Anillos de Grupo:

El Problema del Isomorfismo

Trabajo de Fin de Grado
Facultad de Matemáticas
Universidad de Murcia

Autor: *Àngel García Blàzquez*

Tutor: *Ángel del Río Mateos*

A 25 de Junio de 2018

Índice general

Declaración de originalidad

Àngel García Blàzquez, autor del TFG "*Anillos de Grupo: El Problema del Isomorfismo*" bajo la tutela del profesor Ángel del Río Mateos, declara que el trabajo que presenta es original, en el sentido de que ha puesto el mayor empeño en citar debidamente todas las fuentes utilizadas.

En Murcia, a 25 de junio de 2018.

Firmado: Àngel García Blàzquez[1]

[1] En la Secretaría de la Facultad de Matemáticas se ha presentado una copia firmada de esta declaración

Resumen

Este trabajo de fin de grado ha sido enfocado como una preparación a la investigación matemática, concretamente en el ámbito del álgebra. Es por este motivo que el tema principal elegido es un problema vivo en anillos de grupo. La teoría de anillos de grupo es un punto de encuentro de múltiples materias algebraicas. Las conexiones directas con teoría de grupos y con teoría de anillos son obvias por la íntima relación entre los resultados de anillos de grupo y los hechos fundamentales sobre anillos y grupos. De la misma forma, dado su papel central en el desarrollo de la teoría de representaciones de grupo, es claro que ambas teorías están íntimamente ligadas. Por otro lado, dentro de los anillos de grupo son relevantes los anillos de grupo enteros. Para el estudio de éstos, los números algebraicos desempeñan un papel fundamental. Como consecuencia se aprecia la relación con la teoría algebraica de números. Finalmente, es también relevante mencionar que los anillos de grupo son de interés en otras ramas de las matemáticas, como el álgebra homológica, la topología algebraica y los códigos correctores, que nos llevan a toda una variedad de aplicaciones en el mundo digital, desde el procesamiento de señales hasta la ingeniería de software [12].

Para hacerse una idea sobre la importancia de los anillos de grupo en la investigación algebraica, es suficiente observar que varios de los grandes algebristas contemporáneos han trabajado en algún punto de sus carreras en este área, contribuyendo así a su desarrollo(Ver Figura 1).

En el primer capítulo del trabajo trataremos los resultados básicos referidos a los anillos de grupo. Así, comenzaremos presentando una breve cronología en la que expondremos superficialmente el camino recorrido desde la primera aparición de los anillos de grupo en artículos de investigación hasta la presentación del Problema del Isomorfismo para anillos de grupo, que es la cuestión fundamental de este trabajo. Continuaremos el capítulo definiendo los anillos de grupo como tales, así como algunos conceptos y propiedades relevantes en el estudio de éstos, como la semisimplicidad y la aplicación de aumento.

Figura 1: Algunos algebristas que o bien han trabajado directamente en resultados avanzados sobre anillos de grupo o bien han sentado las bases de estos. Entre ellos podemos mencionar: S.A. Amitsur, H. Bass, I. Kaplansky, D.S. Passman, c. Polcino Milies, A.E. Zalesskii y S.K. Sehgal, entre muchos otros.

De esta forma, acabaremos el capítulo habiendo demostrado varios teoremas relevantes en el estudio de los anillos de grupo, como son el Teorema de Maschke y el Teorema de Perlis-Walker. El primero nos dice que un anillo de grupo RG es semisimple si y solo si G es finito con cardinal invertible en R y R es semisimple. Este teorema es importante porque a partir de él se tiene que, en el caso en que R es un cuerpo, RG es semisimple siempre que la característica de R no divida al cardinal del grupo. Exigiremos esta condición en prácticamente todos los resultados del segundo capítulo, pues la semisimplicidad del anillo de grupo será importante para obtener información sobre su estructura.

El Teorema de Perlis-Walker también exigirá esta condición, además de pedir que el grupo sea abeliano, y nos permitirá dar una descomposición en suma directa del anillo de grupo que será muy útil para trabajar con ejemplos concretos. En particular, lo usaremos para dar un resultado negativo del Problema del Isomorfismo. Podemos enunciar este problema de la siguiente manera:

> *Dados un anillo R y dos grupos G y H, ¿Es cierto que si RG y RH son isomorfos como anillos, entonces G y H son isomorfos como grupos?*
> *De forma más general, podemos considerar el problema de para R y G determinados describir salvo isomorfismo los grupos H para los que RG y RH son isomorfos.*

Cuando hablemos de resultados positivos o negativos concretos del Problema del Isomorfismo nos referiremos a la primera versión.

En el segundo capítulo nos centramos en la estructura del centro de las álgebras de grupo. Comenzaremos viendo que si R es un anillo conmutativo y G un grupo cualquiera, las sumas de clase de G sobre R forman una base del centro de RG. A partir de aquí, introduciremos varios conceptos como los cuerpos de escisión y el idempotente principal junto con resultados auxiliares que de nuevo podremos usar para trabajar con ejemplos concretos.

Nos centraremos entonces en el caso integral. Construiremos la representación regular de un álgebra de grupo en general, y la usaremos para demostrar el Teorema de Higman, que afirma que si G es un grupo abeliano finito, entonces las unidades de torsión de $\mathbb{Z}G$ son triviales.

En este tema le puede surgir al lector la sensación de que nos hemos desviado del Problema del Isomorfismo, pero ocurre todo lo contrario. De hecho, el Teorema de Higman lo usaremos en la primera sección del tercer capítulo para demostrar que el Problema del Isomorfismo tiene respuesta afirmativa para anillos de grupo integrales de grupos abelianos finitos. Esta demostración es sencilla y estará basada en que realmente si tenemos un isomorfismo entre RG y RH, y vemos que la imagen por este mismo isomorfismo de G es H tenemos el resultado obtenido. Aplicando el Teorema de Higman y normalizando el isomorfismo dado, bastará ver que la imagen de cada elemento ha de ser una unidad de torsión, y en el caso en que R es $\mathbb{Z}$ esto es sencillo.

Seguiremos el segundo capítulo centrándonos en los elementos idempotentes. Demostraremos un Teorema de Zalesskii y enunciaremos uno de Kaplansky. Estos resultados nos llevarán a concluir que para cualquier grupo G, el anillo de grupo $\mathbb{Z}G$ solo contiene idempotentes triviales. Después volveremos a hablar de unidades de torsión: demostraremos un Teorema de Passman-Bass y lo usaremos para ver que las unidades centrales de torsión de $\mathbb{Z}G$ están en $\pm\mathcal{Z}(G)$. Así, habremos obtenido un resultado relacionado con la conjetura de Kaplansky sobre las unidades de anillos de grupo. Esta es una conjetura importante dentro del ámbito de la investigación en anillos de grupo y sigue abierta hoy en día. Acabaremos el capítulo enunciándola.

Finalmente, comenzaremos el tercer capítulo introduciendo un poco de historia sobre el Problema del Isomorfismo. Es el momento de explicar por qué le hemos dado tanta importancia al caso de los anillos de grupo enteros: En una de las primeras proposiciones del capítulo veremos que si dos anillos de grupo enteros son isomorfos, también son isomorfos los anillos de grupo de los mismos grupos cambiando el anillo de los enteros por cualquier otro anillo conmutativo.

Hemos dedicado mucho espacio a hablar sobre las unidades del anillo de grupo, y volvemos a ello en este capítulo. El motivo de realizar esto es que el Problema del Isomorfismo puede replantearse usando grupos base. Un grupo base de un R-álgebra A es un grupo de unidades de A que a su vez es una base de A sobre R. Por ejemplo, si $A = RG$, entonces G es un grupo base de R. De hecho, si R es un subanillo del centro de otro anillo A y G es un grupo base

de A sobre R entonces A es isomorfo a RG por la propiedad universal de los anillos de grupo. Por tanto, el Problema del Isomorfismo para anillos de grupo consiste en describir las clases de isomorfía de los grupos base de RG y, en particular, si solo hay una clase de isomorfía entonces se tiene la versión fuerte del Problema del Isomorfismo. Por todo esto estudiar la estructura de las unidades del anillo de grupo es muy útil en este contexto.

A continuación, utilizamos el Teorema de Higman que mencionamos antes para ver que si dos anillos de grupo enteros (con grupos finitos) son isomorfos, entonces su centro también lo es. Ahora, vimos anteriormente que las sumas de clase son base del centro, y usando esto junto con un resultado auxiliar obtenemos una correspondencia que nos permite llevar subgrupos normales de un anillo de grupo al otro, conservando cardinales y otras propiedades.

Esta correspondencia junto con otros resultados nos permitirá demostrar la validez del Problema del Isomorfismo para grupos metabelianos en el caso de los anillos de grupo enteros. Concretamente, demostraremos con el Teorema de Whitcomb que los grupos de longitud derivada 2 están determinados por su anillo de grupo entero.

Continuaremos introduciendo el concepto de los grupos circulares y demostrando que para este tipo de grupos también se cumple el Problema del Isomorfismo. Una consecuencia inmediata que veremos es que si K es un cuerpo finito, el grupo general lineal $GL(n, K)$ está determinado por su anillo de grupo entero. Veremos más ejemplos y daremos una lista no exhaustiva de tipos de grupos para los cuales el Problema del Isomorfismo tiene respuesta positiva.

Finalmente, acabaremos el trabajo dando un resultado negativo del Problema del Isomorfismo. Este resultado fue anunciado por Martin Hertweck en 1997, aunque su publicación no se produjo hasta el 2001. En su trabajo, se construyen un grupo X y un subgrupo Y del grupo de unidades de aumento 1 de $\mathbb{Z}X$ que tiene el mismo orden que X y que cumple que $\mathbb{Z}Y = \mathbb{Z}X$, pero no es isomorfo a X.

El grupo construido por Hertweck tiene longitud derivada 4, y por el Teorema de Whitcomb sabemos que el Problema del Isomorfismo tiene respuesta afirmativa para grupos finitos resolubles con longitud derivada 2, lo cual deja la pregunta de qué ocurre con los grupos con longitud derivada 3. Esta pregunta sigue sin respuesta a día de hoy.

Una variante del Problema del Isomorfismo, el Problema del Isomorfismo Modular, tiene mucho interés últimamente. El problema se enuncia de la siguiente forma:

Sean P y Q p-grupos finitos. Entonces, ¿$\mathbb{F}_pP \cong \mathbb{F}_pQ \Rightarrow P \cong Q$?

Solo unos pocos resultados positivos se conocen al respecto, como el caso en que P y Q sean ambos abelianos, pero el resultado general sigue abierto. El autor de este trabajo espera continuarlo en el futuro ampliándolo con este problema y otros resultados interesantes sobre los anillos de grupo.

Abstract

This project has been made as an introduction into mathematical research, being abstract algebra the primary focus. That is the reason why the main interest chosen is a current problem in group rings. The theory of group rings is a meeting point of various algebraic theories. Taking into account its central role in the development of the theory of group representations, it is clear how close the later is related to it. The direct connections with the theory of groups and with ring theory are also obvious because of the intimate relations between the results on group rings and deep facts about groups and rings. Since integral group rings are of special interest for researchers and the topic involves the use of algebraic numbers, algebraic number theory also has an important role in the development of the subject. Finally, it is worthwhile to mention that group rings are important in other branches of mathematics, such as homological algebra, algebraic topology and algebraic K-theory, and that during the last decade significant applications have been obtained in the theory of error correcting codes, allowing the creation of new codes which are simultaneously efficient and reliable. These codes have several applications, from signal transmission to software engineering [12].

To get a general idea about the importance of group rings in algebraic research, it is enough to observe that several great contemporary algebraists have worked at some point of their lives in the area, contributing fundamentally to its development (See Figura 2)

In the first chapter of this dissertation, we will focus on the basic facts related to group rings. Thus, we will start by introducing a small chronology in which we will expose superficially the path travelled from the first occurrence of group rings in academic articles to the official statement of the Isomorphism Problem, which is the key interest of this work. We will then continue the chapter giving the formal definition of group rings, together with some relevant properties and relations needed for its study, such as semisimplicity and the augmentation mapping.

Figura 2: Some algebraic researchers that have either first-hand worked on contemporary results about group rings or instead they have established the base of group ring research. Among them we can mention: S.A. Amitsur, H. Bass, I. Kaplansky, D.S. Passman, c. Polcino Milies, A.E. Zalesskii and S.K. Sehgal.

Thereafter, when we finish the chapter we will have given the proof of several important theorems in the study of group ring theory, such as Maschke's Theorem and Perlis-Walker's Theorem. The former states that the group ring RG is semisimple if and only if G is a finite group with cardinal invertible in R and R is also semisimple. This theorem has great relevance because in the particular case where R is a field, is shows that RG is semisimple when R has a characteristic that does not divide the number of elements of G. This hypothesis will be mandatory for most of the results of the second chapter, because the semisimplitiy of the group ring will be very important to obtain information from its structure.

Thus, Perlis-Walker's Theorem will also ask for this condition, apart from demanding that the group of the group ring is abelian, and it will allow us to give a decomposition in direct summands for the group ring that will be very useful to work with concrete examples. In particular, we will use it to give a negative result for the Isomorphism Problem. We can state the Isomorphism Problem as follows:

> *Given a ring R and two groups G and H, is it true that if RG and RH are isomorphic as rings, then G and H are isomorphic as groups?*
> *In a more general way, given fixed R and G, we may consider the question of describing up to isomorphism the groups H for which RG and RH are isomorphic.*

When we refer to particular positive or negative results of the Isomorphic Problem we will be relating to the first expression of the problem.

In the second chapter of the memoir, we will focus our attention in the structure of the center of group algebras. We will start the chapter proving that if R is a commutative ring and G is an arbitrary group, then the class sums of G over R are a base of the center of RG. From this point, we will introduce several concepts such as partition fields and the principal idempotent, altogether with some auxiliar results that will allow us to work with some other examples.

Our main focus will be integral group rings. We will define the regular representation for group algebras, and then we will prove Higman's Theorem. This result states that if G is a finite abelian group, then the torsion units of $\mathbb{Z}G$ are trivial.

During this chapter, the reader might get the feeling that we have deviated from the Isomorphism Problem and we have reached the territory of general knowledge about group rings. It is actually the opposite. In fact, in the following chapter we will use the recently stated Higman's Theorem to show that the Isomorphism Problem has an affirmative answer for integral group rings of finite abelian groups. This proof is simple and it is based in the following: If we have an isomorphism between $\mathbb{R}G$ and $\mathbb{R}H$, and we prove that the image by this isomorphism of G is H we get the desired result. The hard part is that most of the time we do not know much about the image of an element by this isomorphism. Using Higman's Theorem in this situation and normalizing the given isomorphism, we will only need to see that the image of each element is a torsion unit. This is not hard at all when R is $\mathbb{Z}$.

We will continue this chapter focusing on idempotent elements. We will show the proof of a theorem from Zalesskii, and we will enunciate another one from Kaplansky. These results will lead us to the conclusion that for each group G, the integral group ring $\mathbb{Z}G$ contains only trivial elements. Later, we will go back to the topic of torsion units. We will prove a Passman-Bass Theorem and we will use it to show that all central units of finite order in $\mathbb{Z}G$ are trivial. Thus, we will have obtained a result related with Kaplansky's Conjecture for group rings. This is a very important conjecture in contemporary research on group rings and it remains open. We will end the chapter explaining this conjecture briefly.

Finally, we will start the third chapter with introducing an small fraction of the history of the Isomorphism Problem. This is the time to explain why we have given so much importance to integral group rings. In one of the first propositions of this chapter we will show that if two integral group rings of the given groups G and H are isomorphic, then, for every commutative ring R, the group rings RG and RH are also isomorphic.

