la acción de G en X es finita. Un dominio fundamental F de X por G es un subconjunto conexo de X que satisface las siguientes condiciones:

1. La clausura de F contiene al menos un representante de cada órbita.

2. El interior de F contiene a lo sumo un representante de cada órbita.

3. La frontera de F tiene medida nula.

A partir de un dominio fundamental de un grupo discontinuo G se puede obtener una presentación de G, pero no vamos a entrar en eso.

El semiespacio positivo de un espacio Euclídeo tridimensional nos proporciona un modelo de espacio hiperbólico tridimensional $\mathbb{H}^3$. Más concretamente definimos

$$\begin{aligned} \mathbb{H}^3 &:= \mathbb{C} \times (0, \infty) \\ &= \{(z, r) | z \in \mathbb{C}, r \in \mathbb{R}, r > 0\} \\ &= \{(x, y, r) | x, y, r \in \mathbb{R}, r > 0\} \end{aligned}$$

Para facilitar los cálculos a menudo pensaremos en $\mathbb{H}^3$ como un subconjunto de los cuaterniones de Hamilton $\mathbb{H}(\mathbb{R})$. La notación para puntos en $\mathbb{H}^3$ es

$$P = (z, r) = (x, y, r) = z + rj$$

donde $z = x + yi$ y $j = (0, 0, 1)$.

$\mathbb{H}^3$ tiene estructura de variedad Riemaniana. La distancia en $\mathbb{H}^3$, llamada distancia hiperbólica, viene dada por la fórmula

$$\cosh d(P, P') = \frac{|z - z'|^2 + r^2 + r'^2}{2rr'}$$

donde $P = z + rj$ y $P' = z' + r'j$.

Dada la una matriz $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$ y un elemento $P = z + rj \in \mathbb{H}^3$ definimos $gP = (aP + b)(cP + d)^{-1}$. Un cálculo tedioso muestra que $gP \in \mathbb{H}^3$. Más concretamente $gP = z^* + r^* j$ donde

$$z^* = \frac{(az + b)(\overline{cz} + \overline{d}) + a\overline{c}r^2}{|cz + d|^2 + |c|^2 r^2}$$

$$r^* = \frac{r}{|cz + d|^2 + |c|^2 r^2}.$$

Esto define un acción de $\mathrm{GL}_2(\mathbb{C})$ en $\mathbb{H}^3$. Además la acción de g en $\mathbb{H}^3$ es una isometría que conserva la orientación [14]. Es decir tenemos un homomorfismo de grupos

$$\mathrm{GL}_2(\mathbb{C}) \to \mathbf{Iso}^+(\mathbb{H}^3)$$

donde $\mathbf{Iso}^+(\mathbb{H}^3)$ denota el grupo de isometrías de $\mathbb{H}^3$ que conserva la orientación. Este homomorfismo de grupos es suprayectivo y su núcleo está formado por $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ que identificamos con las matrices escalares no nulas. Por tanto podemos identificar $\mathbf{Iso}^+(\mathbb{H}^3)$ con $\mathrm{GL}_2(\mathbb{C})/\mathbb{C}^* = \mathrm{PGL}_2(\mathbb{C})$ que a su vez se identifica con $\mathrm{PSL}_2(\mathbb{C}) = \mathrm{SL}_2(\mathbb{C})/\{\pm I\}$. A partir de ahora identificamos $\mathrm{PSL}_2(\mathbb{C})$ con el grupo de isometrías de $\mathbb{H}^3$ que conservan la orientación, y cuando hablemos de que un subgrupo de $\mathrm{PSL}_2(\mathbb{C})$ es discontinuo nos estaremos refiriendo a que lo consideramos como un grupo de homeomorfismos de $\mathbb{H}^3$.

Consideramos $\mathrm{SL}_2(\mathbb{C})$ como un subconjunto de un espacio euclídeo de dimensión 8 identificando $M_2(\mathbb{C})$ con $\mathbb{C}^4 = \mathbb{R}^8$ de forma natural. Un subgrupo discreto de $\mathrm{SL}_2(\mathbb{C})$ es uno en el que la topología inducida por $M_2(\mathbb{C}) = \mathbb{R}^8$ es discreta y un subgrupo discreto de $\mathrm{PSL}_2(\mathbb{C})$ es la imagen de un subgrupo discreto de $\mathrm{SL}_2(\mathbb{C})$.

Recordamos una serie de hechos básicos sobre grupos discontinuos y discretos.

Teorema 4.2.1 (Teorema 1.2 [14]) *Un subgrupo* Γ *de* $\mathrm{PSL}(2, \mathbb{C})$ *es un grupo discontinuo si y sólo si* Γ *es discreto en* $\mathrm{PSL}(2, \mathbb{C})$

Teorema 4.2.2 (Teorema 2.2.6 [15]) *Sea* H *un subgrupo de índice finito de un grupo* G*. Si* H *es discontinuo entonces* G *es discontinuo.*

Definición 4.2.3 *Un grupo Fuschiano es un conjugado de un grupo discreto en* $\mathrm{PSL}(2, \mathbb{R})$.

Teorema 4.2.4 (Teorema 2.2.7 de [15]) *Un subgrupo abeliano de un grupo Fuschiano es cíclico.*

El siguiente teorema es consecuencia inmediata de el Teorema 4.3.5 de [6] y del Teorema 1.8 del Capítulo 2 de [14].

Teorema 4.2.5 *Si Γ un subgrupo libre de torsión, abeliano y discreto de* $\mathrm{PSL}(2,\mathbb{C})$*, entonces* $r(\Gamma) \leq 2$.

Recuérdese que $r(G)$ denota el rango de G, es decir, el menor de los cardinales de sus conjuntos de generadores.

Si $A = \left(\frac{a,b}{K}\right)$ es un algebra de cuaterniones sobre un subcuerpo K de $\mathbb{C}$ la aplicación $\phi : A \to M_2(\mathbb{C})$ que asocia el elemento $x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}$ con

$$\begin{pmatrix} x_o + x_1\sqrt{a} & x_2\sqrt{b} + x_3\sqrt{ab} \\ x_2\sqrt{b} - x_3\sqrt{ab} & x_o - x_1\sqrt{a} \end{pmatrix}$$

es un K-homomorfismo inyectivo de álgebras, luego el grupo de las unidades de A actúa en $\mathbb{H}^3$ a través del homomorfismo ϕ. Además $det(\phi(x)) = N(x)$ donde N denota la norma reducida de A. Por tanto ϕ asocia los elementos de norma reducida 1 con elementos de $\mathrm{SL}_2(\mathbb{C})$. Si R es un subanillo de A denotaremos por R_1 el grupo de los elementos de R de norma reducida 1. Consideraremos R_1 como un subgrupo de $\mathrm{SL}_2(\mathbb{C})$ a través de ϕ.

Si K es un cuerpo y R es un orden en K entonces $R_1 = 1$ y también consideramos R_1 como un subgrupo de $\mathrm{SL}_2(\mathbb{C})$ (obviamente discreto).

Nosotros estamos interesados en los cuerpos y álgebras de cuaterniones que contengan un orden R tal que R_1 es un subgrupo discreto de $\mathrm{SL}_2(\mathbb{C})$. Obviamente los cuerpos y las álgebras de cuaterniones totalmente definidas satisfacen esta condición. Otra familia de álgebras de cuaterniones que satisfacen eta condición son las de la forma $M_2(\mathbb{Q}(\sqrt{n}))$ con $n \leq 0$, esto incluye a $M_2(\mathbb{Q})$. Existen otras álgebras que satisfacen esta condición (véase el Capítulo 10 de [14]) pero no aparecen en nuestra discusión.

4.3. Grupos de tipo kleiniano

Definición 4.3.1 *Sea G un grupo finito. Diremos que G es de tipo kleiniano si todo cociente simple de $\mathbb{Q}G$ es un cuerpo o un álgebra de cuaterniones que contiene un orden R tal que R_1 es un subgrupo discreto de* $\mathrm{SL}_2(\mathbb{C})$.

Obsérvese que todos los grupos que aparecieron en el Capítulo 3 son todos de tipo kleiniano. Si R es un orden en un álgebra de cuaterniones A sobre un subcuerpo K de $\mathbb{C}$ y R_1 es discreto, entonces lo mismo es cierto para todo orden de A. Esto es consecuencia de la Proposición 1.2.1 y el Teorema 4.2.2

Lema 4.3.2 *Sea K es un subcuerpo de $\mathbb{C}$ y R un orden de $M_2(K)$. Entonces R_1 es discreto en* $\mathrm{SL}_2(\mathbb{C})$ *si y sólo si $K = \mathbb{Q}$ o una extensión cuadrática imaginaria de $\mathbb{Q}$.*

Demostración. La condición suficiente es evidente y ya la hemos contado al final de la sección anterior. Recíprocamente supongamos que R_1 es discreto. Podemos suponer que $R = M_2(\mathcal{O})$ donde $\mathcal{O}$ es un orden en K. Si $\alpha_1, \alpha_2, \ldots, \alpha_n$ es una base entera de $\mathcal{O}$, entonces los elementos de la forma $\begin{pmatrix} 1 & \alpha_i \\ 0 & 1 \end{pmatrix}$ con $i = 1, 2, \ldots, n$, generan un subgrupo abeliano libre de torsión de R_1. Por el Teorema 4.2.5 $n = [K : \mathbb{Q}] \leq 2$ y por el Teorema 4.2.4 si $K \subseteq \mathbb{R}$ entonces $n = 1$. Esto acaba la demostración del lema. □

Lema 4.3.3 *La clase de grupos kleinianos es cerrada para subgrupos y cocientes.*

Demostración. Sea G un grupo finito de tipo kleiniano. Si $H = G/N$ es un cociente de G entonces $\mathbb{Q}H$ es isomorfo a $\mathbb{Q}G/\Delta_{\mathbb{Q}}(G, N)$ y por lo tanto los cocientes simples de $\mathbb{Q}H$ son también cocientes de $\mathbb{Q}G$. Por tanto H es de tipo kleiniano.

Supongamos ahora que H es un subgrupo de G y sea A un cociente simple no conmutativo de $\mathbb{Q}H$. Como $\mathbb{Q}H$ es una subálgebra de $\mathbb{Q}G$ entonces A está contenido en un subálgebra simple B de $\mathbb{Q}G$. Como A no es un cuerpo tampoco lo es B, por tanto B es un álgebra de cuaterniones que contiene un orden R tal que R_1 es un subgrupo discreto de $\mathrm{SL}_2(\mathbb{C})$. Entonces A es un álgebra de cuaterniones sobre un subcuerpo K del centro de B (esto es una consecuencia del Lema 3.3.6), $S = R \cap A$ es un orden de B y S_1 también es un subgrupo discreto de $\mathrm{SL}_2(\mathbb{C})$. □

4.4. Las álgebras de grupo

Nuestro objetivo final es caracterizar los grupos de tipo kleiniano. En esta memoria sólo hemos conseguido caracterizar algunos de los grupos de tipo kleiniano. Obsérvese que si G es un grupo de tipo kleiniano entonces todos los cocientes simples de $\mathbb{Q}G$ tienen grado menor o igual que 2, es decir la dimensión sobre su centro es 1 ó 4. Por tanto todas la representaciones irreducibles de G tienen grado menor o igual que 2. Un resultado de Gow-Huppert [16] muestra que esto implica que G tiene un subgrupo nilpotente de índice menor o igual que 2, es decir, G está muy cercano a ser nilpotente. Por esta razón es una buena idea empezar por caracterizar los grupos nilpotentes de tipo kleiniano.

La herramienta principal que utilizaremos son los dos siguientes Teoremas de Jespers y Leal [29] que caracterizan los cocientes simples de un álgebra de grupo $\mathbb{Q}G$ sobre un grupo finito nilpotente G que son de la forma $M_n(D)$ para D un anillo de división y $n \leq 2$.

Para cada entero positivo n, ξ_n representa una raíz $n-$ésima primitiva de la unidad. También necesitamos los siguientes grupos:

$$D_{16}^{+} = \langle a, b | a^8 = b^2 = 1, ba = a^5 b \rangle$$

$$D_{16}^- = \langle a, b | a^8 = b^2 = 1, ba = a^3 b \rangle$$
$$\mathcal{D} = \langle a, b, c | a^2 = b^2 = c^4 = 1, ac = ca, bc = cb, ba = c^2 ab \rangle$$
$$\mathcal{D}^+ = \langle a, b, c | a^4 = b^2 = c^4 = 1, ac = ca, bc = cb, ba = ca^3 b \rangle$$

Los tres primeros grupos tienen orden 16 y el último tiene orden 32.

Sea G un grupo finito de tipo kleiniano y e un idempotente central primitivo de $\mathbb{Q}G$ tal que $\mathbb{Q}Ge$ no es un cuerpo. Entonces $\mathbb{Q}Ge$ es o bien un anillo de división o $M_2(K)$ con K un cuerpo. Además por el Lema 4.3.2, $K = \mathbb{Q}$ ó una extensión cuadrática imaginaria de $\mathbb{Q}$. Como consecuencia inmediata de los Teoremas 2.2 y 2.3 de [29] deducimos lo siguiente:

Proposición 4.4.1 *Sean G un grupo finito nilpotente de tipo kleiniano y e un idempotente central primitivo de $\mathbb{Q}G$ tal que $\mathbb{Q}Ge$ no es un cuerpo.*

1. *Si $\mathbb{Q}Ge$ es un anillo de división no conmutativo, entonces se da uno de los siguientes casos:*
   a) *$Ge \cong Q_{2^n}$ y $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q}(\xi_{2^{n-1}} + \xi_{2^{n-1}}^{-1}))$ para $n \geq 3$,*
   b) *$Ge \cong Q_8 \times C_n$, y $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q}(\xi_n))$ con n impar y el orden de 2 módulo n es impar.*
2. *En caso contrario, es decir, si $\mathbb{Q}Ge \cong M_2(K)$ con K un cuerpo, entonces se da uno de los siguientes casos:*
   a) *$K = \mathbb{Q}$ y $Ge \cong D_4$;*
   b) *$K = \mathbb{Q}(\sqrt{-2})$ y $Ge \cong D_{16}^-$;*
   c) *$K = \mathbb{Q}(i)$ y $Ge \cong D_{16}^+, \mathcal{D}$ ó $\mathcal{D}^+$;*
   d) *$K = \mathbb{Q}(\sqrt{-3})$ y $Ge \cong D_4 \times C_3$ ó $Q_8 \times C_3$.*

Ahora podemos caracterizar los grupos finitos nilpotentes de tipo kleiniano en función de las componentes de la descomposición de Wedderburn del álgebra de grupo $\mathbb{Q}G$.

Teorema 4.4.2 *Sea G un grupo finito nilpotente. Son equivalentes:*

a) *G es de tipo kleiniano.*

b) *Todo cociente simple no conmutativo de $\mathbb{Q}G$ es isomorfo a $\mathbb{H}(K)$ con $K = \mathbb{Q}$ ó $\mathbb{Q}(\sqrt{2})$ o a $M_2(K)$ con $K = \mathbb{Q}$ ó $\mathbb{Q}(\sqrt{-n})$ con $n = 1, 2$ ó 3.*

En tal caso si e es un idempotente central primitivo de $\mathbb{Q}G$ se verifica:

1. *Si* $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q})$ *entonces* $Ge \cong Q_8$.
2. *Si* $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q}(\sqrt{2}))$ *entonces* $Ge \cong Q_{16}$.
3. *Si* $\mathbb{Q}Ge \cong M_2(\mathbb{Q})$ *entonces* $Ge \cong D_4$.
4. *Si* $\mathbb{Q}Ge \cong M_2(\mathbb{Q}(i))$ *entonces* $Ge \cong D_{16}^+, \mathcal{D}$ *ó* $\mathcal{D}^+$.
5. *Si* $\mathbb{Q}Ge \cong M_2(\mathbb{Q}(\sqrt{-2}))$ *entonces* $Ge \cong D_{16}^-$.
6. *Si* $\mathbb{Q}Ge \cong M_2(\mathbb{Q}(\sqrt{-3}))$ *entonces* $Ge \cong D_4 \times C_3$ *ó* $Ge \cong Q_8 \times C_3$

Demostración. $b) \Rightarrow a)$. Se sigue de la definición de grupo de tipo kleiniano.

$a) \Rightarrow b)$. Sea G un grupo finito nilpotente de tipo kleiniano y sea e un idempotente central primitivo de $\mathbb{Q}G$ tal que $\mathbb{Q}Ge$ no es conmutativo.

Si $\mathbb{Q}Ge$ es un anillo de división no conmutativo, entonces por la Proposición 4.4.1 o bien $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q}(\xi_{2^{n-1}} + \xi_{2^{n-1}}^{-1}))$ para $n \geq 3$ o bien $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q}(\xi_n))$ con n impar y el orden de 2 módulo n es impar. En el primer caso $Ge \cong Q_{2^n}$ y por el Lema 4.3.3, Q_{2^n} es un grupo de tipo kleiniano. Pero en la descomposición de Wedderburn de $\mathbb{Q}Q_{2^n}$ aparece una componente simple del estilo $M_2(\mathbb{Q}(\xi_{2^{n-2}} + \xi_{2^{n-2}}^{-1}))$ (véase [29]). Por el Lema 4.3.2 tenemos que $\mathbb{Q}(\xi_{2^{n-2}} + \xi_{2^{n-2}}^{-1}) = \mathbb{Q}$ y por tanto $n \leq 4$. Luego $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q})$ ó $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q}(\sqrt{2}))$.

Supongamos que $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q}(\xi_n))$ con n impar y el orden de 2 módulo n es impar y sea R un orden de $\mathbb{H}(\mathbb{Q}(\xi_n))$ tal que R_1 actúa discontinuamente en $\mathbb{H}^3$. Sea $K = \mathbb{Q}(\xi_n)$. Sea $\mathcal{R}$ el anillo de enteros de $K(\mathbf{i})$. Por el Teorema de las Unidades de Dirichlet, $\mathcal{R}$ tiene rango libre de torsión $\varphi(n) - 1$. Entonces por el Teorema 4.2.5 tenemos que $\varphi(n) - 1 \leq 2$ y por lo tanto $\varphi(n) \leq 3$. Como n es impar tenemos que $n = 3$. Pero el orden de 2 módulo 3 es 2 en contra de que ha de ser impar. Por tanto $\mathbb{Q}G$ no tiene cocientes simples de esta forma.

Lo que queda de demostración es consecuencia inmediata del Lema 4.3.2 y de la Proposición 4.4.1. □

4.5. Grupos que no son 2-grupos

En esta sección vamos a caracterizar los grupos finitos nilpotentes de tipo kleiniano que no son 2-grupos.

Del Teorema 4.4.2 se deduce que si G es un grupo finito nilpotente de tipo kleiniano y S es un cociente simple no conmutativo de $\mathbb{Q}G$ entonces $dim_{\mathbb{Q}} Z(S) \leq 2$. Si $G \times C_n$ es finito nilpotente de tipo kleiniano, donde G no es abeliano y C_n es cíclico de orden n, entonces $\mathbb{Q}(\xi_n)$ está contenido en el centro de un cociente simple de $\mathbb{Q}(G \times C_n)$ ya que si A es un cociente simple de $\mathbb{Q}G$ entonces $A \otimes_{Z(A)} \mathbb{Q}(\xi_n)$ es

un cociente simple de $\mathbb{Q}(G \times C_n) = \mathbb{Q}G \otimes_{\mathbb{Q}} \mathbb{Q}C_n$. Por tanto $dim_{\mathbb{Q}}\mathbb{Q}(\xi_n) \leq 2$ lo que significa que n es un divisor de 4 ó 6.

Si $G_1 \times G_2$ es un grupo de tipo kleiniano donde G_1 y G_2 son nilpotentes no abelianos entonces $\mathbb{Q}(G_1 \times G_2) \cong \mathbb{Q}G_1 \otimes_{\mathbb{Q}} \mathbb{Q}G_2$ tiene un cociente simple en común con una de las siguientes álgebras

$$\mathbb{H}(\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{H}(\mathbb{Q}) \cong \mathbb{H}(\mathbb{Q}) \otimes_{\mathbb{Q}} M_2(\mathbb{Q}) \cong M_2(\mathbb{H}(\mathbb{Q}))$$

$$\mathbb{H}(\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{H}(\mathbb{Q}(\sqrt{2})) \cong M_2(\mathbb{H}(\mathbb{Q}(\sqrt{2})))$$

$$\mathbb{H}(\mathbb{Q}) \otimes_{\mathbb{Q}} M_2(\mathbb{Q}(\sqrt{-n})) \cong M_2(\mathbb{Q}) \otimes_{\mathbb{Q}} M_2(\mathbb{Q}(\sqrt{-n})) \cong M_4(Q(\sqrt{-n}))$$

$$M_2(\mathbb{Q}(\sqrt{-n})) \otimes_{\mathbb{Q}} M_2(\mathbb{Q}(\sqrt{-n})) \cong 2M_4(\mathbb{Q}(\sqrt{-n}))$$

$$M_2(\mathbb{Q}(\sqrt{-n})) \otimes_{\mathbb{Q}} M_2(\mathbb{Q}(\sqrt{-m})) \cong M_4(\mathbb{Q}(\sqrt{-n}, \sqrt{-m}))$$

para $n, m = 1, 2, 3$ y $n \neq m$.

Por tanto si G es un grupo finito nilpotente de tipo kleiniano entonces $G = G_1 \times A$ donde G_1 es indescomponible y A es abeliano de exponente un divisor de 4 ó 6. Como G es nilpotente G_1 es un p-grupo para algún primo p. Por otro lado G_1 tiene un cociente isomorfo a uno de los siguientes grupos $Q_8, D_4, D_{16}^+, D_{16}^-, \mathcal{D}, \mathcal{D}^+, Q_{12}, Q_{16}, Q_8 \times C_3$ ó $D_4 \times C_3$ de donde deducimos que G_1 es un 2-grupo.

Hemos demostrado el siguiente resultado.

Corolario 4.5.1 *Sea G un grupo finito nilpotente no abeliano de tipo kleiniano. Entonces $G = G_1 \times C_2^k \times C_4^m \times C_3^n$ donde G_1 es un $2-$grupo indescomponible no abeliano de tipo kleiniano y $k, m, n \geq 0$ son enteros. Además $nm = 0$, es decir, si aparece C_4 en la descomposición de G no aparece C_3 y viceversa.*

De hecho podemos describir los grupos finitos nilpotentes de tipo kleiniano que no son 2-grupos de forma sencilla.