We have invested quite a lot of time on the units of group rings, and we will go back at it in this chapter. The reason for doing this is that the Isomorphism Problem can be restated in terms of group basis. A group basis of an R-algebra A is a group of units of A which is also a basis of A over R. In fact, if R is a subring of the center of another ring A and G is a group

basis of A over R, then A is isomorphic to RG because of the universal property for group rings. Therefore, the Isomorphism Problem asks to describe the isomorphism classes of the group basis of RG. In particular, if there is only one isomorphism class, then we get that the strong version of the isomorphism problem takes place. Because all of this, studying the structure of the units of group rings is very useful in this matter.

Next, we will use the previously stated Higman's Theorem to see that if two integral group rings (of finite groups) are isomorphic then the centers of these groups are isomorphic too. We also showed previously that class sums are a basis for the center. Using this and an auxiliar result altogether, we will obtain a one-to-one correspondence between the lattice of normal subgroups of G and H, when the integral group rings of these groups are isomorphic. This correspondence will preserve orders and other important properties.

This correspondence, along with other propositions, will allow us to give a positive answer to the Isomorphism Problem for integral group rings with metabelian groups. Specifically, we will prove a Whitcomb's Theorem that shows that groups with derived length 2 are determined by their integral group ring.

Afterwards, we will introduce the concept of circle groups and we will prove that for these groups the Isomorphism Problem has a positive answer too. An immediate consequence is that if K is a finite field, the general linear group $GL(n, K)$ is determined by its integral group ring. We will show some more examples, and we will give a non-exhaustive list of types of groups for which the Isomorphism Problem has a positive answer.

Finally, we will finish our work giving a negative result for the Isomorphism Problem. This result was announced by Martin Hertweck in 1997, though it wasn't published until 2001. In its work, two groups X and Y are built up so that Y is a subgroup of the group of units with augmentation 1 of the integral group ring of X. Y has the same size as X and also $\mathbb{Z}Y = \mathbb{Z}X$, but $X \ncong Y$. This is, he built a group X and a group basis of $\mathbb{Z}X$ non isomorphic to X.

The group given by Hertweck has derived length 4, and we also know that the Isomorphism Problem has a positive answer for finite solvable groups with derived length 2, so that leaves the question of whether solvable groups with derived length 3 have a positive answer or not. This question remains open until the moment this project has been made.

A variant of the Isomorphism Problem, the Modular Isomorphism Problem, has awoken a lot of interest nowadays. The problem can be stated as follows:

Let P y Q be finite p-groups. Then, $\mathbb{F}_pP \cong \mathbb{F}_pQ \Rightarrow P \cong Q$?.

Only a few positive results are known regarding this problem. In general, the question remains open. The author of this project intends to extend it in the future with this problem and other interesting results in group ring theory.

1- Anillos de grupo

En este capítulo introduciremos los conceptos que trataremos a lo largo del trabajo.

- Comenzaremos mostrando una breve historia de los anillos de grupo, incluyendo algunos resultados avanzados sobre el Problema del Isomorfismo.
- Después, definiremos los anillos de grupo como tales y daremos algunos resultados imprescindibles sobre ellos, así como algunas propiedades de especial interés.
- Acabaremos el capítulo dando una descripción completa del anillo de grupo para grupos abelianos finitos sobre un cuerpo cuya característica no divide al cardinal del grupo. Esta condición implicará la semisimplicidad del anillo de grupo. Con esta descripción podremos dar un resultado negativo sencillo de un caso particular del Problema del Isomorfismo.

1.1. Breve historia de los anillos de grupo

El concepto de *Anillo de Grupo* es relativamente viejo. Aparece implícitamente en un artículo de A. Cayley [2] en 1854, que es considerado el primer trabajo en teoría abstracta de grupos. En su artículo, Cayley expuso una construcción formal del anillo de grupo $\mathbb{C}S_3$ que es esencialmente la misma que se realiza hoy en día.

En 1892, volvieron a aparecer los anillos de grupo en un artículo de T. Molien sobre álgebras complejas, en el que introdujo las nociones de álgebras simples y semisimples. En un artículo posterior, Molien obtuvo importantes resultados en teoría de representaciones complejas de grupos finitos, incluyendo las relaciones de ortogonalidad para caracteres de grupo.

Los anillos de grupo complejos para grupos finitos aparecen de forma natural en el estudio de representaciones de grupos finitos, y es en el contexto de teoría de representación cuando fueron estudiados extensivamente. El estudio de anillos de grupo arbitrarios de dimensión finita por su propio interés siguió poco después. El primer libro sobre el tema fue escrito por Donald S. Passman y publicado en 1977 [17].

Gran parte del desarrollo de la teoría de anillos de grupo fue estimulado por la abundante cantidad de problemas aparentemente irresolubles. Una famosa conjetura sobre anillos de grupo es la Conjetura de Kaplansky, que afirma que todas las unidades del anillo de grupo de un cuerpo y un grupo libre de torsión son triviales. Se sabe muy poco de esta conjetura hoy en día. Volveremos a ella al final del capítulo 2, donde usaremos varios enunciados obtenidos para dar resultados ciertos similares al enunciado general de la conjetura.

Un problema interesante en la teoría de anillos de grupo es el *Problema del Isomorfismo*: Si R es un anillo fijo y G y H son grupos de forma que los anillos de grupo RG y RH son isomorfos, ¿se tiene necesariamente que G y H son isomorfos? Es decir, ¿RG determina a G?

En 1940, Graham Higman [10] publicó el primer artículo directamente relacionado con el Problema del Isomorfismo. En los sesenta este problema comenzó a atraer gran atención de los algebristas y fue estimulado por la inclusión de cuestiones sobre anillos de grupo en la famosa lista de problemas en teoría de anillos de Irving Kaplansky [13].

Veremos resultados sencillos en el caso $R = \mathbb{C}$ contrarios al Problema del Isomorfismo. Respecto del caso $R = \mathbb{Z}$, en 2001 Martin Hertweck publicó un artículo [9] en el que muestra una pareja de grupos no isomorfos que tienen anillos de grupo enteros isomorfos. Estudiaremos la situación de los anillos de grupo enteros en detalle, pero no entraremos a desarrollar completamente el resultado dado por Hertweck, por sobrepasar el nivel esperado para un trabajo de fin de grado.

1.2. Hechos básicos

Sean G un grupo no necesariamente finito y R un anillo. Queremos construir un R-módulo que tenga los elementos de G como base y usar las operaciones tanto en G como en R para definir una estructura de anillo en él. En tal R-módulo, que denotaremos como RG, cada elemento a tendrá una expresión única como $\sum_{g\in G} a_g g$ con $a_g \in R$ para todo $g \in G$ y $a_g = 0$ para casi todo $g \in G$.

Cuando sea conveniente, escribiremos los coeficientes a_g como $a(g)$. Nótese que la definición implica que dos elementos $a = \sum_{g\in G} a_g g$ y $b = \sum_{g\in G} b_g g$ son iguales si y solo si $a_g = b_g$ para todo elemento g de G.

Si consideramos dos elementos $a = \sum_{g\in G} a_g g$ y $b = \sum_{g\in G} b_g g$ en RG, su suma viene determinada de forma natural por ser G base y podemos definir su producto de la siguiente manera:

$$ab = \sum_{g,h\in G} a_g b_h gh = \sum_{u\in G} c_u u, \text{ poniendo } c_u = \sum_{u=gh} a_g b_h.$$

Puede verse fácilmente que RG con estas operaciones forma un anillo unitario, siendo $\mathbf{1}= \sum_{g\in G} u_g g$ donde el coeficiente correspondiente al elemento unidad de G es 1 y $u_g = 0$ para cualquier otro elemento g de G. De nuevo, puede verse fácilmente que RG es un R-módulo.

Dado un elemento $\alpha = \sum_{g\in G} a_g g$ perteneciente a RG, definiremos su **soporte** como el subconjunto de elementos de G que aparecen efectivamente en la expresión de α:

$$supp(\alpha) = \{g \in G : a_g \neq 0\}.$$

Definición 1.2.1. *El conjunto RG, con las operaciones definidas arriba, es llamado el **anillo de grupo de** G **sobre** R. Cuando R es conmutativo, también se llama a RG **álgebra de grupo de** G **sobre** R.*

Asumimos además las siguiente notación implícita.

Notación 1.2.2. *Cuando consideremos elementos a, x en RG, salvo mención explícita de lo contrario asumiremos que se expresan como $a = \sum_{g\in G} a_g g$ y $x = \sum_{g\in G} x_g g$ con a_g, $x_g \in R$ para todo g en G.*

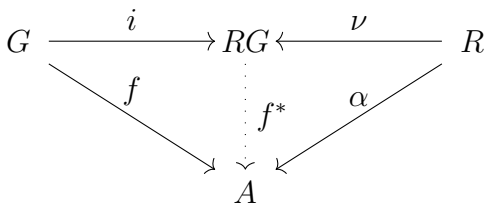
Podemos ver G como subconjunto de RG definiendo la inclusión $i : G \to RG$ de forma que a cada elemento x perteneciente a G se le asigna el elemento $i(x) = \sum_{g\in G} x_g g$ donde $x_g = 1$ para $g = x$, y $x_g = 0$ en el resto.

También podemos ver R como subanillo de RG, a través del monomorfismo de anillos $\nu : R \to RG$ dado por $\nu(r) = \sum_{g\in G} r_g g$, donde $r_{1_G} = r$ y $a_g = 0$ en el resto.

Tras estas identificaciones, dados r perteneciente a R y g en G tenemos claramente que $rg = gr$ en RG. Así, si R es conmutativo tenemos que $R \subseteq \mathcal{Z}(RG)$, el **centro** de RG.

Enunciamos ahora la *propiedad universal de los anillos de grupo*. Llamamos $\mathcal{U}(A)$ al conjunto de elementos de A que poseen inverso.:

Proposición 1.2.3. *Sean G un grupo y R un anillo. Dado cualquier anillo A tal que $R \subseteq A$, se cumple que para todo homomorfismo de grupos $\alpha : R \to A$ y todo homomorfismo de grupos $f : G \to \mathcal{U}(A)$ que cumplan $\alpha(r)f(g) = f(g)\alpha(r)$ para todo $g \in G$ y $r \in R$ existe un único homomorfismo de anillos $f^* : RG \to A$ que hace conmutativo el siguiente diagrama:*



Donde $i : G \to RG$ y $\nu : R \to RG$ son los monomorfismos dados arriba. Más aún, si $R \subseteq \mathcal{Z}(A)$ (y así, A puede verse como R-álgebra), entonces f^* es un homomorfismo de R-álgebras.

Demostración. Dada $f : G \to A$, consideramos $f^* : RG \to A$ definida por:

$$\sum_{g\in G} a_g g \mapsto \sum_{g\in G} \alpha(a_g) f(g).$$

La prueba de la afirmación son solo cuentas ahora. Por ejemplo, para ver que $f^*(ab) = f^*(a)f^*(b)$, poniendo $c_u = \sum_{u=gh} a_g b_h$, tenemos:

$$\begin{aligned} f^*(ab) = f^*\left(\sum_{u\in G} c_u u\right) = \sum_{u\in G} \alpha(c_u) f(u) &= \sum_{u\in G} \sum_{u=gh} \alpha(a_g b_h) f(gh) \\ &= \sum_{u\in G} \sum_{u=gh} \alpha(a_g)\alpha(b_h) f(g) f(h) \\ &= \sum_{g\in G} \alpha(a_g) f(g) \sum_{h\in G} \alpha(b_h) f(h) = f^*(a) f^*(b), \end{aligned}$$

□

Lo siguiente es un caso particular de esta proposición, cuando α es el monomorfismo de anillos que actúa como la identidad entre R y RH (como el monomorfismo ν definido arriba).

Corolario 1.2.4. *Sea $f : G \to H$ un homomorfismo de grupos. Entonces, existe un único homomorfismo de anillos $f^* : RG \to RH$ tal que $f^*(g) = f(g)$ para todo elemento $g \in G$ y $f^*(r) = r$ para todo elemento r en R. Si R es conmutativo, entonces f^* es un homomorfismo de R-álgebras; más aún, si f es un epimorfismo (resp. monomorfismo), entonces f^* también es un epimorfismo (resp. monomorfismo).*

Observamos que si $H = \{1\}$, se deduce de este corolario que la aplicación trivial G $\mapsto \{1\}$ induce un homomorfismo de anillos $\varepsilon : RG \to R$ tal que $\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$.

Definición 1.2.5. *El homomorfismo $\varepsilon : RG \to R$ dado por $\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$ es llamado **aplicación aumento** de RG y su núcleo, denotado $\Delta(G)$, es llamado el **ideal de aumento** de RG.*

Nótese que si a es un elemento de $\Delta(G)$, entonces $\varepsilon(a) = \varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g = 0$. Así, podemos escribir a de la siguiente forma:

$$a = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g(g-1)$$

Ahora, como para todo elemento g perteneciente a G se tiene que $g-1 \in \Delta(G)$, esta observación nos muestra que $\{g-1 : g \in G, g \neq 1\}$ es un conjunto de generadores de $\Delta(G)$ sobre R. Además, nótese que este conjunto es linealmente independiente sobre R. En conclusión, hemos probado lo siguiente:

Proposición 1.2.6. *El conjunto $\{g-1 : g \in G, g \neq 1\}$ es una base de $\Delta(G)$ sobre R.*

Así, podemos escribir

$$\Delta(G) = \left\{ \sum_{g\in G} a_g(g-1) \ : g \in G,\ g \neq 1,\ a_g \in R \right\}$$

asumiendo, igual que antes, que solo una cantidad finita de coeficientes a_g son diferentes de cero. Nótese que si G es finito, entonces $\Delta(G)$ es un R-módulo libre de rango $|G| - 1$.

Acabamos esta sección viendo que los anillos de grupo sobre anillos conmutativos son anillos con involución.

Proposición 1.2.7. *Sea R un anillo conmutativo. La aplicación $* : RG \to RG$ definida como:*

$$\left(\sum_{g\in G} a(g)g\right)^* = \sum_{g\in G} a(g)g^{-1}$$

satisface las siguientes propiedades:

(i) $(a+b)^* = a^* + b^*$

(ii) $(ab)^* = b^*a^*$, *y*

(iii) $(a^*)^* = a$.

La prueba es directa, así que la omitimos.
Vamos a fijar ahora una notación que será muy utilizada durante el resto del trabajo.

Notación 1.2.8. *Dados un anillo R y $X \subseteq R$ finito, denotaremos* $\widehat{X} = \sum_{x\in X} x$

Introducimos para acabar la sección el concepto de anulador. Definimos los anuladores sobre un anillo cualquiera pero los usaremos mayormente sobre RG.

Definición 1.2.9. *Sean R un anillo y $X \subseteq R$. El* ***anulador izquierdo*** *de X es el conjunto*

$$Ann_l(X) = \{\alpha \in R : \alpha x = 0, \forall x \in X\}.$$

De forma similar, definimos el ***anulador derecho*** *de X por:*

$$Ann_r(X) = \{\alpha \in R : \alpha x = 0, \forall x \in X\}.$$

Cuando el anillo sea conmutativo, a veces escribiremos $Ann(\cdot)$ sin especificar el lado y nos referiremos a estos conjuntos como **anuladores** en general.

1.3. Ideales de aumento relativos

Vamos a estudiar la relación entre los subgrupos de G y los ideales de RG. Esta relación, que ya tiene interés en sí misma, nos será útil para estudiar varios problemas sobre la estructura y las propiedades de RG.