Corolario 4.5.2 *Sea G un grupo finito nilpotente que no es un 2-grupo. Entonces G es de tipo kleiniano si y sólo si o es abeliano o es de la forma $H \times C_2^n \times C_3^m$ donde H es uno de los grupos de tipo $(a) - (f)$ del Teorema 3.1.9.*

Demostración. Supongamos que $G = H \times C_2^n \times C_3^m$ con H de de los tipos $(a) - (f)$ del Teorema 3.1.9. Entonces las componentes simples no conmutativas de $\mathbb{Q}(H \times C_2^n)$ son todas isomorfas a $\mathbb{H}(\mathbb{Q})$ ó $M_2(\mathbb{Q})$ y las de $\mathbb{Q}C_3^m$ isomorfas a $\mathbb{Q}$ ó $\mathbb{Q}(\sqrt{-3})$. Por tanto las de $\mathbb{Q}G$ son isomorfas a $\mathbb{H}(\mathbb{Q}), M_2(\mathbb{Q})$ ó $\mathbb{H}(\mathbb{Q}) \otimes \mathbb{Q}(\sqrt{-3}) \cong M_2(\mathbb{Q}(\sqrt{-3})) \cong M_2(\mathbb{Q}) \otimes \mathbb{Q}(\sqrt{-3})$.

Recíprocamente supongamos que G es nilpotente no abeliano de tipo kleiniano que no es un 2-grupo. Por el Corolario 4.5.1, $G \cong H \times C_2^n \times C_3^m$ donde $m \geq 1$ y H es un 2-grupo indescomponible de tipo kleiniano. Si $\mathbb{H}(\mathbb{Q}(\sqrt{2})), M_2(\mathbb{Q}(i))$ ó $M_2(\mathbb{Q}(\sqrt{-2}))$

es isomorfo a un cociente de $\mathbb{Q}H$, entonces $\mathbb{Q}G$ tiene un cociente simple isomorfo a $\mathbb{H}(\mathbb{Q}(\sqrt{2}))\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt{-3}) \cong M_2(\mathbb{Q}(\sqrt{2},\sqrt{-3}))$ ó $M_2(\mathbb{Q}(i))\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt{-3}) \cong M_2(\mathbb{Q}(\sqrt{3},i))$ ó $M_2(\mathbb{Q}(\sqrt{-2}))\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt{-3}) \cong M_2(\mathbb{Q}(\sqrt{-2},\sqrt{-3}))$ y G no sería de tipo kleiniano por el Teorema 4.4.2. Por tanto todos los cocientes simples de $\mathbb{Q}H$ han de ser isopmorfos a $\mathbb{H}(\mathbb{Q})$ ó $M_2(\mathbb{Q})$. Por el Teorema 3.1.9 H es de uno de los tipos $(a)-(i)$ de dicho teorema. Pero como H es nilpotente los tipos (h) e (i) están excluidos. Por otro lado el tipo (g) también está excluido por tener una componente simple isomorfa a $\mathbb{H}(\mathbb{Q}(\sqrt{2}))$. □

De los Corolarios 4.5.1 y 4.5.2 se deduce que la mayor dificultad en la búsqueda de la descripción los grupos nilpotentes de tipo kleiniano está en la determinación de los 2-grupos indescomponibles no abelianos que son de tipo kleiniano.

El resto del Capítulo nos centraremos en el caso en que G es un 2-grupo de tipo kleiniano. Por el Teorema 4.4.2, para cada idempotente central primitivo e de $\mathbb{Q}G$ tal que $\mathbb{Q}Ge$ no es un cuerpo, el grupo Ge es isomorfo a uno de los siguientes siete grupos:

$$D_4, Q_8, D_{16}^+, D, D^+, D_{16}^-, Q_{16}.$$

El siguiente lema nos proporciona algunas propiedades que utilizaremos en la siguiente sección. Su demostración es inmediata.

Lema 4.5.3 *Si $G = D_4, Q_8, D_{16}^+$ ó $\mathcal{D}$, entonces $G/Z(G) \cong C_2$ y $G' \subseteq Z(G)$, mientras que si $G = \mathcal{D}^+, D_{16}^-$ ó Q_{16} ninguna de estas propiedades se verifica.*

4.6. 2-Grupos con conmutador central

Definición 4.6.1 *Denotaremos por $\mathcal{G}$ a la clase de grupos formada por todos los 2-grupos finitos de tipo kleiniano G tales que el subgrupo conmutador es central, es decir, $G' \subseteq Z(G)$.*

Por el Lema 4.5.3 y el Teorema 4.4.2 decir que un grupo $G \in \mathcal{G}$ es equivalente a decir que Ge es un 2-grupo abeliano o isomorfo a D_8, Q_8, D_{16}^+ ó D para todo idempotente central primitivo e de $\mathbb{Q}G$.

Del Lema 4.3.3 se deduce el siguiente lema.

Lema 4.6.2 *La clase $\mathcal{G}$ es cerrada para imágenes homomórficas y subgrupos.*

El siguiente lema será de gran utilidad.

Lema 4.6.3 *Sea $G \in \mathcal{G}$ no abeliano. Entonces se verifica que $Z(G)$ tiene exponente un divisor de 4 y los exponentes de $G/Z(G)$ y G' son ambos igual a 2.*

Demostración. Sea $e_1, e_2, \ldots, e_n$ un conjunto completo de idempotentes centrales primitivos de $\mathbb{Q}G$. Cada Ge_i se puede considerar como un subgrupo multiplicativo de $\mathbb{Q}Ge_i$ y la aplicación $f : G \to \prod_{i=1}^{n} Ge_i$ definida por $f(g) = (ge_1, ge_2, \ldots, ge_n)$ es un homomorfismo inyectivo de grupos. Reordenemos los $e_i's$ de forma que $Ge_1, \ldots, Ge_k$ son abelianos y $Ge_{k+1}, \ldots, Ge_n$ no son abelianos. Como $G \in \mathcal{G}$ por el Lema 4.5.3 tenemos que $Ge_i = D_4, Q_8, D_{16}^+$ ó D para $i = k+1, \ldots, n$ y para todos estos grupos se verifica que su subgrupo conmutador tiene exponente 2. Luego el exponente de G' es 2. Pongamos $H = Ge_1 \times \cdots \times Ge_k$ y $K = Ge_{k+1} \times \cdots \times Ge_n$. Entonces $f(Z(G)) \subset H \times Z(K)$ y por lo tanto f induce un homomorfismo inyectivo $f' : G/Z(G) \to \prod_{i=k+1}^{n} K/Z(K) = \prod_{i=k+1}^{n} Ge_i/Z(Ge_i)$ que tiene exponente 2 por el Lema 4.5.3. Luego $G/Z(G)$ tiene exponente 2.

Sea ahora $g \in Z(G)$. Entonces $g(1 - \widehat{G'})$ es una unidad central de $\mathbb{Q}G(1 - \widehat{G'})$. Como $G \in \mathcal{G}$ tenemos que $\mathbb{Q}G(1 - \widehat{G'}) \cong \mathbb{H}(\mathbb{Q})^m \times M_2(\mathbb{Q})^s \times M_2(\mathbb{Q}(i))^r$ para ciertos $r, s, m \geq 0$, pero las unidades centrales periódicas de orden una potencia de 2 de $\mathbb{H}(\mathbb{Q}), M_2(\mathbb{Q})$ y $M_2(\mathbb{Q}(i))$ tienen orden un divisor de 4. Por lo tanto $g^4(1 - \widehat{G'}) = (1 - \widehat{G'})$. Como G no es abeliano tenemos que $G' \neq 1$ y comparando coeficientes tenemos que $g^4 \in G'$ y por tanto $g^4 - \widehat{G'} = 1 - \widehat{G'}$, con lo que $g^4 = 1$. Luego el orden de g es un divisor de 4. □

Recuérdese que $r(G)$ denota el rango de G, es decir, el menor de los cardinales de los conjuntos generadores de G.

Como consecuencia del Lema 4.6.3, si $G \in \mathcal{G}$, no es abeliano y $r(G) = n$ entonces G es un cociente de un grupo de la forma

$$B_n = \langle x_1, x_2, \ldots, x_n | x_i^8 = [x_i, x_j^2] = [x_i, [x_j, x_k]] = 1, 1 \leq i, j, k \leq n \rangle$$

En estos grupos utilizaremos la notación

$$t_{ij} = [x_i, x_j].$$

De hecho abusaremos de esta notación de la siguiente forma. A menudo pondremos $G = \langle x_1, x_2, \ldots, x_n, Z(G) \rangle$ para un grupo $G \in \mathcal{G}$ y en tal caso pondremos $t_{ij} = [x_i, x_j]$.

Obsérvese que como t_{ij} y x_i^2 son centrales para todo i, j se tiene que $t_{ij}^2 = 1$ y $t_{ij} = t_{ji}$.

La siguiente proposición demuestra que el grupo $B_2 \in \mathcal{G}$ y por tanto ya tenemos caracterizado los grupos en $\mathcal{G}$ de rango 2.

Proposición 4.6.4 *$B_2 \in \mathcal{G}$.*

Demostración. Para demostrar que $B_2 \in \mathcal{G}$ basta demostrar que las componentes simples no conmutativas de $\mathbb{Q}B_2$ son de las que aparecen listadas en el Teorema 4.4.2. De hecho tenemos que los idempotentes centrales primitivos e tales que $\mathbb{Q}B_2e$ no es conmutativo y las correspondientes álgebras simples $\mathbb{Q}B_2e$ son:

$$\begin{aligned}
e_1 &= (1-\widehat{B_2'})\widehat{x_1^2}\widehat{x_2^2},\\
e_2 &= (1-\widehat{B_2'})\widehat{x_1^2}\widehat{x_2^4}(1-\widehat{x_2^2}),\\
e_3 &= (1-\widehat{B_2'})(1-\widehat{x_1^2})\widehat{x_1^4}\widehat{x_2^2},\\
e_4 &= (1-\widehat{B_2'})(1-\widehat{x_1^2})\widehat{x_1^4}(1-\widehat{x_2^2})\widehat{x_2^4},\\
e_5 &= (1-\widehat{B_2'})\widehat{x_1^2}(1-\widehat{x_2^4}),\\
e_6 &= (1-\widehat{B_2'})(1-\widehat{x_1^2})\widehat{x_1^4}(1-\widehat{x_2^4}),\\
e_7 &= (1-\widehat{B_2'})(1-\widehat{x_1^4})\widehat{x_2^4}\widehat{x_2^2},\\
e_8 &= (1-\widehat{B_2'})(1-\widehat{x_1^4})\widehat{x_2^4}(1-\widehat{x_2^2}),\\
e_9 &= (1-\widehat{B_2'})(1-\widehat{x_1^4})(1-\widehat{x_2^4})\widehat{x_1^2x_2^2} \text{ y}\\
e_{10} &= (1-\widehat{B_2'})(1-\widehat{x_1^4})(1-\widehat{x_2^4})(1-\widehat{x_1^2x_2^2}).
\end{aligned}$$

Además

$$\mathbb{Q}Ge_i \cong \begin{cases} M_2(\mathbb{Q}) & \text{si } i<4,\\ \mathbb{H}(\mathbb{Q}) & \text{si } i=4 \text{ y}\\ M_2(\mathbb{Q}(i) & \text{si } i>4. \end{cases}$$

□

Sin embargo $B_n \notin \mathcal{G}$ si $n \geq 3$ ya que no satisface la tesis del siguiente lema.

Lema 4.6.5 *Sea $G \in \mathcal{G}$ tal que $G = \langle x_1, x_2, \ldots, x_n, Z(G)\rangle$. Si para algún $i = 1, 2, \ldots, n$, $G' \neq \langle [x_i, x_j] \,|\, i \neq j\rangle$, entonces $x_i^4 \in \langle [x_i, x_j] \,|\, i \neq j\rangle$.*

Demostración. Para cada i la imagen de x_i en $H = G/\langle [x_i, x_j] \,|\, i \neq j\rangle$ es central. Por el Lema 4.6.2, $H \in \mathcal{G}$ pero como $G' \neq \langle [x_i, x_j] \,|\, i \neq j\rangle$ H no es abeliano. Entonces por el Lema 4.6.3, $x_i^4 \in \langle [x_i, x_j] \,|\, i \neq j\rangle$. □

Del Lema 4.6.5 deducimos condiciones adicionales para los grupos de rango 3 en $\mathcal{G}$.

Lema 4.6.6 *Si $G \in \mathcal{G}$ y $r(G) = 3$ entonces G es cociente de uno de los siguientes grupos*

1. $B_2 \times C_4$
2. $B_{31} = B_3/\langle t_{23}, x_2^4, x_3^4\rangle$

3. $B_{32} = B_3/\langle t_{23}, x_2^4 t_{12}, x_3^4 t_{13}\rangle$

4. $A_{31} = B_3/\langle x_1^4, x_2^4, x_3^4\rangle$

5. $A_{32} = B_3/\langle x_1^4, x_2^4 t_{12}, x_3^4 t_{13}\rangle$

Demostración. Por los comentarios hechos más arriba sabemos que al ser $r(G) = 3$, G es un cociente de B_3 y abusaremos de la notación llamando x_i a la imagen del correspondiente elemento de B_3 en G y t_{ij} al conmutador de x_i y x_j en G para $i, j = 1, 2, 3$.

Si $r(G') = 1$ podemos suponer cambiando el conjunto de generadores de G si fuera necesario que uno de los x_i es central, por ejemplo x_3, con lo que $t_{13} = t_{23} = 1$. Del Lema 4.6.3 se deduce que $x_3^4 = 1$ y por tanto G es un cociente de $B_2 \times C_4 = B_3/\langle t_{13}, t_{23}, x_3^4\rangle$.

Si $r(G') = 2$, cambiando los generadores si es necesario podemos suponer que $t_{23} = 1$ y que t_{12}, t_{13} y $t_{12}t_{13}$ son los tres diferentes de 1. Por el Lema 4.6.5, $x_1^4 \in \langle t_{12}\rangle, x_2^4 \in \langle t_{13}\rangle$ y $(x_1x_2)^4 \in \langle t_{12}t_{13}\rangle$ de donde se deduce que o bien $x_2^4 = x_3^4 = 1$ o bien $x_2^4 = t_{12}$ y $x_3^4 = t_{13}$, es decir G es cociente de B_{31} ó B_{32}.

Finalmente supongamos que $r(G') = 3$. Aplicando de nuevo el Lema 4.6.5 tenemos que existen $\alpha_2, \alpha_3, \beta_1, \beta_3, \gamma_1, \gamma_2 \in \{0, 1\}$ tales que

$$x_1^4 = t_{12}^{\alpha_2} t_{13}^{\alpha_3}, x_2^4 = t_{12}^{\beta_1} t_{13}^{\beta_3} \text{ y } x_3^4 = t_{13}^{\gamma_1} t_{23}^{\gamma_2}$$

Entonces

$$\begin{aligned}(x_1x_2)^4 &= t_{12}^{\alpha_2+\beta_2} t_{13}^{\alpha_3} t_{23}^{\beta_3} \in \langle t_{12}, t_{13}t_{23}\rangle\\ (x_1x_3)^4 &= t_{12}^{\alpha_2} t_{13}^{\alpha_3+\gamma_1} t_{23}^{\gamma_2} \in \langle t_{13}, t_{12}t_{13}\rangle\\ (x_2x_3)^4 &= t_{12}^{\beta_1} t_{13}^{\gamma_1} t_{23}^{\beta_3+\gamma_2} \in \langle t_{23}, t_{12}t_{13}\rangle\end{aligned}$$

de donde se deduce que $\alpha_3 = \beta_3$, $\alpha_2 = \gamma_2$ y $\beta_1 = \gamma_1$. Pongamos $\beta_1 = a_1$, $\alpha_2 = a_2$ y $\alpha_3 = a_3$. Entonces

$$\begin{aligned} x_1^4 &= t_{12}^{a_2} t_{13}^{a_3}\\ x_2^4 &= t_{12}^{a_1} t_{13}^{a_3}\\ x_3^4 &= t_{13}^{a_1} t_{23}^{a_2}\\ (x_1x_2)^4 &= t_{12}^{a_1+a_2} t_{13}^{a_3} t_{23}^{a_3}\\ (x_1x_3)^4 &= t_{12}^{a_2} t_{13}^{a_1+a_3} t_{23}^{a_2}\\ (x_2x_3)^4 &= t_{12}^{a_1} t_{13}^{a_1} t_{23}^{a_2+a_3}\\ (x_1x_2x_3)^4 &= t_{12}^{a_1+a_2} t_{13}^{a_1+a_3} t_{23}^{a_2+a_3}\end{aligned} \tag{4.1}$$

Estudiando los ocho valores posibles de (a_1, a_2, a_3) se deduce que una de las siete potencias cuartas de (4.1) es igual a 1 y cambiando los generadores podemos suponer

que $x_1^4 = 1$ con lo que $a_2 = a_3 = 1$. Entonces $x_2^4 = t_{12}^{a_1}$ y $x_3^4 = t_{13}^{a_1}$ de donde se deduce que G es un cociente de A_{31} (si $a_1 = 0$) ó A_{32} si $(a_1 = 1)$. □

En la demostración del teorema principal de este capítulo veremos que los 5 grupos del lema anterior están en $\mathcal{G}$, con lo que ya tenemos descritos los elementos no abelianos de $\mathcal{G}$ de rango menor o igual que 3 como cocientes de 5 grupos. Para la descripción de los de rango mayor que 3 el siguiente lema nos resultará de gran utilidad.

Lema 4.6.7 (Lema 1,4 **[41])** *Sea G un grupo finito. Entonces $G/Z(G) \cong C_p \times C_p$ si y sólo si $|G'| = p$ y toda representación compleja irreducible de G tiene grado igual a 1 ó p.*

Si $G \in \mathcal{G}$ entonces toda representación irreducible de G tiene grado 1 ó 2. Por tanto del lema anterior se deduce el siguiente resultado.

Lema 4.6.8 *Si $G \in \mathcal{G}$ entonces $r(G/Z(G)) = 2$ si y sólo si $r(G') = 1$.*

A menudo interpretaremos un 2-grupo abeliano elemental como un espacio vectorial sobre el cuerpo $\mathbb{F}_2$ con dos elementos y utilizaremos el lenguaje de álgebra lineal. Los elementos 0 y 1 los interpretaremos indistintamente como números enteros o como elementos de $\mathbb{F}_2$.

Ahora vamos a introducir una notación a la que le sacaremos mucho partido.

Sean $G \in \mathcal{G}$ y $x_1, x_2, \ldots, x_n$ elementos de G tales que $G = \langle x_1, x_2, \ldots, x_n, Z(G)\rangle$. Supongamos que $G' = \langle t\rangle \cong C_2$. Entonces para cada i, j existe $\alpha_{ij} \in \{0, 1\}$ tal que $t_{ij} = t^{\alpha_{ij}}$. Consideraremos entonces la siguiente matriz simétrica $A = (\alpha_{ij})_{ij}$ como un elemento de $M_n(\mathbb{F}_2)$. Consideramos ahora un elemento $x = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ con $\alpha \in \{0, 1\}$. Entonces x es un elemento central de G si y sólo si el vector $(\alpha_1, \cdots, \alpha_n)$ pertenece al espacio nulo de la matriz A. Del Lema 4.6.8 se deduce que esta matriz tiene rango 2.

Lema 4.6.9 *Si un grupo finito G tiene cuatro elementos x_1, x_2, x_3, x_4 tales que $[x_1, x_2] \neq 1$, $[x_3, x_4] \neq 1$ y $[x_i, x_j] = 1$ para todo $1 \leq i \leq 2 < j \leq 4$, entonces $G \notin \mathcal{G}$.*

Demostración. Supongamos que $G \in \mathcal{G}$. Por el Lema 4.6.2 podemos suponer que $G = \langle x_1, x_2, x_3, x_4\rangle$ y que $G' = \langle [x_1, x_2]\rangle = \langle [x_3, x_4]\rangle = C_2$. Entonces la matriz asociada es al siguiente

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

que tiene rango 4, una contradicción. □

Demostramos ahora dos lemas para grupos de rango 4 módulo el centro.

Lema 4.6.10 *Sea $G \in \mathcal{G}$ tal que $r(G/Z(G)) = 4$. Entonces $r(G') = 3$.*

Demostración. Por el Lema 4.6.2 podemos suponer que $r(G) = 4$ y por tanto G es un cociente de B_4, digamos $G = B_4/T$. Entonces $T \subseteq Z(B_4)$ ya que en otro caso $r(G/Z(G)) \leq 3$. Luego $G' \cong B_4'/T \cap B_4'$.

Afirmamos que $T \cap B_4'$ no puede estar contenido en ninguno de los siguientes subgrupos de B_4':

$$\begin{aligned} M_{12-34} &= \langle t_{13}, t_{14}, t_{23}, t_{24}, t_{12}t_{34} \rangle \\ M_{13-24} &= \langle t_{12}, t_{14}, t_{23}, t_{34}, t_{13}t_{24} \rangle \\ M_{14-23} &= \langle t_{12}, t_{13}, t_{24}, t_{34}, t_{14}t_{23} \rangle \end{aligned} \tag{4.2}$$

Supongamos por ejemplo que $T \cap B_4' \subseteq M_{12-34}$. Entonces $t_{12} \notin TM_{12-34}$ ya que en caso contrario tendríamos que $t_{12} = tm$ con $t \in T$ y $m \in M_{12-34}$ luego $t \in T \cap B_4' \subseteq M_{12-34}$ y por lo tanto $t_{12} \in M_{12-34}$, en contra de que G no es abeliano. Análogamente $t_{34} \notin TM_{12-34}$. Entonces el cociente $H = G/TM_{12-34}$ verifica las condiciones del Lema 4.6.9 y por lo tanto $H \notin \mathcal{G}$ lo que contradice el Lema 4.6.2.

Veamos primero que $r(B_4' \cap T) \geq 3$. Por reducción al absurdo suponemos que $r(B_4' \cap T) \leq 2$.