Definición 1.3.1. *Dado un subgrupo H de G, denotaremos por $\Delta_R(G,H)$ al ideal izquierdo de RG generado por el conjunto $\{h-1 : h \in H\}$. Esto es,*

$$\Delta_R(G,H) = \left\{ \sum_{h\in H} \alpha_h(h-1) \, : \, \alpha_h \in RG \right\}$$

Cuando trabajemos con un anillo fijo R omitiremos el subíndice y denotaremos el ideal simplemente por $\Delta(G,H)$. Nótese que el ideal $\Delta(G,G)$ coincide con el ideal $\Delta(G)$ introducido en la sección 1.2.

Lema 1.3.2. *Sean G un grupo y H un subgrupo suyo. Sea además S un conjunto de generadores de H. Entonces el conjunto $\{s-1 : s \in S\}$ es un conjunto de generadores de $\Delta(G,H)$ como ideal izquierdo de RG.*

Demostración. Como S es un conjunto de generadores de H, todo elemento h de H distinto de 1 puede escribirse de la forma $h = s_1^{\varepsilon_1} s_2^{\varepsilon_2} ... s_r^{\varepsilon_r}$ con $s_i \in S$, $\varepsilon_i = \pm 1$ para $1 \leq i \leq r$, siendo r algún entero positivo. Para probar el lema, es suficiente mostrar que todos los elementos de la forma $h-1$ con h en H están en el ideal izquierdo I generado por el conjunto $\{s-1 : s \in S\}$. Esto puede verse aplicando repetidamente las identidades $x^{-1}-1 = x^{-1}(1-x)$ y $xy-1 = x(y-1)+(x-1)$. Veámoslo aplicando inducción en r:

Si $r = 1$, tenemos dos casos:

- $h \in S$, de forma que $h-1$ pertenece a I por definición.
- $h = s^{-1}$ con $s \in S$, en cuyo caso $h-1 = s^{-1}-1 = s^{-1}(1-s) = -s^{-1}(s-1)$, que está en I.

En el caso general, si fijamos $r = n$ y consideramos que para todo h de la forma establecida con $r < n$ se cumple que $h-1$ está en I, entonces, sea $h = s_1^{\varepsilon_1} s_2^{\varepsilon_2} ... s_n^{\varepsilon_n}$. De nuevo, tenemos dos casos:

- Si $\varepsilon_n = 1$, entonces $h-1 = s_1^{\varepsilon_1}s_2^{\varepsilon_2}...s_n - 1 = s_n(s_1^{\varepsilon_1}s_2^{\varepsilon_2}...s_{n-1}^{\varepsilon_{n-1}} - 1) + (s_n - 1)$, que está en I por ser la suma de dos elementos de I, pues $s_1^{\varepsilon_1}s_2^{\varepsilon_2}...s_{n-1}^{\varepsilon_{n-1}} - 1 \in I$ por hipótesis de inducción.

- Si $\varepsilon_n = -1$, entonces $h-1 = s_1^{\varepsilon_1}s_2^{\varepsilon_2}...s_n^{-1} - 1 = s_n^{-1}(s_1^{\varepsilon_1}s_2^{\varepsilon_2}...s_{n-1}^{\varepsilon_{n-1}} - 1) + (s_n^{-1} - 1) = (s_1^{\varepsilon_1}s_2^{\varepsilon_2}...s_{n-1}^{\varepsilon_{n-1}} - 1) + -s_n^{-1}(s_n - 1)$, que está en I, volviendo a usar la hipótesis de inducción.

□

Para dar una mejor descripción de $\Delta_R(G,H)$, denotemos por $\mathcal{T} = \{q_i\}_{i\in I}$ un conjunto completo de representantes de las clases laterales izquierdas de H en $\mathcal{T}$, o sea un **transversal** por la izquierda de H en G. Asumimos que elegimos siempre como representante de la clase H en $\mathcal{T}$ precisamente al elemento identidad de G. Así, cada elemento g de G puede escribirse de forma única de la forma $g = q_ih_j$ con $q_i \in \mathcal{T}$ y $h_j \in H$.

Proposición 1.3.3. *El conjunto* $B_H = \{q(h-1) : q \in \mathcal{T},\ h \in H,\ h \neq 1\}$ *es una base de* $\Delta_R(G,H)$ *sobre* R.

Demostración. Primero mostraremos que este conjunto es linealmente independiente sobre R. Asumamos que tenemos una combinación lineal $\sum_{i,j} r_{ij}q_i(h_j - 1) = 0$, con $r_{ij} \in R$. Entonces, podemos escribir:

$$\sum_{i,j} r_{ij}q_ih_j = \sum_i \left(\sum_j r_{ij}\right) q_i.$$

Como $h_j \neq 1$ para todos los valores de j, se sigue fácilmente que los miembros de la ecuación de arriba tienen soportes disjuntos. Como los elementos de G son linealmente independientes sobre R, se sigue que todos los coeficientes han de ser 0. En particular, $r_{ij} = 0$ para todo i,j.

Para mostrar que B_H también genera $\Delta_R(G,H)$, es suficiente probar que todo elemento de la forma $g(h-1)$, con g en G y h en H, puede escribirse como combinación lineal de elementos en B_H. Ahora, $g = q_ih_j$ para ciertos $q_i \in \mathcal{T}, h_j \in H$. Entonces,

$$g(h-1) = q_ih_j(h-1) = q_i(h_jh - 1) - q_i(h_j - 1)$$

y se sigue el resultado. □

Tomando $H = G$, tenemos la Proposición 1.2.6.

Ahora daremos una interpretación de $\Delta(G,H)$, cuando H es un subgrupo normal de G. En este caso, por la propiedad universal de los anillos de grupo, el homomorfismo canónico $\omega : G \to G/H$ puede extenderse a un epimorfismo $\omega^* : RG \to R(G/H)$ tal que:

$$\omega^*\left(\sum_{g\in G} a(g)g\right) = \sum_{g\in G} a(g)\omega(g)$$

Proposición 1.3.4. *Con las notaciones de arriba, $Ker(\omega^*) = \Delta(G,H)$.*

Demostración. De nuevo, sea $\mathcal{T}$ un transversal por la izquierda de H en G. Entonces, todo elemento α en RG puede escribirse como suma finita $\alpha = \sum_{i,j} r_{ij}q_ih_j$, con r_{ij} en R, q_i en $\mathcal{T}$ y h_j en H. Si además denotamos por $\bar{q}_i$ la imagen de q_i en el grupo cociente G/H entonces tenemos

$$\omega^*(\alpha) = \sum_i \left(\sum_j r_{ij}\right)\bar{q}_i.$$

Así, $\omega \in Ker(\omega^*)$ si y solo si $\sum_j r_{ij} = 0$ para cada valor de i. Así, si $\alpha \in Ker(\omega^*)$ podemos escribir (añadiendo ceros):

$$\begin{aligned}\alpha &= \sum_{i,j} r_{ij}q_ih_j = \sum_{i,j} r_{ij}q_ih_j - \sum_i \left(\sum_j r_{ij}\right) q_i \\ &= \sum_{i,j} r_{ij}q_i(h_j - 1) \in \Delta(G,H).\end{aligned}$$

Luego $Ker(\omega^*) \subseteq \Delta(G,H)$. La otra inclusión es directa. □

Corolario 1.3.5. *Sea H un subgrupo normal de G. Entonces $\Delta(G,H)$ es un ideal bilátero de RG y*

$$\frac{RG}{\Delta(G,H)} \cong R(G/H).$$

De hecho, se verifica el recíproco de este corolario. Si H no es normal en G, entonces existen g en G y h en H tales que $g^{-1}hg \notin H$, luego $g^{-1}hg - 1 = (g^{-1}h - g^{-1})g \notin \Delta(G,H)$ mientras que $g^{-1}h - g^{-1} = g^{-1}(h-1)$ sí que está en $\Delta(G,H)$. Como caso particular, tenemos que $\Delta(G)$ es el núcleo del homomorfismo de aumento de RG.

Llegados a este punto hemos construido una aplicación entre el conjunto de los subgrupos de G y el conjunto de ideales por la izquierda de RG que lleva los subgrupos normales de G a ideales biláteros de RG. Construyamos ahora una aplicación en sentido contrario. Dado un ideal izquierdo I de RG, consideramos el conjunto

$$\nabla(I) = \{g \in G : g - 1 \in I\} = G \cap (1 + I).$$

Afirmamos que $\nabla(I)$ es un subgrupo de G. De hecho, si $g, h \in \nabla(I)$ entonces $gh - 1 = g(h-1)+g-1 \in \nabla(I)$, y así, $gh \in \nabla(I)$. Además, si $g \in \nabla(I)$, entonces $g^{-1}-1 = -g^{-1}(g-1) \in I$, y así $g^{-1} \in \nabla(I)$. Es fácil verificar que si I es un ideal bilátero, de RG, entonces $\nabla(I)$ es normal en G.

Proposición 1.3.6. *Si H es un subgrupo de G, entonces $\nabla(\Delta(G, H)) = H$*

Demostración. Pongamos $g \in \nabla(\Delta(G, H))$, con $1 \neq g$. Entonces $g - 1$ está en $\Delta(G, H)$ y puede entonces escribirse como

$$g - 1 = \sum_{i,j} r_{ij} q_i (h_j - 1), \text{ con } h_j \in H \setminus \{-1\} \text{ y } g_i \in G \setminus H$$

Como 1 aparece en la parte izquierda de la igualdad, también ha de aparecer en la parte derecha; luego uno de los elementos q_i ha de ser $q_1 = 1$. Como consecuencia, hay un término de la forma $r_{1j}(h_j - 1)$ en la parte derecha de la igualdad. Como todos los elementos de G en la parte derecha son diferentes dos a dos, tenemos que $g = h_j$ está en H. Así, $\nabla(\Delta(G, H)) \subseteq H$. □

Uno podría pensar entonces que ambas aplicaciones son inversas entre sí, pero no. Como ejemplo en el que no se cumple esto, podemos tomar $I = RG$. En este caso $\nabla(RG) = \{g \in G : g - 1 \in RG\} = G$, y así $\Delta(G, \nabla(RG)) = \Delta(G)$, distinto de RG.

1.4. Semisimplicidad

Definición 1.4.1. *Se dice que un R-módulo M es **semisimple** si todo submódulo de M es un sumando directo. Los anillos que son módulos semisimples sobre sí mismos se llaman **anillos semisimples***

La estructura de los anillos semisimples queda determinada por el Teorema de Artin-Wedderburn, que los caracteriza como isomorfos a un producto directo de anillos de matrices sobre anillos de división. Lo enunciamos sin demostración.

Teorema 1.4.2 (Artin-Wedderburn)**.** *Sea R un anillo semisimple. Entonces*

$$R \overset{\phi}{\cong} \bigoplus_{i=1}^{r} M_{n_i}(D_i), \text{ con } D_i \text{ anillos de división.}$$

En esta fórmula, r es el número de R-módulos simples y n_i y D_i están determinados por R salvo isomorfismos.

Vamos a determinar las condiciones necesarias y suficientes sobre R y G para que el anillo de grupo RG sea semisimple. Primero veremos algunos resultados auxiliares.

Proposición 1.4.3. *Si $X \subseteq G$ entonces $\widehat{X}$ (recordamos que $\widehat{X} = \sum_{x \in X} x$) es central en RG si y solo si $g^{-1}Xg = X$ para todo $g \in G$. En particular, si H es un subgrupo finito entonces H es normal en G si y solo si $\widehat{H}$ es central en RG*

Demostración. Como decir que $\widehat{X}$ es central en RG equivale a que para todo $g \in G$ se cumpla $g^{-1}\widehat{X}g = \widehat{X}$, o sea $\sum_{x \in X} g^{-1}xg = \sum_{x \in X} x$, el resultado se sigue por ser G base de RG sobre R. El caso particular se deduce directamente de la definición de subgrupo normal. □

Lema 1.4.4. *Sean H un subgrupo de G y R un anillo. Entonces $Ann_r(\Delta(G,H)) \neq 0$ si y solo si H es finito. En este caso tenemos*

$$Ann_r(\Delta(G,H)) = \widehat{H} \cdot RG.$$

Más aún, si H es un subgrupo normal de G, entonces $\widehat{H} \in \mathcal{Z}(RG)$ y tenemos

$$Ann_r(\Delta(G,H)) = Ann_l(\Delta(G,H)) = RG \cdot \widehat{H}.$$

Demostración. Asumamos $Ann_r(\Delta(G,H)) \neq 0$ y elijamos a distinto de 0 en $Ann_r(\Delta(G,H))$. Para cada elemento $h \in H$ tenemos que $(h-1)a = 0$, y así $ha = a$. Esto es,

$$a = \sum_{g \in G} a_g g = \sum_{g \in G} a_g hg.$$

Tomemos $g_0 \in supp(a)$. Entonces, $a_{g_0} \neq 0$, luego la ecuación de arriba nos muestra que $hg_0 \in supp(a)$ para todo elemento $h \in H$. Como $supp(a)$ es finito, esto claramente implica que H ha de ser finito. Nótese que este argumento muestra que siempre que tomemos $g_0 \in supp(a)$, el coeficiente de todo elemento de la forma hg_0 es igual al coeficiente de g_0, así que podemos escribir a de la forma:

$$a = a_{g_0}\widehat{H}g_0 + a_{g_1}\widehat{H}g_1 + \cdots + a_{g_t}\widehat{H}g_t = \widehat{H}\beta, \ \beta \in RG.$$

Esto muestra que si H es finito, entonces $Ann_r(\Delta(G,H)) \subseteq \widehat{H} \cdot RG$. La inclusión opuesta se sigue trivialmente, pues $h\widehat{H} = \widehat{H}$ implica que $(h-1)\widehat{H} = 0$, para todo $h \in H$.

El resto del enunciado se deduce de la Proposición 1.4.3, pues si H es un subgrupo normal de G, sabemos por dicha proposición que $\widehat{H} \in \mathcal{Z}(G)$ y entonces

$$Ann_r(\Delta(G,H)) = Ann_l(\Delta(G,H)) = \widehat{H} \cdot RG = RG \cdot \widehat{H}.$$

□

Corolario 1.4.5. *Sea G un grupo finito. Entonces:*

(i) $Ann_l(\Delta(G)) = Ann_r(\Delta(G)) = R \cdot \widehat{G}$.

(ii) $Ann_r(\Delta(G)) \cap \Delta(G) = \{a\widehat{G} : a \in R, \ a|G| = 0\}$

Demostración. Se sigue del Lema 1.4.4, tomando $H = G$ para el primer caso y notando que $\alpha = a\widehat{G} \in \Delta(G)$ si y solo si $\varepsilon(\alpha) = a\varepsilon(\widehat{G}) = a|G|$ es igual a cero. □

El siguiente resultado será muy usado más adelante:

Lema 1.4.6. *Sea I un ideal bilátero de R. Supongamos que existe un ideal izquierdo J tal que $I \cap J = (0)$. Entonces $J \subseteq Ann_r(I)$*

Demostración. Tomemos $x \in J$ e $y \in I$ arbitrarios. Como J es un ideal izquierdo e I es bilátero, tenemos que $yx \in J \cap I = (0)$. Como consecuencia, $yx = 0$ y así $x \in Ann_r(I)$. □

Lema 1.4.7. *Si el ideal de aumento $\Delta(G)$ es un sumando directo en RG (como RG-módulo), entonces G es finito y $|G|$ es invertible en R.*

Demostración. Suponiendo la hipótesis como cierta, existe J distinto del vacío tal que $RG = \Delta(G) \oplus J$. Así, $\Delta(G) \cap J = (0)$ y el Lema 1.4.6 nos muestra que $J \subseteq Ann_r(\Delta(G))$. De esta forma, $Ann_r(\Delta(G)) \neq (0)$ y así, aplicando el Lema 1.4.4 obtenemos que G es finito y $Ann_r(\Delta(G)) = \widehat{G}(RG) = \widehat{G}R$.