Afirmamos que t_{ij} no pertenece a T para ninguna pareja $1 \leq i, j \leq 4$ con $i \neq j$. Esto es consecuencia del párrafo anterior si $r(T \cap B_4') \leq 1$. Por lo tanto supongamos que $r(T \cap B_4') = 2$ y que $t_{ij} \in T$ para algún $i \neq j$. Por simetría podemos suponer que $t_{12} \in T$, luego

$$T \cap B_4' = \langle t_{12}, t_{13}^{\alpha_1} t_{14}^{\alpha_2} t_{23}^{\alpha_3} t_{24}^{\alpha_4} t_{34}^{\alpha_5} \rangle$$

para ciertos $\alpha_i \in \{0, 1\}$. Como $T \cap B_4' \not\subseteq M_{13-24}$ y $T \cap B_4' \not\subseteq M_{14-23}$ tenemos que $\alpha_1 \neq \alpha_4$ y $\alpha_2 \neq \alpha_3$. Por simetría podemos suponer que $\alpha_1 = 1$ y por tanto $\alpha_4 = 0$. Si $\alpha_2 = 1$ entonces $T \cap B_4' = \langle t_{12}, t_{13}t_{14}t_{34}^{\alpha_5} \rangle$. Haciendo el cambio de variable x_3 por x_3x_4 tenemos que $T \cap B_4' = \langle t_{12}, t_{13}t_{34}^{\alpha_5} \rangle \subseteq M_{14-23}$ una contradicción. Por tanto $\alpha_2 = 0$, con lo que $T \cap B_4' = \langle t_{12}, t_{13}t_{23}t_{34}^{\alpha_5} \rangle$. Si $\alpha_5 = 0$, haciendo el cambio de variable x_1 por x_1x_2 tenemos que $T \cap B_4' \subseteq M_{14-23}$ y si $\alpha_5 = 1$ haciendo el cambio de variable x_4 por $x_1x_2x_4$ tenemos que $T \cap B_4' \subseteq M_{13-24}$ una contradicción.

Por lo tanto $t_{ij} \notin T$ para todo $i \neq j$. Podemos suponer que el elemento $t_{12}t_{13}^{\alpha_1}t_{14}^{\alpha_2}t_{23}^{\alpha_3}t_{24}^{\alpha_4}t_{34}^{\alpha_5} \in T$ para ciertos $\alpha_i \in \{0, 1\}$ y con los cambios sucesivos de x_2 por $x_2x_3^{\alpha_1}x_4^{\alpha_2}$ y de x_1 por $x_1x_3^{\alpha_1}x_4^{\alpha_2}$ podemos suponer que $t_{12}t_{34}^{\alpha_5} \in T$. Como $t_{ij} \notin T$ tenemos que $\alpha_5 = 1$, es decir, $t_{12}t_{34} \in T$. Por lo tanto existen unos nuevos α_i's tales que

$$T \cap B_4' = \langle t_{12}t_{34}, t = t_{12}^{\alpha_1}t_{13}^{\alpha_2}t_{14}^{\alpha_3}t_{23}^{\alpha_4}t_{24}^{\alpha_5}t_{34}^{\alpha_6} \rangle$$

Como $T \cap B_4' \not\subseteq M_{12-34}$ necesariamente $\alpha_1 \neq \alpha_6$. Por simetría podemos suponer que $\alpha_1 = 1$ y $\alpha_6 = 0$ obteniendo que $T \cap B_4' = \langle t_{12}t_{34}, t_{12}t_{13}^{\alpha_2}t_{14}^{\alpha_3}t_{23}^{\alpha_4}t_{24}^{\alpha_5}\rangle$. Por argumentos similares $\alpha_2 \neq \alpha_5$ y $\alpha_3 \neq \alpha_4$. De nuevo podemos apelar a la simetría y suponer que $\alpha_2 = 1$ y por tanto $\alpha_5 = 0$. Si $\alpha_3 = 1$ entonces $T \cap B_4' = \langle t_{12}t_{34}, t_{12}t_{13}t_{14}\rangle$. Cambiando x_2 por $x_2x_3x_4$ obtenemos que $t_{12} \in T$, una contradicción. Si $\alpha_3 = 0$ entonces $T \cap B_4' = \langle t_{12}t_{34}, t_{12}t_{13}t_{23}\rangle$. Cambiando x_1 por $x_1x_2x_4$ obtenemos que $t_{13} \in T$, de nuevo una contradicción.

Por lo tanto $r(T \cap B_4') \geq 3$, de donde deducimos que $r(G') \leq 3$. Además por el Lema 4.6.8 tenemos que $r(G') \neq 1$, luego $2 \leq r(G') \leq 3$ y sólo nos falta demostrar que $r(G') \neq 2$.

Supongamos que $r(G') = 2$. Veamos que existen $x_1, x_2, x_3 \in G$ tales que t_{12} y t_{13} son linealmente independientes y por tanto $G' = \langle t_{12}, t_{13}\rangle$. Esto es equivalente a demostrar que $G' = \langle t_{ax}, t_{ay}\rangle$ para ciertos $a, x, y \in \{1, 2, 3, 4\}$. Podemos suponer que $t_{12} \neq 1$. Sea $H = \langle t_{12}, t_{13}, t_{14}, t_{23}, t_{24}\rangle$. Si $r(H) = 2$ podemos suponer que t_{12} y t_{13} son linealmente independientes. En caso contrario tenemos que $H = \langle t_{12}\rangle$ y al ser $r(G') = 2$ deducimos que $G' = \langle t_{12}, t_{34}\rangle$. Pero por el Lema 4.6.9 existe $1 \leq i \leq 2 < j \leq 4$ tal que $t_{ij} \neq 1$ y $t_{ij} = t_{12}$, luego $G' = \langle t_{ij}, t_{34}\rangle$ tal y como queríamos demostrar. Luego podemos suponer que $G' = \langle t_{12}, t_{13}\rangle$ y considerando 4 casos podemos suponer que $t_{23} = 1$, por ejemplo, si $t_{23} = t_{12}t_{13}$ reemplazando x_1, x_2, x_3 por x_1, x_1x_2, x_2x_3 obtenemos que $t_{23} = 1$. Las imágenes de x_1, x_2, x_3 en $G/Z(G)$ son linealmente independientes y podemos obtener una base de $G/Z(G)$ añadiendo la imagen de un $x_4 \in G$.

Pongamos $t_{i4} = t_{12}^{\alpha_i}t_{13}^{\beta_i}$ para $i = 1, 2, 3$. Sea $H = G/\langle t_{12}\rangle$ entonces $H' = t_{13} \cong C_2$ y la matriz asociada es (véase el párrafo anterior al Lema 4.6.9)

$$\begin{pmatrix} 0 & 0 & 1 & \beta_1 \\ 0 & 0 & 0 & \beta_2 \\ 1 & 0 & 0 & \beta_3 \\ \beta_1 & \beta_2 & \beta_3 & 0 \end{pmatrix}.$$

Como el rango de esta matriz ha de ser 2, $\beta_2 = 0$. Un argumento similar con $H = G/\langle t_{13}\rangle$ nos lleva a la matriz

$$\begin{pmatrix} 0 & 1 & 0 & \alpha_1 \\ 1 & 0 & 0 & \alpha_2 \\ 0 & 0 & 0 & \alpha_3 \\ \alpha_1 & \alpha_2 & \alpha_3 & 0 \end{pmatrix}$$

de donde deducimos que $\alpha_3 = 0$. Considerando ahora $H = G/\langle t_{12}t_{13}\rangle$ que nos lleva a la matriz

$$\begin{pmatrix} 0 & 1 & 1 & \alpha_1 + \beta_1 \\ 1 & 0 & 0 & \alpha_2 \\ 1 & 0 & 0 & \beta_3 \\ \alpha_1 + \beta_1 & \alpha_2 & \beta_3 & 0 \end{pmatrix}$$

y por tanto $\alpha_2 = \beta_3$. En resumen

$$t_{14} = t_{12}^{\alpha_1} t_{13}^{\beta_1}, \quad t_{24} = t_{12}^{\alpha_2}, \quad t_{34} = t_{13}^{\alpha_2}$$

Cambiando x_4 por $x_1^{\alpha_2} x_4$ podemos suponer que $\alpha_2 = 0$. Entonces $x_2^{\alpha_1} x_3^{\beta_1} x_4$ es central, una contradicción. En conclusión $r(G') = 3$ tal y como queríamos demostrar. □

Lema 4.6.11 *Si $G \in \mathcal{G}$ y $r(G/Z(G)) = 4$ entonces existen $x_1, x_2, x_3, x_4 \in G$ tales que $G = \langle x_1, x_2, x_3, x_4, Z(G)\rangle$ y $t_{23} = t_{24} = t_{34} = 1$ con lo que $G' = \langle t_{12}, t_{13}, t_{14}\rangle \cong C_2^3$.*

Demostración. Empezamos demostrando que existen $x_1, x_2, x_3, x_4 \in G$ tales que $G = \langle x_1, x_2, x_3, x_4, Z(G)\rangle$ y $G' = \langle t_{12}, t_{13}, t_{14}\rangle$. Sean $x_1, x_2, x_3, x_4 \in G$ tales que sus imágenes en $G/Z(G)$ forman una base de $G/Z(G)$. Por reducción al absurdo supongamos que para toda permutación $axyz$ de $\{1,2,3,4\}$ t_{ax}, t_{ay}, t_{az} son linealmente dependientes. Como $r(G') = 3$ puedo suponer que t_{12} y t_{13} son linealmente independientes.

Supongamos que $G' = \langle t_{12}, t_{13}, t_{23}\rangle$. Como t_{ax}, t_{ay}, t_{az} son linealmente dependientes para toda permutación $axyz$ de $\{1,2,3,4\}$, necesariamente

$$t_{14} \in \langle t_{12}, t_{13}\rangle, \quad t_{24} \in \langle t_{12}, t_{23}\rangle, \quad t_{34} \in \langle t_{13}, t_{23}\rangle.$$

Si $t_{14} = t_{12}^a t_{13}^b$, cambiando x_4 por $x_2^a x_3^b x_4$ podemos suponer que $t_{14} = 1$. Pongamos

$$t_{24} = t_{12}^{\alpha_1} t_{23}^{\alpha_3} \quad \text{y} \quad t_{34} = t_{13}^{\beta_1} t_{23}^{\beta_2}.$$

Razonando como en el lema anterior con los cocientes $G/\langle t_{12}, t_{13}t_{23}\rangle$, $G/\langle t_{13}, t_{12}t_{23}\rangle$ y $G/\langle t_{23}, t_{12}t_{13}\rangle$ obtenemos que las siguientes tres matrices han de tener rango 2:

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & \alpha_3 \\ 1 & 1 & 0 & \beta_1+\beta_2 \\ 0 & \alpha_3 & \beta_1+\beta_2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & \alpha_1+\alpha_3 \\ 0 & 1 & 0 & \beta_2 \\ 0 & \alpha_1+\alpha_3 & \beta_2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & \alpha_1 \\ 1 & 0 & 0 & \beta_1 \\ 0 & \alpha_1 & \beta_1 & 0 \end{pmatrix}.$$

Deducimos que $\alpha_3 = \beta_2 = 0$ y $\alpha_1 = \beta_1$ y por tanto $x_1^{\alpha_1} x_4$ es central, una contradicción.

Por lo tanto hemos demostrado que $G' \neq \langle t_{12}, t_{13}, t_{23}\rangle$. Luego sólo tenemos dos posibilidades para G': $G' = \langle t_{12}, t_{13}, t_{24}\rangle$ ó $G' = \langle t_{12}, t_{13}, t_{34}\rangle$. Como x_2 y x_3 representan papeles simétricos podemos suponer que $G' = \langle t_{12}, t_{13}, t_{24}\rangle$. Además como estamos suponiendo que t_{ax}, t_{ay}, t_{az} son linealmente dependientes para toda permutación $axyz$ de $\{1,2,3,4\}$ tenemos que $t_{23} \in \langle t_{12}, t_{13}\rangle \cap \langle t_{12}, t_{24}\rangle = \langle t_{12}\rangle$. Podemos suponer que $t_{23} = 1$ haciendo el cambio x_3 por $x_1 x_3$ si fuese necesario. Además $t_{14} \in \langle t_{12}, t_{13}\rangle$, luego $t_{14} = t_{12}^a t_{13}^b$ y haciendo el cambio x_4 por $x_2^a x_3^b x_4$ obtenemos que $t_{14} = 1$.