Para la segunda parte, escribimos $RG = \Delta(G) \oplus J$ y $1 = e_1 + e_2$, con $e_1 \in \Delta(G), e_2 \in J$. Entonces $1 = \varepsilon(1) = \varepsilon(e_1) + \varepsilon(e_2) = \varepsilon(e_2)$. Como $e_2 = a\widehat{G}$ para algún $a \in R$, tenemos que $a\varepsilon(\widehat{G}) = 1$, luego $a|G| = 1$. Esto muestra que $|G|$ es invertible en R y que $|G|^{-1} = a$. □

Estamos listos para determinar condiciones suficientes y necesarias sobre R y G para que el anillo de grupo RG sea semisimple. Varios resultados en este sentido, en relación con grupos finitos de transformaciones, fueron obtenidos en 1898-1899 por Heinrich Maschke (1853-1908) un estudiante de Félix Klein que emigró a los Estados Unidos y se unió a Oskar Bolza y a Eliakim Hastings Moore para formar el Departamento de Matemáticas de la Universidad de Chicago.

Teorema 1.4.8 (Teorema de Maschke)**.** *Sea G un grupo. Entonces el anillo de grupo RG es semisimple si y solo si se cumplen las siguientes condiciones:*

(*i*) *R es un anillo semisimple.*

(*ii*) *G es finito.*

(*iii*) *$|G|$ es invertible en R.*

Demostración. $\boxed{\Longrightarrow}$: Asumimos que RG es semisimple. Sabemos que $R \cong RG/\Delta(G)$ (Corolario 1.3.5). Como los anillos cocientes de anillos semisimples son semisimples, se sigue que R lo es. La semisimplicidad de RG implica que $\Delta(G)$ es un sumando directo y así el Lema 1.4.7 nos muestra que se cumplen también las condiciones (ii) y (iii).

$\boxed{\Longleftarrow}$: Por el otro lado, si asumimos como ciertas las condiciones (i), (ii) y (iii) y si M es un RG-submódulo cualquiera de RG, entonces existe un R-submódulo N de RG tal que

$$RG = M \oplus N.$$

Sea $\pi : RG \to M$ la proyección canónica asociada a la suma directa. Definimos $\pi^* : RG \to M$ como el R-homomorfismo que se obtiene sacando el promedio:

$$\pi^*(x) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gx), \text{ para todo } x \in RG.$$

Si probamos que π^* es un RG-homomorfismo tal que $(\pi^*)^2 = \pi^*$ y $Im(\pi^*) = M$, entonces $Ker(\pi^*)$ será un RG-submódulo tal que $RG = M \oplus Ker(\pi^*)$ y el teorema estará probado. Como π^* ya es R-homorfismo, para ver que es también RG-homomorfismo bastará probar que:

$$\pi^*(ax) = a\pi^*(x), \text{ para todo } x \in G, \text{ y para todo } a \in G.$$

Tenemos que

$$\pi^*(ax) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gax) = \frac{a}{|G|} \sum_{g \in G} (ga)^{-1}\pi((ga)x).$$

Ahora, cuando g recorre todos los elementos de G, el producto ga también recorre todos los elementos de G, luego

$$\pi^*(ax) = a\frac{1}{|G|} \sum_{t \in G} t^{-1}\pi(tx) = a\pi^*(x).$$

Como π es una proyección en M, sabemos que $\pi(m) = m$, para todo m elemento de M. Además, como M es un RG-módulo, sabemos que $gm \in M$, para todo g elemento de G. Así,

$$\pi^*(m) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gm) = \frac{1}{|G|} \sum_{g \in G} g^{-1}gm = m.$$

Dado un elemento arbitrario x en RG, tenemos que $\pi(gx) \in M$, luego $\pi^*(x) \in M$ y se sigue que $Im(\pi^*) \subseteq M$. Consecuentemente, $\pi^*(\pi^*(x)) = \pi^*(x)$ para todo x elemento de RG, y así, $(\pi^*)^2 = \pi^*$.

Por último, el hecho de que $\pi^*(m) = m$ para todo $m \in M$ también implica que $M \subseteq Im(\pi^*)$ y se sigue el resultado. □

El caso en que R es un cuerpo es de importancia significativa, tanto por razones históricas como por sus implicaciones en teoría de representación. En este caso, R es siempre semisimple y $|G|$ es invertible en R siempre que $|G| \neq 0$ en R, esto es, si y solo si $char(R) \nmid |G|$. Como consecuencia directa tenemos el siguiente resultado:

Corolario 1.4.9. *Sea G un grupo finito y K un cuerpo. Entonces KG es semisimple si y solo si $char(K) \nmid |G|$*

Una adaptación del Teorema de Wedderburn-Artin a este contexto nos dará mucha información sobre la estructura de un álgebra de grupo. Éste es el Teorema de Maschke original y, de hecho, antes de Maschke, el resultado fue demostrado por Molien

Teorema 1.4.10. *Sea G un grupo finito y K un cuerpo tal que $char(K) \nmid |G|$. Entonces:*

(i) KG está en suma directa formada por una cantidad finita de ideales bilateros $\{B_i\}_{1\leq i\leq r}$, los componentes simples de RG. Cada B_i es un anillo simple.

(ii) Cada ideal bilátero de KG está en suma directa dada por miembros de la familia $\{B_i\}_{1\leq i\leq r}$.

(iii) Cada componente simple $\{B_i\}$ es isomorfa a un anillo de matrices de la forma $M_{n_i}(D_i)$, donde D_i es un anillo de división que contiene una copia isomorfa a K en su centro, y el isomorfismo

$$KG \overset{\phi}{\cong} \bigoplus_{i=1}^{r} M_{n_i}(D_i)$$

es un isomorfismo de K-álgebras.

Corolario 1.4.11. *Sean G un grupo finito y K un cuerpo algebraicamente cerrado tal que $char(K) \nmid |G|$. Entonces:*

$$KG \cong \bigoplus_{i=1}^{r} M_{n_i}(K)$$

y además $n_1^2 + n_2^2 + ... + n_r^2 = |G|$.

Demostración. Como $char(K) \nmid |G|$, tenemos que

$$KG \cong \bigoplus_{i=1}^{r} M_{n_i}(D_i) \tag{1.4.12}$$

donde D_i es un anillo de división que contiene una copia de K en su centro. Si calculamos la dimensión sobre K en ambos lados de (1.4.12), tenemos que

$$|G| = \sum_{i=1}^{r} n_i^2 [D_i : K],$$

y se sigue que cada anillo de división tiene dimensión finita sobre K. Como K es algebraicamente cerrado, tenemos que $D_i = K$ para todo i con $1 \leq i \leq r$, y se sigue el resultado. □

1.5. Álgebras de grupo abelianas

En esta sección daremos una descripción completa del anillo de grupo correspondiente a un grupo finito abeliano G sobre un cuerpo K tal que $char(K) \nmid |G|$. Esta caracterización fue dada por primera vez que S. Perlis y G. Walker [19]. La prueba elemental que mostraremos apareció por primera vez en [8].

Comenzaremos con el caso en que G es cíclico, $G =< a : a^n = 1 >$ y K es un cuerpo tal que $char(K) \nmid |G|$. Consideramos la aplicación $\phi : K[X] \to KG$ dada por:

$$K[X] \ni f \mapsto f(a) \in KG$$

Es fácil ver que ϕ es un epimorfismo de anillos. Así:

$$KG \cong \frac{K[X]}{Ker(\phi)},$$

donde $Ker(\phi) = \{f \in K[X] : f(a) = 0\}$. Como $K[X]$ es un dominio de ideales principales, $Ker(\phi)$ es el ideal generado por el polinomio mónico f_0 de menor grado tal que $f_0(a) = 0$. Es importante recordar, para posterior uso, que bajo este isomorfismo el elemento a tiene como imagen la clase $X + (f_0) \in \frac{K[X]}{(f_0)}$.

Como $a^n = 1$, se sigue que $X^n - 1 \in Ker(\phi)$. Nótese que si $f = \sum_{i=0}^{r} k_i X^i$ es un polinomio de grado $r < n$, tenemos que $f(a) = \sum_{i=0}^{r} k_i a^i$ es distinto de 0, porque los elementos $\{1, a, a^2, ..., a^r\}$ son linealmente independientes sobre K. Entonces $Ker(\phi) = (X^n - 1)$, así que

$$KG \cong \frac{K[X]}{(X^n - 1)}.$$

Sea $X^n - 1 = f_1 f_2 \cdots f_t$ la descomposición de $X^n - 1$ en polinomios mónicos irreducibles en $K[X]$. Como estamos asumiendo que $char(K) \nmid n$, este polinomio es separable y así, $f_i \neq f_j$ si $i \neq j$. Usando el Teorema Chino de los Restos,

$$KG \cong \frac{K[X]}{(f_1)} \oplus \frac{K[X]}{(f_2)} \oplus \cdots \oplus \frac{K[X]}{(f_t)}$$

Bajo este isomorfismo, el generador a va al elemento

$$(X + (f_1), ..., X + (f_t)).$$

Tomamos como ζ_i una raíz de f_i, con $1 \leq i \leq t$. Entonces tenemos que $\frac{K[X]}{(f_i)} \cong K(\zeta_i)$. Como consecuencia

$$KG \cong K(\zeta_1) \oplus K(\zeta_2) \oplus \cdots \oplus K(\zeta_t).$$

Y como todas las ζ_i son raíces de $X^n - 1$, hemos mostrado que KG es isomorfo a una suma directa de **extensiones ciclotómicas** de K. Bajo este último isomorfismo, el elemento a va a $(\zeta_1, \zeta_2, ..., \zeta_t)$.

Veamos algún ejemplo:

- Si fijamos $G =< a : a^{13} = 1 >$ y $K = \mathbb{Q}$, tenemos que la descomposición irreducible de $X^{13} - 1$ en $\mathbb{Q}[X]$ es

  $$X^{-13} - 1 = (X - 1)(X^{12} + X^{11} + ... + X + 1)$$

  y así, si ζ denota una raíz primitiva de orden 13 de la unidad, tenemos

  $$\mathbb{Q}G \cong \mathbb{Q} \oplus \mathbb{Q}(\zeta)$$

- Fijando $G =< a : a^{13} = 1 >$ y $K = \mathbb{Q}$, tenemos que la descomposición irreducible de $X^{12} - 1$ en $\mathbb{Q}[X]$ es

  $$(X - 1)(X^2 + X + 1)(X + 1)(X^2 - X + 1)(X^2 + 1)(X^4 - X^2 + 1)$$

  y así, tenemos

  $$\mathbb{Q}G \cong \mathbb{Q} \oplus \mathbb{Q}\left(\frac{-1 + i\sqrt{3}}{2}\right) \oplus \mathbb{Q} \oplus \mathbb{Q}\left(\frac{1 + i\sqrt{3}}{2}\right) \oplus \mathbb{Q}(i) \oplus \mathbb{Q}\left(\frac{\sqrt{3} + i}{2}\right)$$

  Aquí $\frac{-1+i\sqrt{3}}{2}$ es una raíz de $X^2 + X + 1$, $\frac{1+i\sqrt{3}}{2}$ es una raíz de $X^2 - X + 1$ y $\frac{\sqrt{3}+i}{2}$ es una raíz de $X^4 - X^2 + 1$. Nótese que el segundo y el cuarto sumando son el mismo cuerpo.

Queremos dar una descripción más precisa de KG en el caso general. Para esto, trataremos de calcular los sumandos directos en la descomposición de KG. Recordamos que, dado un entero positivo d, el **polinomio ciclotómico** de orden d, que denotamos por Φ_d, es el producto $\Phi_d = \Pi_j(X - \xi_j)$, donde ξ_j recorre las raíces d-ésimas primitivas de la unidad. Además, sabemos que $X^n - 1 = \Pi_{d|n}\phi_d$, el producto de todos los polinomios ciclotómicos Φ_d en $K[X]$, para todo d divisor de n. Para cada d, sea $\Phi_d = \Pi_{i=1}^{a_d} f_{d_i}$ la descomposición de Φ_d como producto de polinomios irreducibles en $K[X]$.

Entonces, la descomposición de KG puede realmente ponerse de la siguiente forma:

$$KG \cong \oplus_{d|n} \oplus_{i=1}^{a_d} \frac{K[X]}{(f_{d_i})} \cong \oplus_{d|n} \oplus_{i=1}^{a_d} K(\zeta_{d_i}),$$

donde ζ_{d_i} denota una raíz de f_{d_i}, para $1 \leq i \leq a_d$. Si fijamos d, todos los elementos ζ_{d_i} son raíces primitivas d-ésimas de la unidad. De esta forma, todos los cuerpos de la forma $K(\zeta_{d_i})$, con $1 \leq i \leq a_d$ son iguales entre sí y podemos escribir

$$KG \cong \oplus_{d|n} a_d K(\xi_d),$$

donde ξ_d es una raíz primitiva de la unidad de orden d y $a_d K(\xi_d)$ denota la suma directa de a_d cuerpos distintos, todos ellos isomorfos a $K(\xi_d)$. Además, como el grado de f_{d_i} es $[K(\xi_d) : K]$, vemos que todos los polinomios f_{d_i}, con $1 \leq i \leq a_d$, tienen el mismo grado. Así, tomando grados en la descomposición de Φ_d, obtenemos

$$\phi(d) = a_d[K(\xi_d) : K]$$

donde ϕ denota la **función indicatriz de Euler**[1]

Como G es un grupo cíclico de orden n, para cada divisor d de n el número de elementos de orden d en G, que denotamos por n_d, es precisamente $\phi(d)$. Así, podemos escribir

$$a_d = \frac{n_d}{[K(\xi_d) : K]}$$

Con esto, podemos generalizar los ejemplos anteriores:

- Sea $G =< a : a^n = 1 >$un grupo cíclico de orden n y consideremos $K = \mathbb{Q}$. Es bien sabido que el polinomio $X^n - 1$ se descompone en $\mathbb{Q}[X]$ como producto de polinomios ciclotómicos

  $$X^n - 1 = \Pi_{d|n} \Phi_d(X)$$

  y estos son irreducibles. Así, en este caso la descomposición de $\mathbb{Q}G$ es

  $$\mathbb{Q}G \cong \oplus_{d|n} \mathbb{Q}(\xi_d)$$

  Nótese que, igual que antes, en este isomorfismo el generador a se corresponde con la tupla cuyas entradas son las raíces d-ésimas primitivas de la unidad, cuando d recorre los divisores de n (con una raíz por cada d).

Podemos extender la descripción dada para anillos de grupo con grupos cíclicos a anillos de grupo con grupos abelianos finitos en general:

[1] Podemos escribir esta función de forma sencilla como $\phi(d) = |\{n \in \mathbb{N} : n \leq d \text{ y } mcd(d, n) = 1\}|$, aunque se presupone que el lector ya la conoce.

Teorema 1.5.1 (Perlis-Walker[19]). *Sea G un grupo abeliano finito de orden n y K un cuerpo tal que $char(K) \nmid n$. Entonces:*

$$KG \cong \underset{d|n}{\oplus} a_d K(\xi_d)$$

donde ξ_d denota una raíz primitiva d-ésima de la unidad y $a_d = \frac{n_d}{[K(\xi_d):K]}$. En esta fórmula, n_d denota el número de elementos de orden d en G.

Demostración. Procedemos por inducción en el orden de G. Asumimos que el resultado se cumple para todos los grupos abelianos de orden menor que n.