Pongamos $t_{34} = t_{12}^a t_{13}^b t_{24}^c$. Consideramos ahora los siguientes cocientes $G/\langle t_{13}, t_{24}\rangle$, $G/\langle t_{12}t_{13}, t_{24}\rangle$ y $G/\langle t_{12}, t_{13}t_{24}\rangle$ de los que obtenemos las siguientes tres matrices:

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & a \\ 0 & 0 & a & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & a+b \\ 0 & 0 & a+b & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & b+c \\ 0 & 1 & b+c & 0 \end{pmatrix}.$$

Forzando a que estas matrices tengan rango 2 llegamos a la conclusión de que $a = b = c = 0$, o sea $t_{34} = 1$. Consideramos ahora el cociente $G/\langle t_{12}t_{13}, t_{12}t_{24}\rangle$ obtenemos la matriz

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

que tiene rango 4, una contradicción.

Por lo tanto hemos demostrado que podemos suponer $G' = \langle t_{12}, t_{13}, t_{14}\rangle$. Veamos ahora que también podemos suponer que $t_{23} = t_{24} = t_{34} = 1$.

Si $t_{23} \notin \langle t_{12}, t_{13}\rangle$ considerando $G/\langle t_{12}, t_{13}\rangle$ obtenemos una matriz de la forma

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & * \\ 0 & 1 & 0 & * \\ 1 & * & * & 0 \end{pmatrix}$$

que tiene rango 4. Por tanto $t_{23} \in \langle t_{12}, t_{13}\rangle$ y por argumentos similares tenemos que $t_{24} \in \langle t_{12}, t_{14}\rangle$ y $t_{34} \in \langle t_{13}, t_{14}\rangle$. Si $t_{23} = t_{12}^a t_{13}^b$, cambiando x_2 y x_3 por $x_1^b x_2$ y $x_1^a x_3$ respectivamente podemos suponer que $t_{23} = 1$. Pongamos

$$t_{24} = t_{12}^{a_1} t_{14}^{c_1}$$
$$t_{34} = t_{13}^{b_2} t_{14}^{c_2}$$

con $a_i, b_i, c_i \in \{0, 1\}$. Cambiando x_4 por $x_1^{a_1} x_4$ podemos suponer que $a_1 = 0$. Considerando los siguientes cocientes $G/\langle t_{12}t_{14}, t_{13}\rangle$, $G/\langle t_{12}, t_{13}t_{14}\rangle$ y $G/\langle t_{12}t_{13}, t_{14}\rangle$ obtenemos las siguientes tres matrices:

$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & c_1 \\ 0 & 0 & 0 & c_2 \\ 1 & c_1 & c_2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & c_1 \\ 1 & 0 & 0 & b_2+c_2 \\ 1 & c_1 & b_2+c_2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & b_2 \\ 0 & 0 & b_2 & 0 \end{pmatrix}.$$

de donde se deduce que $c_2 = c_1 = b_2 = 0$, es decir, $t_{24} = t_{34} = 1$ lo que faltaba por demostrar. □

En realidad el último lema se puede generalizar a grupos de rango mayor o igual que 4. Para el paso inductivo en la demostración de este hecho necesitamos el siguiente lema.

Lema 4.6.12 *Sea $G \in \mathcal{G}$ tal que $r(G/Z(G)) = n \geq 3$. Entonces existe un subgrupo H de G tal que $r(H/Z(H)) = r(G/Z(G)) - 1$.*

Demostración. Haremos la demostración por inducción en n. El resultado es trivial para $n = 3$, basta elegir $H = \langle x, y \rangle$ donde x e y son dos elementos de G que no conmutan.

Supongamos ahora que $n \geq 4$ y que el resultado es cierto para todo $S \in \mathcal{G}$ con $3 \leq r(S/Z(S)) < n$. Sea H un subgrupo de G maximal para la condición:

$$r(H/Z(H)) = \max\{r(K/Z(K)) | K \text{ subgrupo de G}, Z(G) \subseteq K, r(K/Z(K)) \neq n\}$$

Claramente $Z(G) \subseteq H$ y $2 \leq r(H/Z(H)) < n$. Sea $\{x_1 Z(G), x_2 Z(G), \ldots, x_k Z(G)\}$ una base de $H/Z(G)$ que extendemos a una base $\{x_1 Z(G), x_2 Z(G), \ldots, x_n Z(G)\}$ de $G/Z(G)$. Demostraremos que se verifica la condición buscada, es decir, $k = n - 1$.

Por reducción al absurdo supongamos que $k \leq n - 2$. Si $k < i \leq n$ y $K_i = \langle H, x_i \rangle$ entonces $k \leq r(K_i/Z(K_i)) \leq k + 1 < n$. La maximalidad de H implica que $r(K_i/Z(K_i)) = k$. Por lo tanto existe un $h_i \in H$ tal que $y_i = h_i x_i \in Z(K_i)$. Luego $G = \langle x_1, \ldots, x_k, y_{k+1}, \ldots, y_n, Z(G) \rangle$ y $[x_i, y_j] = 1$ para $1 \leq i \leq k \leq n$. Podemos suponer que $[x_1, x_2] \neq 1 \neq [y_{k+1}, y_{k+2}]$. Consideremos ahora el subgrupo $M = \langle x_1, x_2, y_{k+1}, y_{k+2} \rangle$ de G. Por el Lema 4.6.2, M es de tipo kleiniano, lo que contradice el Lema 4.6.8. Luego $k = n - 1$ □

Podemos ya pasar a generalizar el Lema 4.6.11

Lema 4.6.13 *Sea $G \in \mathcal{G}$ tal $r(G/Z(G)) = n \geq 4$. Entonces $r(G') = n - 1$ y existen $x_1, x_2, \ldots, x_n \in G$ tales que $G = \langle x_1, x_2, \ldots, x_n, Z(G) \rangle$, $G' = \langle t_{12}, t_{13}, \ldots, t_{1n} \rangle$ y $t_{ij} = 1$ para $2 \leq i < j \leq n$.*

Demostración. Procedemos por inducción en n. Para $n = 4$ es el Lema 4.6.10.

Supongamos ahora que $n > 4$ y que el resultado se verifica para todo grupo $H \in \mathcal{G}$ con $4 \leq r(H/Z(H)) < n$. Por el Lema 4.6.12, G tiene un subgrupo H tal que $r(H/Z(H)) = n - 1$. Por la hipótesis de inducción existen elementos $x_1, x_2, \ldots, x_{n-1}$ tales que $H = \langle x_1, x_2, \ldots, x_{n-1}, Z(H) \rangle$, $t_{ij} = 1$ para todo $2 \leq i \leq n - 1$ y $t_{12}, \ldots, t_{1(n-1)}$ son linealmente independientes. En particular $r(G') \geq n - 2$. Entonces existe un $x_n \in G$ tal que $G = \langle x_1, x_2, \ldots, x_n, Z(G) \rangle$.

Veamos primero que $r(G') \neq n - 2$. Supongamos lo contrario, es decir $r(G') = n - 2$. Entonces $G' = \langle t_{12}, \ldots, t_{1(n-1)} \rangle$, luego $t_{1n} = t_{12}^{a_2} \ldots t_{1(n-1)}^{a_{n-1}}$. Entonces haciendo el cambio x_n por $x_2^{a_2} \ldots x_{n-1}^{a_{n-1}} x_n$ podemos suponer que $t_{1n} = 1$.

Ahora aseguramos que $t_{in} \in \langle t_{1i} \rangle$ para todo $1 < i < n$. Si no es cierto consideramos el cociente $S = G/\langle t_{1i} \rangle$. Vamos a probar que $r(S/Z(S)) = n$. Para simplificar supondremos que $i = 2$ y aumentaremos el abuso de notación denotando por x_i y t_{ij} a las imágenes de x_i y t_{ij} en S. Obsérvese que $t_{12} = 1$, que

$t_{13}, \ldots, t_{1(n-1)}$ son linealmente independientes y que $t_{2n} \neq 1$ en S. Supongamos que $y = x_1^{a_1} \ldots x_n^{a_n} \in Z(S)$ con $a_i \in \{0,1\}$. Entonces $1 = [x_2, y] = t_{2n}^{a_n}$ y por lo tanto $a_n = 0$. Además $1 = [x_1, y] = t_{13}^{a_3} \ldots t_{1(n-1)}^{a_{n-1}}$ y como $t_{13}, \ldots, t_{1(n-1)}$ son linealmente independientes tenemos que $a_3 = \cdots = a_{n-1} = 0$. Finalmente $1 = [x_3, y] = t_{13}^{a_1}$, luego $a_1 = 0$. Esto prueba que $x_1 Z(S), \ldots, x_n Z(S)$ son linealmente independientes y por lo tanto $r(S/Z(S)) = n$. Por el Lema 4.6.12 existe un subgrupo K de S tal que $r(K/Z(K)) = n-1$ y $r(K') = n-2$ lo que contradice que el hecho de que $r(S') = n-3$. Por lo tanto $t_{1n} = 1$ y $t_{in} \in \langle t_{1i} \rangle$ para todo $1 < i < n$.

Obsérvese que como x_n no es central existe un $2 \leq i < n$ tal que $t_{in} \neq 1$. Además como $x_1 x_n$ no es central existe algún $2 \leq i < n$ tal que $t_{in} \neq t_{1i}$ y por tanto $t_{in} = 1$. Reorganizando los x_i, si fuese necesario, podemos suponer que $t_{3n} = t_{13}$ y que $t_{2n} = 1$. Consideremos ahora el cociente $S = G/\langle t_{12} t_{13} \rangle$. Para este cociente tenemos que $r(S') = n-3$ y que $t_{12} = t_{13} = t_{3n} \neq 1$. Por un argumento similar al anterior llegaremos a contradicción demostrando que $r(S/Z(S)) = n$. En efecto sea $y = x_1^{a_1} \ldots x_n^{a_n} \in Z(S)$ con $a_i \in \{0,1\}$, entonces $1 = [x_2, y] = t_{12}^{a_1}$, luego $a_1 = 0$. Además $1 = [x_3, y] = t_{3n}^{a_n}$, luego $a_n = 0$. Más aún $1 = [x_1, y] = t_{13}^{a_2 + a_3} t_{14}^{a_4} \ldots t_{1(n-1)}^{a_{n-1}}$ y como $t_{13}, \ldots, t_{1(n-1)}$ son linealmente independientes tenemos que $a_4 = \cdots = a_{n-1} = 0$ y $a_2 = a_3$. Finalmente $1 = [x_n, y] = t_{3n}^{a_3}$, luego $0 = a_3 = a_2$. Por lo tanto hemos probado que $r(G') \geq n-1$. Veamos ahora que efectivamente $r(G') = n-1$. Tenemos dos casos que considerar: (Recordamos que $t_{ij} = 1$ para $2 \leq i < j \leq n-1$).

1. Si $t_{1n} \in \langle t_{12}, \ldots, t_{1(n-1)} \rangle$, entonces existe $1 < i < n$ tal que $t_{12}, \ldots, t_{1(n-1)}, t_{in}$ son linealmente independientes. Sea $1 < j < n$ con $j \neq i$. Por el caso $n = 4$ tenemos que $r(\langle x_1, x_i, x_j, x_n \rangle') \leq 3$ y, por lo tanto, $t_{1n}, t_{jn} \in \langle t_{1i}, t_{1j}, t_{in} \rangle$, luego $G' = \langle t_{12}, \ldots, t_{1(n-1)}, t_{in} \rangle$ y así $r(G') = n-1$.