Si G es cíclico, ya hemos visto que el teorema es válido, pues aquí $n_d = \phi(d)$. En otro caso, podemos usar el Teorema de estructura de grupos abelianos finitos para escribir $G = G_1 \times H$, donde H es cíclico y $|G_1| = n_1 < n$. Por la hipótesis de inducción, podemos escribir $KG_1 \cong \underset{d_1|n_1}{\oplus} a_{d_1} K(\xi_{d_1})$, donde $a_{d_1} = \frac{n_{d_1}}{[K(\xi_{d_1}):K]}$ y n_{d_1} denota el número de elementos de orden d_1 en G_1. Así, tenemos:

$$KG = K(G \times H) \cong (KG_1)H \cong \left(\underset{d_1|n_1}{\oplus} a_{d_1} K(\xi_{d_1}) \right) H \cong \underset{d_1|n_1}{\oplus} a_{d_1} K(\xi_{d_1}) H,$$

ahora, descomponiendo cada sumando directo, obtenemos

$$KG \cong \underset{d_1|n_1}{\oplus} \underset{d_2||H|}{\oplus} a_{d_1} a_{d_2} K(\xi_{d_1}, \xi_{d_2}),$$

donde $a_{d_2} = \frac{n_{d_2}}{[K(\xi_{d_1},\xi_{d_2}):K(\xi_{d_1}]}$ y n_{d_2} denota el número de elementos de orden d_2 en H. Si tomamos $d = mcm(d_1, d_2)$, tenemos que $K(\xi_{d_1}, \xi_{d_2}) = K(\xi_d)$. Así,

$$KG \cong \underset{d|n}{\oplus} a_d K(\xi_d),$$

con $a_d = \sum a_{d_1} a_{d_2}$, donde la suma se toma sobre todos los pares d_1, d_2 tales que $mcm(d_1, d_2) = d$. Ahora, como $[K(\xi_d) : K] = [K(\xi_{d_1}, \xi_{d_2}) : K(\xi_{d_1})][K(\xi_{d_1}) : K]$, tenemos que

$$a_d[K(\xi_d) : K] = \sum_{d_1,d_2} a_{d_1} a_{d_2} [K(\xi_{d_1}, \xi_{d_2}) : K(\xi_{d_1})][K(\xi_{d_1}) : K] = \sum_{d_1,d_2} n_{d_1} n_{d_2}$$

Por último, como se tiene que $G = G_1 \times H$, entonces cada elemento g de G puede escribirse de la forma $g = g_1 h$, con $g_1 \in G_1$ y $h \in H$. Además, al escribir g de esa forma se tiene que $o(g) = mcm(o(g_1), o(h))$. Así, se tiene que $\sum_{d_1,d_2} n_{d_1} n_{d_2} = n_d$, el número de elementos de orden d en G, de forma que tenemos que:

$$a_d = \frac{n_d}{[K(\xi_d) : K]}$$

y se sigue el resultado. □

Corolario 1.5.2. *Sea G un grupo abeliano finito de orden n. Entonces,*

$$\mathbb{Q}G \cong \underset{d|n}{\oplus} a_d \mathbb{Q}(\xi_d)$$

donde ξ_d denota una raíz primitiva d-ésima de la unidad y a_d es el número de subgrupos cíclicos de orden d de G.

Demostración. Hemos visto en el Teorema 1.5.1 que $a_d = \frac{n_d}{[\mathbb{Q}(\xi_d),\mathbb{Q}]}$, donde n_d es el número de elementos de orden d en G.

Ahora, $[\mathbb{Q}(\xi_d),\mathbb{Q}] = \phi(d)$, donde ϕ denota la función de Euler. Nótese que el número de generadores de un grupo cíclico de orden d es precisamente $\phi(d)$, porque $< \alpha >=< \alpha^n >$ si y solo si $mcd(o(\alpha), n) = 1$ $\left(\text{esto se puede ver fácilmente usando la fórmula } o(\alpha^n) = \frac{o(\alpha)}{mcd(o(\alpha),n)}\right)$. Así, $n_d/\phi(d)$ es el número de subgrupos cíclicos de orden d en G. □

Corolario 1.5.3. *Sea G un grupo abeliano de orden n y K un cuerpo tal que $char(K) \nmid n$. Si K contiene una raíz primitiva de la unidad de orden n, entonces*

$$KG \cong \underbrace{K \oplus \cdots \oplus K}_{n}$$

Demostración. Si K contiene una raíz primitiva de la unidad de orden n, entonces $K(\zeta_d) = K$, para todo d entero divisor de n y el resultado se sigue directamente del Teorema 1.5.1. Para ver que ha de haber exactamente n sumandos es suficiente calcular las dimensiones sobre K en ambos lados de la ecuación. □

Si G y H son grupos isomorfos, es obvio que las álgebras de grupo respectivas RG y RH sobre cualquier anillo R serán también isomorfas. Sin embargo, el recíproco no es cierto siempre. Estamos ya listos para dar un primer ejemplo negativo en el que no se da el recíproco.

Si G y H son dos grupos abelianos no isomorfos del mismo orden n y K es un cuerpo tal que $char(K)$ no divide a n, que además contiene una raíz primitiva n-ésima de la unidad, entonces el Corolario 1.5.3 muestra que:

$$KG \cong \underbrace{K \oplus \cdots \oplus K}_{\text{n}} \cong KH$$

Por ejemplo, si C_n denota el grupo cíclico de orden n, entonces para las álgebras de grupo

complejas siguientes sucede que:

$$\mathbb{C}(C_2 \times C_2) \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \cong \mathbb{C}C_4, \text{ pero } C_2 \times C_2 \ncong C_4$$

Este es nuestro primer resultado negativo del *Problema del Isomorfismo*, que podemos enunciar de forma breve como sigue: **¿Bajo qué condiciones sobre R y G sucede que $\mathbf{RG \cong RH \Rightarrow G \cong H}$?**

Este problema será el tema principal del trabajo y lo trataremos en profundidad en el tercer capítulo de este trabajo.

2- Estructura y elementos relevantes de las álgebras de grupo

- Comenzaremos este capítulo dando una descripción del centro de un álgebra de grupo.
- Esta información será importante para determinar la estructura de un álgebra de grupo semisimple. Para éstas, también trabajaremos con la suma de los componentes simples, información que será importante en determinar la estructura de ejemplos concretos.
- En la segunda parte del capítulo, estudiaremos algunos elementos algebraicos en álgebras de grupo usando la representación regular (que veremos en detalle) y demostraremos un importante teorema de Higman.
- Continuaremos demostrando un teorema de Passman y usándolo para obtener unos resultados relacionados con la Conjetura de Kaplansky. Acabaremos el capítulo enunciando esta conjetura.

2.1. Álgebras de grupo semisimples: Estructura

Comencemos definiendo unos elementos de RG que tendrán especial importancia en la estructura del centro del anillo de grupo.

Definición 2.1.1. *Sea G un grupo, R un anillo conmutativo y $\{C_i\}_{i\in I}$ el conjunto de las clases de conjugación de G que contienen solo una cantidad finita de elementos. Para cada $i \in I$, sea $\gamma_i = \widehat{C_i} = \sum_{x\in C_i} x$, considerado como elemento de RG. Llamamos a estos elementos las **sumas de clase** de G sobre R.*

Teorema 2.1.2. *Sea G un grupo y R un anillo conmutativo. Entonces el conjunto $\{\gamma_i\}_{i\in I}$ de las sumas de clase forma una base de $\mathcal{Z}(RG)$, el centro de RG, sobre R.*

Demostración. Primero notemos que dado un elemento arbitrario g en G, se tiene que $g^{-1}\gamma_i g = \sum_{x\in C_i} g^{-1}xg$. Como la conjugación por g es un automorfismo de G que mantiene las sumas de clases (esto es, para i en I arbitrario se tiene que $C_i^g = C_i$), entonces $\sum_{x\in C_i} g^{-1}xg = \sum_{y\in C_i} y = \gamma_i$. Así, para todo elemento $g \in G$ se tiene que $\gamma_i g = g\gamma_i$, mostrando que γ_i pertenece a $\mathcal{Z}(RG)$ para cualquier elemento i de I.

Por otro lado, se tiene que estos elementos son linealmente independientes sobre R, porque tienen soportes disjuntos. Finalmente, tomemos a en $\mathcal{Z}(RG)$. Tenemos que probar que si g está en $supp(a)$, entonces cualquier otro elemento h de G que esté en la clase de conjugación de g cumple que $a_g = a_h$. Así, tomamos $h = x^{-1}gx$ para cierto x elemento de G. Como a es central, tenemos que $a = x^{-1}ax$. Esto es,

$$\sum_{g\in G} a(g)g = \sum_{g\in G} a(g)x^{-1}gx.$$

Comparando el coeficiente de h en ambos lados de la ecuación, tenemos que $a_g = a_h$. Esto muestra que podemos factorizar los coeficientes de los elementos en cada clase de conjugación y escribir

$$a = \sum_{i\in I} a_i\gamma_i$$

Así, $\{\gamma_i\}_{i\in I}$ es también un conjunto generador de $\mathcal{Z}(RG)$ y hemos acabado. □

Proposición 2.1.3. *Sean G un grupo finito y K un cuerpo algebraicamente cerrado de forma que $char(K)$ no divide a $|G|$. Entonces, el número de componentes simples de KG es igual al número de clases de conjugación de G.*

Demostración. Usando el Teorema 2.1.2, será suficiente mostrar que en el caso presente la dimensión de $\mathcal{Z}(RG)$ sobre K es igual al número de componentes simples de KG. Por el Corolario 1.4.11 sabemos que

$$KG \cong \bigoplus_{i=1}^{r} M_{n_i}(K)$$

y así,

$$\mathcal{Z}(KG) \cong \bigoplus_{i=1}^{r} \mathcal{Z}(M_{n_i}(K))$$

Es fácil ver que para un anillo de matrices $M_n(K)$,

$$\mathcal{Z}(M_n(K)) = \{\alpha I : \alpha \in K\}$$

y así, $\mathcal{Z}(M_n(K)) \cong K$. Por ello,

$$\mathcal{Z}(KG) \cong \underbrace{K \oplus \cdots \oplus K}_{r \text{ veces}} \cong K^r;$$

Como consecuencia, $[\mathcal{Z}(KG) : K] = r$. □

Nótese que la hipótesis de que K sea algebraicamente cerrado solo se ha usado porque con ella tenemos que $D_i = K$, para $1 \leq i \leq r$. Esto puede pasar en otros cuerpos no algebraicamente cerrados.

Definición 2.1.4. *Un cuerpo K es llamado **cuerpo de escisión** para un grupo finito G si el álgebra de grupo KG es isomorfa a una suma directa de anillos de matrices sobre K.*

Es claro que la Proposición 2.1.3 se cumple siempre que K sea un cuerpo de escisión para G. Como hemos visto, los cuerpos algebraicamente cerrados son cuerpos de escisión para cualquier grupo G finito, pero no tiene por qué darse siempre el recíproco. De hecho, si n es el orden de un grupo finito G, entonces $\mathbb{Q}(\zeta_n)$ es un cuerpo de escisión de G, siendo ζ_n una raíz primitiva n-ésima de la unidad. Esto es consecuencia del **Teorema de Escisión de Brauer**, que puede consultarse en [4].

Por otro lado, sabemos que si e es un elemento idempotente y central en un anillo R, entonces induce una descomposición de R como suma directa de ideales biláteros: $R = R(e) \oplus R(1-e)$. Hay una forma estándar de construir idempotentes en un anillo de grupo a partir de los subgrupos del grupo dado.

Lema 2.1.5. *Sean R un anillo con unidad y H un subgrupo de un grupo G. Si $|H|$ es invertible en R, entonces $\bar{H} = \frac{1}{|H|}\widehat{H}$ es un elemento idempotente de RG. H es un subgrupo normal de G si y solo si $\bar{H}$ es central.*

Demostración. $\bar{H}$ es idempotente:

$$\bar{H}\bar{H} = \frac{1}{|H|^2}\widehat{H}\widehat{H} = \frac{1}{|H|^2}(\sum_{h\in H} h)\widehat{H} = \frac{1}{|H|^2}\sum_{h\in H}(h\widehat{H}) = \frac{1}{|H|^2}\sum_{h\in H}\widehat{H} = \frac{1}{|H|^2}|H|\widehat{H} = \bar{H}$$

Y ya sabemos, por la Proposición 1.4.3, que H es un subgrupo normal de G si y solo si $\widehat{H}$ es central, así que el resultado se sigue inmediatamente. □

El siguiente resultado nos dice qué forma tiene la descomposición obtenida de uno de estos idempotentes.

Proposición 2.1.6. *Sean R un anillo y H un subgrupo normal de un grupo G. Si $|H|$ es invertible en R y $\bar{H} = \frac{1}{|H|}\widehat{H}$, tenemos una suma directa de anillos:*

$$RG = RG(\bar{H}) \oplus R(1-\bar{H})$$

donde

$$RG(\bar{H}) \cong R(G/H) \text{ y } R(1-\bar{H}) = \Delta(G,H)$$

Demostración. Como hemos mostrado en el Lema 2.1.5 que $\bar{H}$ es un idempotente central, queda claro que $RG = RG(\bar{H}) \oplus RG(1-\bar{H})$. Para ver que $RG(\bar{H}) \cong R(G/H)$ primero veremos que $G/H \cong G(\bar{H})$ como grupos. De hecho, es fácil ver que la aplicación $\phi : G \to G(\bar{H})$ dada por $g \mapsto g\bar{H}$ es un epimorfismo de grupos. Como $Ker(\phi)) = H$, ya tenemos el resultado. Ahora, como $G(\bar{H})$ es un conjunto generador de $RG(\bar{H})$ sobre R, tenemos claramente que $RG(\bar{H}) \cong R(G/H)$.

Finalmente, se sigue del Lema 1.4.6 que $RG(1-\bar{H})$ es el anulador de $RG(\bar{H})$ (por ambos lados) y puede mostrarse fácilmente, operando de la misma manera que en la demostración del Lema 1.4.4, que $Ann_r(RG(\bar{H})) = Ann_l(RG(\bar{H})) = \Delta(G,H)$. □

Definición 2.1.7. *Sean R un anillo y G un grupo finito tal que $|G|$ es invertible en R. El idempotente $\bar{G} = \frac{1}{|G|}\widehat{G}$ es llamado* ***idempotente principal*** *de RG.*

Como consecuencia inmediata de la Proposición 2.1.6, usando el idempotente principal de RG podemos mostrar que las álgebras de grupo semisimples siempre contienen al menos un componente simple, isomorfo al anillo de coeficientes.

Corolario 2.1.8. *Sean R un anillo y G un grupo finito tal que $|G|$ es invertible en R. Entonces podemos escribir RG como suma directa de anillos*

$$RG \cong R \oplus \Delta(G).$$

De ahora en adelante denotaremos como G' el **subgrupo conmutador** de G, esto es, el subgrupo generado por todos los elementos de la forma $(g,h) = g^{-1}h^{-1}gh$, con g y h en G. Para probar el último resultado de la sección necesitaremos un lema auxiliar:

Lema 2.1.9. *Sea I un ideal de un álgebra de grupo RG siendo R un anillo conmutativo. Entonces el anillo cociente RG/I es conmutativo si y solo si $\Delta(G,G') \subseteq I$.*

Demostración. $\boxed{\Longrightarrow}$: Sea I un ideal en RG tal que RG/I es conmutativo. Entonces para cualesquiera g,h elementos de G tenemos que $gh - hg \in I$, luego también se cumple que $hg(g^{-1}h^{-1}gh - 1) \in I$. Como hg es invertible, también tenemos que $g^{-1}h^{-1}gh - 1 = (g,h) - 1$ es un elemento de I. Se sigue del Lema 1.3.2 que $\Delta(G,G') \subseteq I$.

$\boxed{\Longleftarrow}$: Como $gh - hg = hg((g,h) - 1)$ está en $\Delta(G,G')$, entonces si $\Delta(G,G') \subseteq I$, tenemos que para cualesquiera $g,h \in G$ se cumple que $gh \equiv hg \pmod{I}$ y así se tiene que RG/I es conmutativo. □

Proposición 2.1.10. *Sea RG un álgebra de grupo semisimple. Podemos escribir*

$$RG = RG(\bar{G'}) \oplus \Delta(G,G'),$$

donde $RG(\bar{G'}) \cong R(G/G')$ es la suma de todos las componentes simples conmutativas de RG y $\Delta(G,G')$ es la suma de las demás.