2. Si $t_{1n} \notin \langle t_{12}, \ldots, t_{1(n-1)} \rangle$ tenemos que $t_{12}, \ldots, t_{1(n-1)}, t_{1n}$ son linealmente independientes. Sean $1 < i, j < n$ con $i \neq j$. Por el caso $n = 4$ tenemos que $r(\langle x_1, x_i, x_j, x_n \rangle') \leq 3$ y por lo tanto $t_{in} \in \langle t_{1i}, t_{1j}, t_{1n} \rangle$, luego $G' = \langle t_{12}, \ldots, t_{1(n-1)}, t_{in} \rangle$ y así $r(G') = n-1$.

Falta por demostrar que podemos suponer que $t_{in} = 1$ para todo $1 < i < n$. En efecto, sea $1 < i < n$. Vamos a probar que $t_{in} \in \langle t_{1i} \rangle$. Para simplificar supondremos que $i = 2$. Si $t_{2n} \notin \langle t_{12} \rangle$ sea $S = G/\langle t_{12} \rangle$. Claramente $r(S') = n-2$ y demostrando que $r(S/Z(S)) = n$ obtendremos una contradicción. Sea $y = x_1^{a_1} \ldots x_n^{a_n} \in Z(S)$ con $a_i \in \{0,1\}$, entonces $1 = [x_2, y] = t_{12}^{a_n}$, luego $a_n = 0$. También $1 = [x_3, y] = t_{13}^{a_1}$, luego $a_1 = 0$. Además $1 = [x_1, y] = t_{13}^{a_3} \ldots t_{1(n-1)}^{a_{n-1}}$ luego $a_3 = \cdots = a_{n-1} = 0$. Finalmente $1 = [x_n, y] = t_{2n}^{a_2}$ luego $a_2 = 0$.En conclusión $t_{in} \in \langle t_{1i} \rangle$ para todo $1 < i < n$.

Ahora considerando el cociente $S = G/\langle t_{1i} t_{1j} \rangle$ para $1 < i < j < n$ y argumentando como antes podemos excluir la posibilidad $t_{in} = 1$ y $t_{1j} = t_{nj}$, viendo que si se pudiera dar esta posibilidad entonces $r(S/Z(S)) = n$ y $r(S') = n-2$ llegando a contradicción.

Por lo tanto podemos deducir que o bien $t_{in} = 1$ para todo $1 < i < n$ o bien $t_{in} = t_{1i}$ para todo $1 < i < n$. Ahora bien el segundo caso se reduce al primero

mediante el cambio x_1 por x_1x_n. Por lo tanto el Lema queda demostrado. □

Ya tenemos todas las herramientas necesarias para demostrar el teorema principal de este capítulo.

Teorema 4.6.14 *Sea G un 2-grupo finito nilpotente tal que $G' \subseteq Z(G)$. Entonces G es de tipo kleiniano si y sólo si es isomorfo a un cociente de $H \times C_4^m$ donde $m \geq 0$ y $H = B_2, A_{31}, A_{32}, B_{n1}$ ó B_{n2} con $n \geq 3$ siendo*

$$
\begin{aligned}
B_2 = \quad & \langle x_1, x_2 | x_i^8 = [x_i, x_j^4] = [x_i, [x_j, x_k]] = 1, i, j, k = 1, 2 \rangle \\
A_{31} = \quad & \langle x_1, x_2, x_3 | x_i^4 = [x_i, x_j^2] = [x_i, [x_j, x_k]] = 1, 1 \leq i, j, k \leq 3 \rangle \\
A_{32} = \quad & \langle x_1, x_2, x_3 | x_1^4 = x_2^4 [x_1, x_2] = x_3^4 [x_1, x_3] = [x_i, x_j^2] = 1, 1 \leq i, j, k \leq 3 \rangle \\
B_{n1} = \quad & \langle x_1, x_2, \ldots, x_n | x_1^8 = x_k^4 = [x_i, x_j^2] = [x_k, x_l] = [x_i, [x_1, x_k]] = 1, 1 \leq i, j \leq n, \\
& 2 \leq k, l \leq n \rangle \\
B_{n2} = \quad & \langle x_1, x_2, \ldots, x_n | x_1^8 = x_k^4 [x_1, x_k] = [x_i, x_j^2] = [x_k, x_l] = [x_i, [x_1, x_k]] = 1, \\
& 1 \leq i, j \leq n, 2 \leq k, l \leq n \rangle
\end{aligned}
$$

Demostración. Empezaremos demostrando que si G es un cociente de $H \times C_4^m$ con $m \geq 0$ y $H = B_2, A_{31}, A_{32}, B_{n1}$ ó B_{n2} con $n \geq 3$ entonces $G \in \mathcal{G}$. Para ver esto observemos que si $G \in \mathcal{G}$, entonces $G \times C_4 \in \mathcal{G}$ ya que los cocientes simples no conmutativos de $\mathbb{Q}G$ son de la forma $\mathbb{H}(\mathbb{Q}), M_2(\mathbb{Q})$ y $M_2(\mathbb{Q}(i))$, con lo que los de $\mathbb{Q}(G \times C_4)$ son de la forma $\mathbb{H}(\mathbb{Q}), M_2(\mathbb{Q}), M_2(\mathbb{Q}(i)), \mathbb{H}(\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}(i) \cong M_2(\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}(i) \cong M_2(\mathbb{Q}(i))$ o un cociente de $M_2(\mathbb{Q}(i)) \otimes_{\mathbb{Q}} \mathbb{Q}(i) \cong 2M_2(\mathbb{Q}(i))$ en definitiva $M_2(\mathbb{Q}(i))$ de nuevo. Utilizando el Lema 4.6.2, tenemos que basta demostrar que los grupos $B_2, A_{31}, A_{32}, B_{n1}$ y B_{n2} con $n \geq 3$ están todos en $\mathcal{G}$. Ya vimos en la Proposición 4.6.4 que $B_2 \in \mathcal{G}$. Para demostrar que los otros grupos están en $\mathcal{G}$ consideremos el conjunto $\mathcal{H}$ de subgrupos maximales de G' donde $G = A_{31}, A_{32}, B_{n1}$ ó B_{n2} con $n \geq 3$. Entonces el conjunto $\{\widehat{S}(1 - \widehat{G'}) | S \in \mathcal{H}\}$ es un conjunto completo de idempotentes centrales ortogonales de $\mathbb{Q}G(1 - \widehat{G'})$. Como todos los cocientes simples no conmutativos de $\mathbb{Q}G$ son cocientes simples de $\mathbb{Q}G(1 - \widehat{G'})$, cada cociente simple de $\mathbb{Q}G$ es un cociente simple de $\mathbb{Q}G\widehat{S}(1 - \widehat{G'})$ para algún $S \in \mathcal{H}$, que a su vez es un cociente simple de $\mathbb{Q}G\widehat{S}$ y éste es isomorfo a $\mathbb{Q}(G/S)$ (véase la Sección 1.4). Lo que vamos a ver es que G/S es isomorfo a un cociente de $B_2 \times C_4^k$ para algún k, con lo que tendremos demostrado que las componentes simples de $\mathbb{Q}G$ son como queremos ya que $B_2 \times C_4^k \in \mathcal{G}$.

Supongamos primero que $G = A_{31}$ ó A_{32}. En este caso tenemos que los elementos

de $\mathcal{H}$ son los siete siguientes:

$$\begin{aligned} S_1 &= \langle t_{12}, t_{13} \rangle \\ S_2 &= \langle t_{12}, t_{23} \rangle \\ S_3 &= \langle t_{13}, t_{23} \rangle \\ S_4 &= \langle t_{12}t_{13}, t_{23} \rangle \\ S_5 &= \langle t_{12}t_{23}, t_{13} \rangle \\ S_6 &= \langle t_{13}t_{23}, t_{12} \rangle \\ S_7 &= \langle t_{12}t_{13}, t_{13}t_{23} \rangle \end{aligned} \tag{4.3}$$

Para cada uno de los S_i, $Z(G/S_i)$ contiene propiamente a $Z(G)/S_i$ con lo que $r(G/S_i/Z(G/S_i)) = 2$. Sean $x, y \in G/S_i$ dos elementos linealmente independientes módulo $Z(G)$. Entonces $G/S_i = \langle x, y \rangle \times C_4$ donde $\langle x, y \rangle$ es isomorfo a un cociente de B_2 y por lo tanto G/S_i es un cociente de $B_2 \times C_4$ tal y como queríamos demostrar.

Supongamos ahora que $G = B_{n1}$ ó B_{n2}.

Consideremos ahora la aplicación $\varphi : G' \to G$ dada por $\varphi(t_{12}^{a_2} \cdot \cdots \cdot t_{1n}^{a_n}) = x_2^{a_2} \cdot \cdots \cdot x_n^{a_n}$ para cada $(a_2, \ldots, a_n) \in \{0,1\}^{n-1}$. Obsérvese que $[x_1, \varphi(x)] = x$ para cada $x \in G'$. Sea $\{c_3, \ldots, c_n\}$ una base de S y $\{c_2c_3, \ldots, c_n\}$ una base de G'. Sea $y_i = \varphi(c_i)$. Entonces $\{x_1Z(G), y_2Z(G), \ldots, y_nZ(G)\}$ es una base de $G/Z(G)$ con lo que $G = \langle x_1, y_2, \ldots, y_n \rangle$. Cambiando de variable podemos suponer que $y_i = x_i$, es decir, $[x - i, x_i] \in S$ para $i \geq 3$ y $[x_1, x_2] \in G' \setminus S$. Por tanto

$$G/S \cong \langle x_1, x_2 \rangle \times \langle x_3, \ldots, x_n \rangle \cong \langle x_1, x_2 \rangle \times C_4^{n-2}$$

y $\langle x_1, x_2 \rangle$ es isomorfo a un cociente de B_2, lo que demuestra lo que queríamos.

Recíprocamente, sea $G \in \mathcal{G}$ no abeliano y sea $n = r(G/Z(G))$. Sean $x_1, x_2, \ldots, x_n$ elementos de G tales que $\{x_1Z(G), x_2Z(G), \ldots, x_nZ(G)\}$ es una base de $G/Z(G)$. Sea $Z(G) = \langle z_1 \rangle \times \cdots \times \langle z_m \rangle$ y con z_i de orden k_i. Si $H = \langle x_1, x_2, \ldots, x_n \rangle$ entonces H tiene una presentación de la forma $\langle x_1, x_2, \ldots, x_n | R \rangle$ para cierto conjunto de relaciones R. Además

$$Z(G) = \langle z_1, \ldots, z_m | z_i^{k_i} = [z_i, z_j] = 1, 1 \leq i, j \leq m \rangle$$

es una presentación de $Z(G)$. Entonces G tiene una presentación de la forma

$$\langle x_1, \ldots, x_n, z_1, \ldots, z_m | R, z_i^{k_i} = [z_i, z_j] = [z_i, x_k] = 1, h = z$$

$$\text{para todo } h \in H, z \in Z(G) \text{ tales que } h = z \text{ en } G \rangle$$

Por el Lema 4.6.3, k_i divide a 4 para cada $i = 1, 2, \ldots, m$ y por tanto G es isomorfo a un cociente de

$$\langle x_1, \ldots, x_n, z_1, \ldots, z_m | R, z_i^{k_i} = [z_i, z_j] = [z_i, x_k] = 1 \rangle = H \times C_4^m.$$

Como $r(H) = R(H/Z(H)) = n$, hemos demostrado que podemos suponer sin pérdida de generalidad que $n = r(G) = r(G/Z(G))$.