.

Demostración. Tanto el hecho de que RG pueda descomponerse de la forma escrita como el hecho de que $RG(\bar{G}') \cong R(G/G')$ se siguen de la Proposición 2.1.6.

Es claro que $RG(\bar{G}') \cong R(G/G')$ es conmutativo, así que es ciertamente suma de componentes simples conmutativas de RG. Para completar la prueba es suficiente mostrar que no hay componentes simples conmutativas en $\Delta(G, G')$. Así, asumamos que podemos poner $\Delta(G, G') = A \oplus B$, con A una componente simple conmutativa y B su complementario. Entonces $RG = RG(\bar{G}') \oplus A \oplus B$, así que tenemos que $RG/B \cong RG(\bar{G}') \oplus A$, que es conmutativo. Se sigue del Lema 2.1.9 que $\Delta(G, G') \subseteq B$, una contradicción. □

Veamos un par de ejemplos:

- Sea S_3 el grupo de las permutaciones de 3 elementos y queremos describir su álgebra de grupo sobre $\mathbb{Q}$. Tenemos que $S_3' = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$, luego $|S_3/S_3'| = 2$. Por ello, $\mathbb{Q}(S_3/S_3')$ es de dimensión 2 sobre $\mathbb{Q}$. Ahora, como acabamos de ver que siempre va a contener al menos una componente isomorfa a $\mathbb{Q}$, vemos que $\mathbb{Q}S_3$ contiene exactamente dos componentes conmutativas simples: ambas isomorfas a $\mathbb{Q}$. Como la dimensión de $\Delta(S_3, S_3')$ es al menos 4 y la dimensión de todo el álgebra de grupo sobre $\mathbb{Q}$ es $|S_3| = 6$, tenemos que ha de ser:

$$\mathbb{Q}S_3 = \mathbb{Q} \oplus \mathbb{Q} \oplus B,$$

  donde B es una componente conmutativa simple de dimensión 4 sobre $\mathbb{Q}$. Dado que $\mathbb{Q}S_3$ contiene elementos nilpotentes (por ejemplo $\mu = (1 + (2\ 3))(1\ 2\ 3)(1 - (2\ 3))$ cumple $\mu^2 = (1 + (2\ 3))(1\ 2\ 3)(1 - (2\ 3))(1 + (2\ 3))(1\ 2\ 3)(1 - (2\ 3)) = (...)(1 + (2\ 3) - (2\ 3) - (2\ 3)(2\ 3)(...) = (...)(1 - 1)(...) = 0$), entonces no puede ser suma directa de anillos de división, luego tenemos solo una posibilidad

$$\mathbb{Q}S_3 = \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q})$$

  Así que se sigue por la fuerza que $\mathbb{Q}$ es también un cuerpo de escisión para S_3.

2.2. Álgebras de grupo: Representación regular

En esta sección trataremos con la representación regular de un álgebra de grupo.

Dada un álgebra A de dimensión finita y con unidad, sobre un cuerpo K; definimos una aplicación $T : A \to Hom_K(A, A)$ asignando a cada elemento $a \in A$ la aplicación $T_a(x) = ax$, para cada $x \in A$. Vemos fácilmente que, para $a, b \in A$ arbitrarios y cualquier $k \in K$ se tiene:

$$T_{a+b} = T_a + T_b$$
$$T_{ab} = T_a T_b$$
$$T_{ka} = kT_a$$

Más aún, la aplicación $a \mapsto T_a$ es inyectiva, pues $T_a(1) = a$. Escogiendo una base $\{a_1, a_2, ..., a_n\}$ de A sobre K, podemos representar T_a por una matriz $\rho(a) \in M_n(K)$, luego tenemos también una representación matricial:

$$a \mapsto \rho(a) \in M_n(K)$$

Si a es un elemento algebraico de A, esto es, si existe $f(X)$ en $K[X]$ tal que $f(a) = 0$, entonces los autovalores de la matriz $\rho(a)$ también satisfacen $f(X)$. Así, por ejemplo, si a es un elemento nilpotente, entonces todos los autovalores de $\rho(a)$ son cero y si a tiene orden (multiplicativo) m, entonces todos los autovalores de $\rho(a)$ son raíces m-ésimas de la unidad.

Lema 2.2.1. *Sean G un grupo finito y K un cuerpo. Si ρ es la representación regular de KG y sea $\gamma = \sum_{g \in G} \gamma(g)g \in KG$. Entonces, la traza de $\rho(\gamma)$ viene dada por*

$$tr\rho(\gamma) = |G|\gamma(1).$$

Demostración. Sabemos que $tr\rho(\gamma)$ es independiente de la base elegida, así que tomamos $G = \{g_1, g_2, ..., g_n\}$ como K-base de KG. Entonces,

$$\rho(\gamma) = \rho\left(\sum_{g \in G} \gamma(g)g\right) = \sum_{g \in G} \gamma(g)\rho(g).$$

Para un elemento $g \neq 1$ de G, tenemos que $gg_i \neq g_i$, para todo i. Se sigue entonces que la diagonal de la matriz $\rho(g)$ es nula. Así, $tr\rho(g) = 0$, para todo $g \neq 1$. Más aún, como $\rho(1)$ es la matriz identidad, tenemos que $tr\rho(1) = n$. Luego se tiene que

$$tr\rho(\gamma) = \sum_{g \in G} \gamma(g) tr\rho(g) = \gamma(1) tr\rho(1) = \gamma(1)|G|,$$

como pedíamos. □

El Lema 2.2.1 tendrá muchas aplicaciones, entre ellas el siguiente resultado de Berman y Higman.

Lema 2.2.2. *Sea $\gamma = \sum_{g\in G} \gamma(g)g$ una unidad de orden finito en el anillo de grupo entero $\mathbb{Z}G$ con G un grupo finito y asumamos que $\gamma(1) \neq 0$. Entonces, $\gamma = \gamma(1) = \pm 1$.*

Demostración. Sea $|G| = n$ y asumamos que $\gamma^m = 1$ para cierto m entero positivo. Consideramos la representación regular ρ del álgebra de grupo $\mathbb{C}G$ y vemos $\mathbb{Z}G$ como subanillo de $\mathbb{C}G$. Entonces $tr\rho(\gamma) = n\gamma(1)$, por el Lema 2.2.1.

Como $\gamma^m = 1$, tenemos que $(\rho(\gamma))^m = \rho(\gamma^m) = I$. Se sigue que $\rho(\gamma)$ es una raíz del polinomio $X^m - 1$, cuyas raíces son todas distintas con multiplicidad 1. Esto implica que existe una base de $\mathbb{C}G$ para la cual la matriz de $\rho(\gamma)$ es diagonal, con la forma:

$$A = \begin{bmatrix} \xi_1 & & & \\ & \xi_2 & & \\ & & \ddots & \\ & & & \xi_n \end{bmatrix} \text{ y } \xi_i^m = 1 \text{ para todo } i.$$

De esta forma, $tr\rho(\gamma) = \sum_{i=1}^{n} \xi_i$ y así

$$n\gamma(1) = \sum_{i=1}^{n} \xi_i.$$

Así, tomando valores absolutos,

$$|n\gamma(1)| = \left|\sum_{i=1}^{n} \xi_i\right| \leq \sum_{i=1}^{n} |\xi_i| = n.$$

Como $|n\gamma(1)| = n|\gamma(1)| \leq n$, debemos tener $|\gamma(1)| = 1$ y además $|\sum_{i=1}^{n} \xi_i| = \sum_{i=1}^{n} |\xi_i|$. Esto pasa si y solo si $\xi_1 = \xi_2 = ... = \xi_n$. Así, $n\gamma(1) = n\xi_1$ y como consecuencia $\gamma(1) = \xi_1 = \pm 1$. Concluimos que $\rho(\gamma) = \pm I$, luego $\gamma = \pm 1$, como afirmábamos. □

Corolario 2.2.3. *Supongamos que $\gamma = \sum_{g\in G} \gamma(g)g$ es una unidad central de orden finito en el anillo de grupo entero $\mathbb{Z}G$ de un grupo finito G. Entonces γ es de la forma $\gamma = \pm g$, con $g \in \mathcal{Z}(G)$.*

Demostración. Sea $\gamma = \sum_{g\in G} \gamma(g)g$ central de orden finito m. Supongamos que $\gamma(g_0)$ para algún $g_0 \in G$. Entonces, γg_o^{-1} es también una unidad de orden finito en $\mathbb{Z}G$. Más aún, tenemos que

el coeficiente de 1 en la expresión de γg_o^{-1} es $\gamma(g_0) \neq 0$. Se sigue del Lema 2.2.2 que $\gamma g_0 = \pm 1$. Así, $\gamma = \pm g_0$. □

Una consecuencia es el famoso Teorema de Graham Higman [10].

Teorema 2.2.4 (Teorema de Higman)**.** *Sea A un grupo abeliano finito. Entonces, el grupo de las unidades de torsión del anillo de grupo $\mathbb{Z}A$ es $\pm A$.*

2.3. Elementos idempotentes

Nos fijaremos ahora en los elementos idempotentes. Por supuesto, en cualquier anillo unitario los elementos 1 y 0 son idempotentes (son los **idempotentes triviales** del anillo). Veremos que los idempotentes e en un álgebra de grupo están fuertemente influenciados por su primer coeficiente $e(1)$, también llamado la **traza** de e.

Teorema 2.3.1. *Sean G un grupo finito y K un cuerpo de característica 0. Supongamos que $e \in KG$ es un elemento idempotente. Entonces*

- $e(1) \in \mathbb{Q}$,
- $0 \leq e(1) \leq 1$,
- $e(1) = 0 \Leftrightarrow e = 0$ *y* $e(1) = 1 \Leftrightarrow e = 1$.

Demostración. Consideremos de nuevo la representación regular ρ de KG, escrita con respecto a la base G de KG. Entonces, por el Lema 2.2.1, tenemos que $tr\rho(e) = |G|e(1)$. Más aún, dado que $e^2 = e$, $\rho(e)$ satisface el polinomio $X^2 - X = X(X-1)$, así que puede diagonalizarse. Los autovalores de $\rho(e)$ han de ser 1 o 0. Como la traza es la suma de los autovalores, tenemos que $tr\rho(e) = r$, donde r es el número de autovalores iguales a 1 y así también es el rango de $\rho(e)$. Concluimos que $e(1) = r/|G|$ es un número racional y además que $0 \leq e(1) \leq 1$.

Nótese que $e(1) = 0$ si y solo si el rango de $\rho(e)$ es 0 y esto ocurre si y solo si $e = 0$. De forma similar, $e(1) = 1$ si y solo si el rango de $\rho(e)$ es precisamente $|G|$ y esto sucede si y solo si $\rho(e)$ es la matriz identidad, luego si y solo si $e = 1$. □

Hemos probado en el Teorema 2.3.1 que si K es un cuerpo de característica 0 y G un grupo finito, entonces cualquier idempotente $e \in KG$ cumple la propiedad de que $e(1) \in \mathbb{Q}$. Daremos ahora un análogo de este resultado para cuerpos de característica $p > 0$ y grupos arbitrarios.

Para ello primero necesitamos introducir la noción de **conmutador de Lie** y demostrar algunos resultados auxiliares.

Definición 2.3.2. *Dados dos elementos x e y en un anillo R, el **conmutador de Lie** de x e y es el elemento $[x, y] = xy - yx$. Denotamos por $[R, R]$ el subgrupo aditivo de R generado por todos los conmutadores de Lie $[x, y]$, $x, y \in R$.*

Queremos calcular $[RG, RG]$ para un grupo G dado y siendo R cualquier anillo conmutativo. Primero observamos que $[RG, RG]$ es de hecho un R-módulo, pues $k[x, y] = [kx, y]$ para todo $k \in R$ y cualesquiera $x, y \in RG$. Dado un elemento $\alpha \in RG$, definimos

$$\varepsilon_g(\alpha) = \sum_{x \in g^G} \alpha(x),$$

donde g^G denota la clase de conjugación de g en G.

Lema 2.3.3. *(i) $[RG, RG]$ es el subespacio R-lineal generado por todos los conmutadores de Lie $[g, h]$, con $g, h \in G$.*

(ii) Si $\alpha \in [RG, RG]$, entonces $\varepsilon_g(\alpha) = 0$ para todo $g \in G$. En particular, $\alpha(z) = 0$ para todo $z \in \mathcal{Z}(G)$.

Demostración. Sean β y γ dos elementos de RG. Entonces,

$$[\beta, \gamma] = [\sum_{g \in G} \beta(g)g, \sum_{g \in G} \gamma(g)g] = \sum_{g,\, h} \beta(g)\gamma(h)[g, h] = \sum_{g,\, h} \beta(g)\gamma(h)(gh - hg).$$

Sea $\alpha \in [RG, RG]$. Entonces, α es combinación lineal de elementos de la forma $(gh - hg)$. Pero $hg = g^{-1}(gh)g$ es conjugado de gh. Se sigue que $\varepsilon_g(\alpha) = 0$ para todo $g \in G$. □

Lema 2.3.4. *Sea R un anillo que tiene como característica un primo p. Entonces, para cualesquiera $x, y \in R$ y n entero positivo, se tiene*

$$(x + y)^{p^n} = x^{p^n} + y^{p^n} + \delta,$$

donde $\delta \in [R, R]$.

Demostración. Veamos el caso $n = 1$:

Cuando expandimos $(x + y)^p$ obtenemos la suma de todos los productos de p elementos de la forma $z_1 z_2 \dots z_p$ donde cada factor z_i es igual a x o y. En particular, hay un término donde todos los factores son x y otro donde todos los factores son y, luego obtenemos una expresión como sigue:

$$(x + y)^p = x^p + y^p + \sum z_1 z_2 \dots z_p, \tag{2.3.5}$$

donde no todos los factores z_i son iguales. Sea $\delta = \sum z_1 z_2 \dots z_p$. Dada una palabra $z_1 z_2 \dots z_p$ en δ, entonces todas sus permutaciones cíclicas

$$z_1 z_2 \dots z_p, \qquad z_2 z_3 \dots z_p z_1, \qquad \cdots \qquad z_p z_1 \dots z_{p-1}$$

también aparecen en δ.

Afirmamos que cada uno de estos elementos difieren del primero por un conmutador de Lie. Dado $z_i z_{i+1} \dots z_p z_1 \dots z_{i-1}$, si ponemos $\alpha = z_i z_{i+1} \dots z_p$ y $\beta = z_1 \dots z_{i-1}$, tenemos que:

$$z_i z_{i+1} \dots z_p z_1 \dots z_{i-1} = \alpha\beta = \beta\alpha + \alpha\beta - \beta\alpha = z_1 z_2 \dots z_p + \alpha\beta - \beta\alpha.$$

Se sigue que la suma de estas permutaciones cíclicas es igual a $p z_1 z_2 \dots z_p$ más un elemento de $[R,\, R]$. Dado que la característica de R es p, la suma está en $[R,\, R]$ y tenemos en (2.3.5) que

$$(x + y)^p = x^p + y^p + \delta, \text{ con } \delta \in [R,\, R]. \tag{2.3.6}$$

Entonces, como consecuencia de (2.3.6) se tiene lo siguiente:

$$\gamma \in [R,\, R] \Rightarrow \gamma^p \in [R, R]. \tag{2.3.7}$$

Para ver esto, nótese que un elemento $\gamma \in [R,\, R]$ es de la forma $\gamma = \sum_i a_i \alpha_i$, con $a_i \in \mathbb{Z}$, y α_i un conmutador de Lie. Por ello, se sigue de la expresión (2.3.6) que $\gamma^p = \sum_i a_i^p \alpha_i^p + \delta$, con $\delta \in [R,\, R]$. Ahora, para cualquier conmutador de Lie $xy - yx \in [R,\, R]$ se tiene que

$$\begin{aligned}(xy - yx)^p &\equiv (xy)^p - (yx)^p \bmod [R,\, R] \\ &\equiv [x, (yx)^{p-1} y] \bmod [R,\, R] \\ &\equiv 0 \bmod [R,\, R].\end{aligned}$$

El resultado se sigue a partir de (2.3.6) y (2.3.7) por inducción en n. □

Ya podemos dar el análogo del Teorema 2.3.1 para cuerpos de característica $p > 0$.