Como G no es abeliano, $n \geq 2$. Si $n = 2$, entonces G es un cociente de B_2. Si $n = 3$ entonces del Lema 4.6.6 deducimos que G es un cociente de $B_2 \times C_4, A_{31}, A_{32}, B_{31}$ ó B_{32}. Sin embargo de la hipótesis $r(G/Z(G)) = 3$ se deduce que el primer caso no se da. Finalmente supongamos que $n \geq 4$. Del Lema 4.6.13 tenemos que $r(G') = n - 1$ y podemos elegir los x_i's de forma que $G' = \langle t_{12}, \ldots, t_{1n} \rangle$ y $t_{ij} = 1$ para $2 \leq i, j \leq n$. Las relaciones $x_i^8 = [x_i, x_j^2] = [x_i, t_{ij}] = 1$ se deducen del Lema 4.6.3. Por el Lema 4.6.5 tenemos que $x_i^4 \in \langle t_{1i} \rangle$ para todo $2 \leq i \leq n$. Sólo falta ver que o bien $x_i^4 = 1$ para todo $2 \leq i \leq n$ o bien $x_i^4 = t_{1i}$ para todo $2 \leq i \leq n$. En caso contrario, podemos reordenar los x_i's y suponer que $x_2^4 = 1$ y $x_3^4 = t_{13}$. Pero en tal caso $(x_2 x_3)^4 = t_{13} \notin \langle [x_1, x_2 x_3] \rangle$ lo que contradice el Lema 4.6.5. $\square$

Bibliografía

[1] A. Bak y U. Rehmann, The congruence subgroup and metaplectic problems for $\mathrm{SL}_{n\geq 2}$ of division algebras, *J. Algebra* **78** (1982), 475–547.

[2] J. Bamberg, Non-free points for groups generated by a pair of 2×2 matrices, *J. London Math. Soc.* **62** (2) (2000), 795–801.

[3] B. Banieqbal, Classification of finite subgroups of 2×2 matrices over a division algebra of characteristic zero, *J. Algebra* **119** (1988), 449–512.

[4] H. Bass, The Dirichlet Unit Theorem, induced characters and Whitehead group, *Topology* **4** (1966), 391–410.

[5] H. Bass, J. Milnor y J.P. Serre, Solution of the congruence problem for SL_n ($n \geq 3$), and SP_{2n}, *Publ. Math. IHES* **33** (1967), 59–137.

[6] A. F. Beardon, *The Geometry of Discrete Groups*. Springer 1983.

[7] L. Bianchi, Sui gruppi de sostituzioni lineari con coeficienti appartenente a corpi quadratici imaginari, *Math. Ann.* **40** (1892), 332–412.

[8] A. A. Borel y Harish-Chandra, Arithmetic Subgroups of algebraic groups, *Ann. Math.* **75** (1962), 485–535.

[9] B. Chang, S. A. Jennings y R. Ree, On certains pairs of matrices which generate free groups, *Canad. J. Math.* **10** (1958), 279–284.

[10] D.B. Coleman, Finite groups with isomorphic group algebras, *Trans. Amer. Math. Soc.* **105** (1962), 1–8.

[11] Ch. W. Curtis y I. Reiner, *Methods of Representation Theory*, Wiley, New York, 1981.

[12] A. Dooms y E. Jespers, Normal complements of the trivial units in the unit group of some integral group rings, *Preprint*.

[13] M. Eichler, Über die Einheiten der Divisionsalgebren, *Math. Ann.* **114** (1937), 635–654.

[14] J. Elstrodt, F. Grunewald y J. Mennicke, *Groups Acting on Hyperbolic Space. Harmonic Annalysis and Number Theory*, Springer, 1998.

[15] B. Fine, *The Algebraic structure of the Bianchi Groups*, Marcel Dekker, 1989.

[16] R. Gow y B. Huppert, Degree problems of representation theory over arbitrary fields of characteristic 0. On Theorems of N. Itô and J.G. Thompson, *J. Reine Angew. Math.* **381** (1987), 136–147.

[17] R. Gow y B. Huppert, Degree problems of representation theory over arbitrary fields of characteristic 0, Part 2: Groups which have only two reduced degree, *J. Reine Angew. Math.* **389** (1988), 122–132.

[18] B. Hartley y P.F. Pickel, Free subgroups in the unit group of integral group rings, *Canad. J. Math.* **32** (1980), 1342–1352.

[19] K. Hey, *Analytische Zahlentheorie in Systemen hyperkomplexer Zahlen*, Tesis Doctoral, Hamburgo, 1929.

[20] G. Higman, *Units in group rings*, D. Phil. Thesis, University of Oxford, Oxford, 1940.

[21] G. Higman, The units of group rings, *Proc. London Math. Soc.* **46** (1940), 231–248.

[22] J. A. Ignatov, Free groups generated by two parabolic-fractional linear transformations, *Modern Algebra* **4** (1976), 87–90.

[23] J. A. Ignatov, Free and nonfree subgroups of $\mathrm{PSL}_2(\mathbb{C})$ that are generated by two parabolic elements, *Math. USSR Sbornik.* **35** (1979), 49–55.

[24] E. Jespers, Free normal complements and the unit group in integral group rings, *Proc. Amer. Math. Soc.* **122** (1) (1994), 59–66.

[25] E. Jespers, Units in integral group rings: a survey, *Lect. Notes Pure Appl. Math.* **198** (1998), 141–169.

[26] E. Jespers, On some problems of units in integral group rings, *Preprint.*

[27] E. Jespers y G. Leal, Describing units in integral group rings of some 2-groups, *Comm. Algebra* **19** (1991), 1809–1827.

[28] E. Jespers y G. Leal, Generators of large subgroups of the unit group of integral group rings, *Manuscripta Math.* **78** (1993), 303–315.

[29] E. Jespers y G. Leal, Degree 1 and 2 representations of nilpotent groups and applications to units of group rings, *Manuscripta Math.* **86** (1995), 479–498.

[30] E. Jespers y G. Leal, Free products of abelian groups in the unit group of integral group rings, *Proc. Amer. Math. Soc.* **1** (26) (1998), 1257–1265.

[31] E. Jespers, G. Leal y C. Polcino Milies, Units of integral group rings of some metacyclic groups, *Can. Math. Bull.* **37** (2) (1994), 228–237.

[32] E. Jespers, G. Leal y Á. del Río, Products of free groups in the unit group of integral group rings, *J. Algebra* **180** (1996), 22–40.

[33] E. Jespers y M.M. Parmenter, Bicyclic units in $\mathbb{Z}S_3$, *Bull. Belg. Math. Soc.* **44** (1992), 141–146.

[34] E. Jespers y M.M. Parmenter, Units of group rings of groups of order 16, *Glasgow Math. J.* **35** (1993), 367–379.

[35] E. Jespers y Á. del Río, A structure theorem for the unit group of the integral group ring of some finite groups, *J. Reine Angew. Math.* **521** (2000), 99–117.

[36] E. Jespers, Á. del Río y M. Ruiz, Groups generated by two bicyclic units in integral group rings, *J. Group Theory* **5** (4) (2002), 493–511.

[37] M. I. Kargapolov y J. I. Merzljakov, *Fundamental of the theory of groups*, Springer Verlag, New York, 1979.

[38] G. Karpilovsky, *Units in Group Rings*, Longman, Essex, 1989.

[39] E. Kleinert, Units of classical orders: a survey, *L'Enseignement Mathématique* **40** (1994), 205–248.

[40] E. Kleinert, *Units in Skew Fields*, Birkhäuser Verlag, Basilea 2000.

[41] G. Leal y C. Polcino Milies, Isomorphic groups (and loop) algebras, *J. Algebra* **155** (1993), 195–210.

[42] G. Leal y Á. del Río, Products of free groups in the unit group of integral group rings II, *J. Algebra* **191** (1997), 240–251.

[43] R.C. Lyndon, P.E. Schupp, *Combinatorial Group Theory*, Springer-Verlag, Berlin 1977.

[44] R.C. Lyndon y J. L. Ullman. Groups generated by two parabolic linear fractional transformations, *Canad. J. Math.* **21** (1969), 1388–1403.

[45] W. Magnus, A. Karras y D. Solitar, *Combinatorial Group Theory*, J. Wiley and Sons, New York 1966.

[46] Z.S. Marciniak y S.K. Sehgal, Constructing free subgroups of integral group rings, *Proc. Amer. Math. Soc.* **125** (1997), 1005–1009.

[47] M. Newman, *Integral matrices*, Academic Press, 1972.

[48] M.M. Parmenter, Free Torsion-free normal complements in integral group rings, *Comm. Algebra* **21** (10) (1993), 3611–3617.

[49] I.B.S. Passi, *Group Rings and their Augmentation Ideals*, Lecture Notes in Mathematics, 715 Springer, Nueva York 1979.

[50] D.S. Passman, *Algebraic Structure of the Group Rings*, Insterscience, Nueva York, 1989.

[51] R.S. Pierce, *Associative algebras*, Springer-Verlag, 1982.

[52] H. Poincaré, Mémoire sur les groupes kleinées, *Acta Math.* **3** (1883), 49–92.

[53] R.A. Rankin, *Modular forms and functions*. Cambridge University Press, 1977.

[54] I. Reiner, *Maximal orders*, Academic Press, 1975.

[55] A. del Río y M. Ruiz, Computing large direct products of free groups in integral group rings, *Comm. Algebra* **30** (4) (2002), 1751–1767.

[56] J. Ritter y S.K. Sehgal, Generators of Subgroups of $\mathcal{U}(\mathbb{Z}G)$, *Contemp. Math.* **93** (1988), 331–347.

[57] J. Ritter y S.K. Sehgal, Construction of units in integral group rings of finite nilpotent groups, *Bull. Amer. Math. Soc.* **20** (1989), 165–168.

[58] J. Ritter, S.K. Sehgal, Construction of units in integral group rings of finite nilpotent groups, *Trans. Amer. Math. Soc.* **324** (2) (1991), 603–621.

[59] J. Ritter y S.K. Sehgal, Construction of units in group rings of monomial and symmetric groups, *J. Algebra* **142** (1991), 511–526.

[60] D.J. Robinson, *A course in the theory of groups*, Springer-Verlag, 1982.

[61] M. Ruiz Marín, *La estructura del grupo de las unidades de un anillo de grupo*. Tesina de Licenciatura. Publicaciones del Departamento de Matemáticas de la Universidad de Murcia, 2000.

[62] A. Salwa, On free subgroups of units of rings, *Preprint*.

[63] I.N. Sanov, A property of a representation of a free group, *Doklady Akad. SSSR* **57** (1947), 657–659.

[64] S.K. Sehgal, *Topics in Group Rings*, Marcel Dekker, Nueva York y Basilea, 1978.

[65] S.K. Sehgal, *Units of Integral Group rings*, Longman Scientific and Technical Essex, 1993.

[66] L.N. Vaserstein, On the group SL_2 over Dedekind rings of arithmetic type, *Math. USSR-Sb* **18** (1973), 321–332.