Teorema 2.3.8 (Zalesskii). *Sea K un cuerpo de característica $p > 0$ y G un grupo cualquiera. Si $e \in KG$ es idempotente, entonces $e(1)$ pertenece al subcuerpo primo de K (que por ser de característica p es $\mathbb{Z}/p\mathbb{Z}$, también denotado como $\mathbb{F}_p$).*

Demostración. Sea $e = e^2 = \sum e(g)g \in KG$. Consideremos n un entero positivo lo suficientemente grande como para que todo p-elemento (es decir, cada elemento que tiene como orden una potencia de p) del soporte de e tenga orden menor que p^n. Entonces, por el Lema 2.3.4 tenemos que

$$e = e^{p^n} = \sum e(g)^{p^n} g^{p^n} + \delta, \qquad \delta \in [KG, KG]$$

Ahora computemos el primer coeficiente, $e(1)$, de e. Recordemos que sabemos por el Lema 2.3.3 que $\delta(1) = 0$. Así,

$$e(1) = \sum_{g^{p^n}=1} e(g)^{p^n} + \delta(1) = \sum_{g^{p^n}=1} e(g)^{p^n}.$$

Por la misma razón, tenemos que

$$e(1) = \sum_{g^{p^{n+1}}=1} e(g)^{p^{n+1}} = \sum_{g^{p^n}=1} e(g)^{p^{n+1}} = \left(\sum_{g^{p^n}=1} e(g)^{p^n} \right)^p = e(1)^p.$$

La segunda igualdad se tiene porque para cada p-elemento g en G tal que $e(g) \neq 0$ ocurre que si tiene orden p^m, entonces m es menor que n (por la elección de n) y así $g^{p^m} = 1$ implica que $\left(g^{p^m}\right)^{n-m} = g^{p^n} = 1$. En conclusión, cada sumando no nulo del primer sumatorio también está en el segundo.

Se sigue que $e(1)$ satisface la ecuación $x^p = x$ y así, está en el subcuerpo primo de K, como afirmábamos. □

Habíamos probado el teorema anterior para $p = 0$ en el Teorema 2.3.1 solo para grupos finitos. También es cierto para grupos infinitos, pero la demostración requiere resultados avanzados. Puede consultarse en [17]. Enunciamos el resultado general como sigue:

Teorema 2.3.9 (Zalesskii). *Sea G un grupo arbitrario y K un cuerpo de característica cero. Si e es un elemento idempotente de KG, entonces se tiene que $e(1) \in \mathbb{Q}$.*

El resto de afirmaciones del Teorema 2.3.1 también son ciertas para grupos arbitrarios. Tampoco hacemos la demostración de este resultado, por el mismo motivo. Pueden consultarse en [17] también.

Teorema 2.3.10 (Kaplansky). *Sea G un grupo arbitrario y K un cuerpo de característica cero. Si e es un elemento idempotente de KG, entonces:*

(i) $0 \leq e(1) \leq 1$

(ii) $e(1) = 0 \Leftrightarrow e = 0$ *y* $e(1) = 1 \Leftrightarrow e = 1$

Supongamos que e es idempotente de $\mathbb{Z}G$. Como $e(1)$ es entero, se sigue del Teorema de Kaplansky que es 1 o 0. Así, tenemos lo siguiente:

Corolario 2.3.11. *Sea G un grupo arbitrario. El anillo de grupo entero $\mathbb{Z}G$ contiene únicamente idempotentes triviales.*

2.4. Unidades de torsión

Hemos visto en el Lema 2.2.2 que si G es un grupo finito y $\gamma \in \mathbb{Z}G$ es una unidad de orden finito tal que $\gamma(1) \neq 0$, entonces $\gamma = \pm 1$. Resulta que este resultado es también cierto para grupos infinitos. Probamos esto a continuación.

Teorema 2.4.1 (Passman-Bass). *Sea $\gamma \in \mathbb{Z}G$ tal que $\gamma^n = 1$ para algún n entero positivo. Entonces, si $\gamma(1) \neq 0$ se tiene que $\gamma = \pm 1$.*

Demostración. Sea $\mathbb{C}[X]$ el anillo de polinomios con coeficientes en $\mathbb{C}$. Consideramos el homomorfismo $\varphi : \mathbb{C}[X] \to \mathbb{C}[\gamma]$ dado por $X \mapsto \gamma$. El núcleo de este homomorfismo es el ideal generado por el polinomio mínimo $f(X)$ de γ. Entonces $f(X)$ es divisor de $X^n - 1$ y como tal tiene raíces distintas. Así, tenemos:

$$\mathbb{C}[\gamma] \cong \frac{\mathbb{C}[x]}{< f(X) >} \cong \mathbb{C} \oplus \mathbb{C} \oplus \cdots \oplus \mathbb{C} \cong \oplus_i \mathbb{C} e_i,$$

donde $\{e_i\}_i$ son idempotentes ortogonales y primitivos de $\mathbb{C}[\gamma]$. Podemos escribir γ como[1]

$$\gamma = \sum_i \xi_i e_i \text{ donde } \xi_i \in \mathbb{C},\ \xi_i^n = 1 \text{ y } e_i e_j = \delta_{ij} e_j \text{ siendo } \delta_{ij} \textbf{ la delta de Kronecker}.$$

[1] **La delta de Kronecker**, δ_{ij}, vale 1 si $i = j$ y 0 en caso contrario

Calculando el primer coeficiente en ambos lados de la ecuación y usando el Teorema de Kaplansky de la sección anterior obtenemos

$$\gamma(1) = \sum \xi_i e_i(1) = \sum \xi_i \frac{r_i}{s}, \text{ con } r_i \in \mathbb{Z},\ s \in \mathbb{Z}, \text{ y ambos } r_i, s \geq 0.$$

Entonces, $s\gamma(1) = \sum \xi_i r_i$. Además, como $\sum e_i = 1$, tenemos que $1 = \sum r_i/s$, luego $\sum r_i = s$. Por ello

$$|s\gamma(1)| = |\sum \xi_i r_i| \leq \sum |\xi_i||r_i| = \sum |r_i| = s.$$

Como $|s\gamma(1)| \leq s$, ha de ser $|\gamma(1)| = 1$ y también $|\sum \xi_i r_i| = \sum |\xi_i||r_i|$. Se sigue que todos los ξ_i son iguales y así $\gamma = \sum \xi_1 e_i = \xi_1 = \gamma(1) \in \mathbb{Z}$. Luego $\gamma = \pm 1$. □

El último resultado tiene varias consecuencias útiles. Recordamos que, como vimos en la Proposición 1.2.7, existe una involución dada por

$$\gamma = \sum \gamma(g)g \qquad \mapsto \qquad \gamma^* = \sum \gamma(g)g^{-1},$$

de forma que

$$(\gamma\gamma^*)(1) = \sum (\gamma(g))^2$$

que implica que $\gamma\gamma^* = 0$ si y solo si $\gamma = 0$.

Corolario 2.4.2. *Sea γ un elemento de $\mathbb{Z}G$ que conmuta con γ^*. Entonces si γ es una unidad de orden finito, se tiene que $\gamma = \pm g_0$ para algún $g_0 \in G$.*

Demostración. Dado que existe un entero positivo n tal que $\gamma^n = 1$ y además se tiene por hipótesis que $\gamma\gamma^* = \gamma^*\gamma$, tenemos también que $(\gamma\gamma^*)^n = 1$. Más aún, $(\gamma\gamma^*)(1) = \sum \gamma(g)^2 \neq 0$. Entonces se sigue del Teorema de Passman-Bass que $\gamma\gamma^* = 1$. Consecuentemente, $\sum \gamma(g)^2 = 1$. Así, hay un único coeficiente $\gamma(g_0)$ distinto de cero. Concluimos que $\gamma = \pm g_0$. □

Como consecuencias inmediatas tenemos los siguientes corolarios:

Corolario 2.4.3. *Todas las unidades centrales de orden finito de $\mathbb{Z}G$ son triviales.*

Corolario 2.4.4. *Si A es un grupo abeliano cualquiera, entonces las unidades de torsión de $\mathbb{Z}A$ son todas triviales.*

Estos corolarios están relacionados con la **Conjetura de Zaplansky sobre anillos de grupo**, que podemos enunciar como sigue:

> *Sean K un dominio y G un grupo libre de torsión. Entonces KG no contiene unidades no triviales.*

El mismo Kaplansky enunció otras conjeturas similares, cambiando *unidades* por *idempotentes* y *divisores de cero*:

> *Sean K un dominio y G un grupo libre de torsión. Entonces KG no contiene idempotentes no triviales.*

> *Sean K un dominio y G un grupo libre de torsión. Entonces KG no contiene divisores de cero no triviales.*

A día de hoy, hay pocos resultados sobre estas conjeturas. En particular, siguen abiertas las tres.

3- El Problema del Isomorfismo

Finalmente, en este capítulo trataremos el Problema del Isomorfismo

- Primero expondremos un poco de historia de este problema y lo enunciaremos formalmente.
- Seguidamente, daremos varios resultados sobre grupos metabelianos y demostraremos que en este caso el problema se resuelve con respuesta positiva.
- Después definiremos el concepto de grupo circular y veremos como a partir de esta estructura pueden obtenerse muchos ejemplos de grupos determinados por su anillo de grupo entero.
- Acabaremos el capítulo y el trabajo dando algunos resultados más para casos particulares y exponiendo la construcción de un resultado negativo de la versión fuerte del problema.

3.1. Introducción al problema

Hemos visto en el Corolario 1.5.3 que si G y H son dos grupos abelianos finitos del mismo orden, entonces $\mathbb{C}G$ es isomorfo a $\mathbb{C}H$. Esto muestra que un grupo abeliano finito no está determinado por su anillo de grupo sobre el cuerpo de los números complejos. El Problema del Isomorfismo para anillos de grupo aparece por primera vez particularizado para los anillos de grupo enteros, en la tesis de G.Higman [11], donde dice:

> *"Whether it is possible for two non-isomorphic groups to have isomorphic integral group rings, I do not know; but the results of section 5 suggest it is unlikely."* [1]

Fue propuesto como problema por primera vez en la Conferencia de Álgebra de Michigan de 1947 por T.M. Thrall, que lo formuló de la siguiente manera:

> *"Given a group G and a field K, determine all groups H such that $KG \cong KH$."* [2]

En 1950, S. Perlis y G. Walker [19] probaron que los grupos abelianos finitos están determinados por su anillo de grupo sobre el cuerpo de los números racionales y poco después, en 1956, W.E. Deskins [7] mostró que los p-grupos abelianos finitos están determinados por su anillo de grupo sobre cualquier cuerpo de característica p. En ese sentido, algunos resultados parciales sobre grupos finitos no abelianos fueron obtenidos por D.B. Coleman [3] D.S. Passman [16],[15].

Estos resultados parecen sugerir que, dada una familia de grupos, podría ser posible obtener un cuerpo adecuado para el cual el Problema del Isomofismo tenga una respuesta afirmativa. Brauer, de hecho, propuso que si $KG \cong KH$ para todo cuerpo K, entonces $G \cong H$[4]. Sin embargo, en 1972, E. Dade [5] dio un ejemplo de dos grupos metabelianos no isomorfos cuyas álgebras de grupo sobre *cualquier* cuerpo son isomorfas.

Puede verse fácilmente (Teorema de Whitcomb) que los anillos de grupo enteros de los grupos dados por Dade **no** son isomorfos. La forma más fuerte de considerar el Problema del Isomofismo es precisamente cuando el anillo de coeficientes es el anillo de los números enteros. Puede plantearse el problema como sigue:

$$\mathbb{Z}G \cong \mathbb{Z}H \Rightarrow G \cong H$$

La razón de concentrarse en el anillo entero es la siguiente observación:

[1] *"No sé si es posible para dos grupos no isomorfos tener anillos de grupo enteros isomorfos, pero los resultados de la sección 5 sugieren que es improbable."*

[2] *"Dados un grupo G y un cuerpo $\mathbb{K}$, determinar todos los grupos H tales que $\mathbb{K}G \cong \mathbb{K}H$."*

Lema 3.1.1. *Sean G y H dos grupos tales que $\mathbb{Z}G \cong \mathbb{Z}H$. Entonces, $RG \cong RH$ para cualquier anillo conmutativo R (como R-álgebras).*

Demostración. Asumamos que G y H son tales que $\mathbb{Z}G \cong \mathbb{Z}H$ y sea R un anillo cualquiera. Entonces se tiene:

$$RG \cong R \otimes_{\mathbb{Z}} \mathbb{Z}G \cong R \otimes_{\mathbb{Z}} \mathbb{Z}H \cong RH.$$

□

Estaremos interesados en isomorfismos que preserven aumentos, así que daremos una definición explícita.

Definición 3.1.2. *Un isomorfismo $\varphi : \mathbb{Z}G \to \mathbb{Z}H$ diremos que está **normalizado** si para todo $\alpha \in \mathbb{Z}G$, tenemos que $\epsilon(\alpha) = \epsilon(\varphi(\alpha))$ o, equivalentemente, si para todo elemento $g \in G$ tenemos que $\epsilon(\varphi(g)) = 1$).*

Remarcamos que si existe un isomorfismo $\varphi : RG \to RH$, entonces también existe siempre un isomorfismo normalizado entre estos anillos. De hecho, es suficiente considerar la aplicación $\psi : RG \to RH$ dada de la siguiente manera: para cada elemento α de RG, de la forma $\alpha = \sum_{i=1}^{n} r_i g_i$, definimos $\psi(\alpha) = \sum_{i=1}^{n} \epsilon(\varphi(g_i))^{-1} r_i \varphi(g_i)$ (Nótese que como $g \in G$ es invertible y ϵ es un epimorfismo, tenemos que $\epsilon(\varphi(g))$ es invertible en R). Es fácil verificar que ψ es, de hecho, un isomorfismo normalizado. Así, de aquí en adelante, cada vez que consideremos el Problema del Isomorfismo, asumiremos, sin pérdida de generalidad, que los isomorfismos bajo consideración están normalizados.

Supongamos que G y H son grupos finitos. Sea $\varphi : \mathbb{Z}G \to \mathbb{Z}H$ un isomorfismo normalizado. Nótese que si $\varphi(g)$ está en H para todo g en G, entonces la propia aplicación φ define un isomorfismo entre los grupos H y G. La principal dificultad es que, en general, no hay motivo por el cual esto debería ocurrir (aunque veremos que hay al menos algunas familias de grupos para las cuales éste es realmente el caso). En el caso general, no tenemos gran conocimiento sobre los elementos de la forma $\varphi(g)$, con g en G. Sin embargo, sí sabemos ciertos hechos. Nótese que, como $|G| = n$, tenemos que $g^n = 1$ para todo $g \in G$ y, de esta manera, $\varphi(g)^n = 1$. Esto significa que $\varphi(g)$, con g en G es siempre un elemento invertible de orden finito en $\mathbb{Z}G$.

Introducimos la siguiente definición:

Notación 3.1.3. *Sea G un grupo. Entonces,*

$$\mathcal{U}(\mathbb{Z}G) = \{\alpha \in \mathbb{Z}G : \alpha \text{ es invertible } \}$$

$$\mathcal{V}(\mathbb{Z}G) = \{\alpha \in \mathcal{U}(\mathbb{Z}G) : \epsilon(\alpha) = 1\}$$

Llamamos al primer grupo ***grupo de unidades*** *de $\mathbb{Z}G$ y al segundo, que es subgrupo del primero,* ***grupo de unidades normalizadas*** *de $\mathbb{Z}G$.*

Se sigue directamente que

$$\mathcal{U}(\mathbb{Z}G) = \{\pm 1\} \times \mathcal{V}(\mathcal{Z}G)$$

Hemos visto en el Teorema 2.2.4 que si G es un grupo abeliano finito, entonces toda unidad de orden finito de $\mathbb{Z}G$ es trivial. En otras palabras, tenemos que:

$$T\mathcal{U}(\mathbb{Z}G) = \{\pm 1\} \times G$$

$$T\mathcal{V}(\mathbb{Z}G) = G$$

donde $T\mathcal{U}(\mathbb{Z}G)$ es el **conjunto de unidades de torsión** de $\mathbb{Z}G$ (y lo mismo para $T\mathcal{V}(\mathbb{Z}G)$).

Usaremos este hecho para dar una prueba simple del teorema de G. Higman para isomorfismos de anillos de grupo enteros para grupos abelianos finitos.

Teorema 3.1.4. *Sea G un grupo abeliano finito y H otro grupo tal que $\mathbb{Z}G \cong \mathbb{Z}H$. Entonces $G \cong H$.*

Demostración. Si $\mathbb{Z}G \cong \mathbb{Z}H$, entonces podemos asumir que existe un isomorfismo normalizado. Si G es un grupo abeliano, entonces $\mathbb{Z}G$ es conmutativo, luego $\mathbb{Z}H$ también y se sigue que H es abeliano.

Como el rango de un módulo libre sobre $\mathbb{Z}$ es invariante, se sigue inmediatamente que H también es finito y que $|G| = |H|$. Para cada elemento g de G tenemos que $\varphi(g)$ es una unidad normalizada de orden finito en $\mathbb{Z}H$. Se sigue del Teorema 2.2.4 que $\varphi(g) \in \pm H$ y como φ está normalizado, vemos que $\varphi(g) \in H$. Esto muestra que $\varphi(G) \subseteq H$ y, como $|G| = |H|$, tenemos que $\varphi(G) = H$. En otras palabras, la restricción de φ a G nos proporciona un isomorfismo entre G y H. □

Nótese que con los mismos argumentos puede mostrarse que el centro de un grupo finito es invariante bajo isomorfismos de anillos de grupo.

Proposición 3.1.5. *Sea G un grupo finito y H otro grupo tal que $\mathbb{Z}G \cong \mathbb{Z}H$. Entonces $\mathcal{Z}(G) = \mathcal{Z}(H)$, donde $\mathcal{Z}(G)$ y $\mathcal{Z}(H)$ denotan los centros de G y de H, respectivamente.*

Mostraremos en las secciones posteriores que hay muchos más subgrupos importantes que se preservan bajo isomorfismos del anillo de grupo entero.

3.2. Correspondencia de subgrupos normales

Recordamos de la sección 2.1 que una base para el centro del anillo de grupo entero $\mathbb{Z}G$ de un grupo finito G viene dada por los elementos $\gamma_i = \sum_{x \in C_i} x$, con i en I, donde $\{C_i\}_{i \in I}$ es el conjunto de las clases de conjugación de G.

Comenzamos esta sección enunciado un resultado sin demostrarlo que afirma que estos elementos se preservan bajo isomorfismos de anillos de grupo enteros. Puede consultarse en [15], atribuido a G. Glauberman, pero ya había aparecido en un artículo de S. D. Berman [1].

Teorema 3.2.1. *Sean G y H grupos finitos y sea $\varphi : \mathbb{Z}G \to \mathbb{Z}H$ un isomorfismo normalizado. Denotamos por $\{\gamma_i\}_{i \in I}$ y $\{\delta_j\}_{j \in J}$ las sumas de clase de G y H respectivamente. Entonces, para cada γ_i existe un único δ_j tal que $\varphi(\gamma_i) = \delta_j$. Esto es, existe una correspondencia uno a uno entre las sumas de clase de G y de H.*

Podemos usar este resultado para probar que existe una correspondencia uno a uno entre el retículo de los subgrupos normales de G y el de los de H. Recordamos que dado un subconjunto N de G, denotamos $\widehat{N} = \sum\limits_{x \in N} x$.

Teorema 3.2.2. *Si $\theta : \mathbb{Z}G \to \mathbb{Z}H$ un isomorfismo normalizado con G y H grupos finitos entonces existe un isomorfismo $\widehat{\theta}$ entre los retículos de subgrupos normales de G y H de forma que $\theta(\widehat{N}) = \widehat{\theta(N)}$ para cualquier subgrupo normal N de G.*

Demostración. Por ser N un subgrupo normal de G, es unión disjunta de clases de conjugación: $N = C_1 \cup C_2 \cup \ldots \cup C_t$ y, si γ_i, para $1 \leq i \leq t$ denotan las sumas de clase correspondientes, tenemos que $\widehat{N} = \sum_{i=1}^{t} \gamma_i$. Sea $\theta(\gamma_i) = \omega_i$, una suma de clases de H. Como $\widehat{N}\widehat{N} = |N|\widehat{N}$ y $\theta(\widehat{N}) = \theta(\sum_{i=1}^{t} \gamma_i) = \sum_{i=1}^{t} \omega_i = \widehat{M}$, para algún subconjunto M de H, vemos que $\widehat{M}\widehat{M} = |N|\widehat{M}$. Esto implica que M es cerrado bajo multiplicación y así, M es un subgrupo. Como es unión de

clases de conjugación, se sigue que M es normal en H. Finalmente, como M es subgrupo, tenemos que $\widehat{M}\widehat{M} = |M|\widehat{M} = |N|\widehat{M}$ y así, $|N| = |M|$. La correspondencia $N \mapsto M$ es isomorfismo por construcción. □

Realmente, la correspondencia obtenida arriba tiene otras propiedades interesantes, que veremos en la Proposición 3.3.10.

3.3. Grupos metabelianos

En esta sección estudiaremos el Problema del Isomorfismo para la clase de grupos metabelianos.

Definición 3.3.1. *Un grupo G es llamado* ***metabeliano*** *si contiene un subgrupo normal A tal que ambos A y G/A son abelianos.*

Mostraremos que estos grupos están determinados por sus anillos de grupo enteros. Para hacer esto, necesitaremos unos pocos resultados técnicos. Para empezar, sabemos que si g y h son elementos de G entonces tenemos la siguiente identidad:

$$gh - 1 = (g-1) + (h-1) + (g-1)(h-1)$$

Como $(g-1)(h-1) \in \Delta^2(G)$, esta identidad implica

$$gh - 1 \equiv (g-1) + (h-1) \pmod{\Delta^2(G)} \tag{3.3.2}$$

Tomando $h = g^{-1}$, vemos que

$$g^{-1} - 1 \equiv -(g-1) \pmod{\Delta^2(G)}$$

Y así, para todo entero a,

$$g^a - 1 \equiv a(g-1) \pmod{\Delta^2(G)} \tag{3.3.3}$$

Así, la aplicación $\phi : G \to \Delta(G)/\Delta(G)^2$ dada por $\phi(g) = (g-1) + (\Delta(G)^2)$ es realmente un homomorfismo de G en el grupo aditivo $\Delta(G)/\Delta(G)^2$. Usaremos esta observación para mostrar que el grupo G/G' es invariante bajo isomorfismos de anillos de grupo. Primero notamos lo siguiente:

Lema 3.3.4. *Sean G un grupo y G' su subgrupo conmutador. Entonces*

$$\frac{G}{G'} \cong \frac{\Delta(G)}{\Delta(G)^2}$$

Demostración. Dado G, definimos $\phi : G \to \Delta(G)/\Delta(G)^2$ como arriba. Dado que la imagen de ϕ es un grupo abeliano, se sigue que $G' \subseteq Ker(\phi)$. Por ello ϕ induce un homomorfismo de grupos $\phi^* : G/G' \to \Delta(G)/\Delta(G)^2$. Queremos mostrar que ϕ^* es realmente un isomorfismo. Para ello buscamos su inverso. Recordamos que hemos mostrado en la Proposición 1.2.6 que el conjunto de elementos $\{g-1 : g \in G\}$ es una base de $\Delta(G)$ sobre $\mathbb{Z}$. Así, podemos definir una aplicación $\psi : \Delta(G) \to G/G'$ dándole valor en los elementos de la base:

$$\psi : (g-1) \mapsto gG', \text{ para cada } g \in G.$$

Nótese que si tomamos $\alpha \in \Delta(G)^2$ de la forma $\alpha = -(a-1)(b-1)$ entonces $\alpha = (a-1)+(b-1)-(ab-1)$ así que tenemos que

$$\psi(\alpha) = aG' \cdot bG' \cdot (ab)^{-1}G' = abb^{-1}a^{-1}G' = G',$$

y así, $\alpha \in Ker(\psi)$. Esto muestra que $\Delta(G)^2 \subseteq Ker(\psi)$, pues $\Delta(G)^2$ está generado como grupo aditivo por los elementos de la forma $(g-1)(h-1)$. De esta forma, ψ induce un homomorfismo $\psi^* : \Delta(G)/\Delta(g)^2 \to G/G'$ y un cálculo directo nos muestra que ϕ^* y ψ^* son inversos entre sí. □

Nótese que el argumento de la prueba implica, en particular, que $Ker(\phi) = G'$. Dado que $Ker(\phi) = \{g \in G : g-1 \in \Delta^2(G)\} = G \cap (1+\Delta^2(G))$, hemos obtenido el siguiente resultado:

Corolario 3.3.5. *Sean G un grupo y G' su subgrupo conmutador. Entonces,*

$$G \cap (1+\Delta^2(G)) = G'$$

Corolario 3.3.6. *Sean G y H grupos tales que $\mathbb{Z}G \cong \mathbb{Z}H$. Entonces,*

$$\frac{G}{G'} \cong \frac{H}{H'}$$

Demostración. Sea $\theta : \mathbb{Z}G \to \mathbb{Z}H$ un isomorfismo normalizado. Como $\Delta(G)$ y $\Delta(H)$ son los núcleos de las aplicaciones de aumento respectivas, tenemos que $\theta(\Delta(G)) = \Delta(H)$ y así, $\theta(\Delta^2(G)) = \Delta^2(H)$. Así,

$$\frac{G}{G'} \cong \frac{\Delta(G)}{\Delta^2(G)} \cong \frac{\Delta(H)}{\Delta^2(H)} \cong \frac{H}{H'}$$

□

De hecho también se cumpliría $\mathbb{Q}G \cong \mathbb{Q}H \Rightarrow G/G' \cong H/H'$. Usando el Teorema de Perlis-Walker tenemos que $\mathbb{Q}(G/G')$ es la suma de todas las componentes simples abelianas de $\mathbb{Q}(G/G')$, luego aplicando el Corolario 3.3.6 recién demostrado, tenemos que también se tiene $\mathbb{Q}(G/G') \cong \mathbb{Q}(H/H')$, y como G/G' y H/H' son ambos abelianos, se deduce que $G/G' \cong H/H'$ por el Teorema 3.1.4.

Para afinar el Corolario 3.3.6 necesitamos lo siguiente:

Lema 3.3.7. *Sea N un subgrupo normal de un grupo G. Si un elemento g de G es tal que $g - 1 \in \Delta(G)\Delta(G, N)$, entonces $g \in N'$.*

Demostración. Un elemento de $\Delta(G)\Delta(G, N)$ es una combinación lineal de productos de la forma $(x - 1)y(n - 1)$, con x e y en G y n en N. Como $(x - 1)y = (xy - 1) - (y - 1)$, vemos que podemos escribir $g - 1$ de la forma:

$$g - 1 = \sum_{i,j} a_{ij}(x_i - 1)(n_j - 1), \text{ con } x_i \in G,\ a_{ij} \in \mathbb{Z} \text{ y } n_j \in N. \tag{3.3.8}$$

Sea $\mathcal{T}$ un transversal de N en G que contiene el 1. Entonces, todo elemento x de G puede escribirse de forma única como producto $x = tn$, con $t \in \mathcal{T}$ y $n \in N$. Definimos una aplicación $\theta : G \to N$ por

$$\theta\colon x = tn \mapsto n,$$

que extendemos de forma lineal a $\mathbb{Z}G$. Entonces $\theta : \mathbb{Z}G \to \mathbb{Z}N$ es una aplicación lineal, aunque posiblemente no sea un homomorfismo bajo el producto.

Si en (3.3.8) escribimos $x_i = t_i m_i$, con $m_i \in N$ y $t_i \in \mathcal{T}$y aplicamos θ a ambos lados de la ecuación, obtenemos

$$\theta(g) - 1 = \sum_{i,j} a_{ij}(m_i - 1)(n_j - 1).$$

Esto es porque

$$\begin{aligned}\theta((t_i m_i - 1)(n_j - 1)) &= \theta(t_i m_i n_j - t_i m_i - n_j + 1 \\ &= m_i n_j - m_i - n_j + 1 \\ &= (m_i - 1)(n_j - 1).\end{aligned}$$

Sacando módulos sobre N, (3.3.8) nos da $\overline{g} - \overline{1} = 0$, así que tenemos que g está en N. Así, $\theta(g) = g$ y obtenemos

$$g - 1 = \sum_{i,j} a_{ij}(m_i - 1)(n_j - 1) \in \Delta^2(N).$$

Como consecuencia, $g \in N \cap (1 + \Delta^2(N)) = N'$ (Corolario 3.3.5). □

Corolario 3.3.9. *Sea N un subgrupo normal de un grupo G. Entonces,*

$$\frac{N}{N'} \cong \frac{\Delta(G, N)}{\Delta(G)\Delta(G, N)}.$$

Demostración. Definimos $\phi : N \to \Delta(G, N)/\Delta(G)\Delta(G, N)$ por

$$n \mapsto 1 - n + \Delta(G)\Delta(G, N).$$

Es fácil ver que ϕ es suprayectivo usando las fórmulas 3.3.2 y 3.3.3. Así, el Lema 3.3.7 nos muestra que $Ker(\phi) = N'$. Así, tenemos

$$\frac{N}{N'} \cong \frac{\Delta(G, N)}{\Delta(G)\Delta(G, N)}.$$

Como se nos pedía. □

Ahora estamos listos para dar información extra sobre la correspondencia entre subgrupos normales.

Proposición 3.3.10. *Sean G y H grupos finitos y $\theta : \mathbb{Z}G \to \mathbb{Z}H$ un isomorfismo normalizado. Si N es un subgrupo normal de G y $M = \widehat{\theta}(N)$ (ver Teorema 3.2.2, entonces:*

(i) $\mathbb{Z}(G/N) \cong \mathbb{Z}(H/M)$

(ii) $N/N' \cong M/M'$

(iii) Si N es abeliano entonces M también lo es.

Demostración. Primero, recordamos que el anulador de $\widehat{N}$ es:

$$Ann(\widehat{N}) = \{x \in \mathbb{Z}G : x\widehat{N} = 0\} = \Delta(G, N).$$

Tenemos que $\theta(\widehat{N}) = \widehat{M}$ así que también $\theta(\Delta(G, N))) = \Delta(H, M)$. Así, θ induce un isomorfismo $\theta^* : (\mathbb{Z}G/\Delta(G, N)) \to \mathbb{Z}H/\Delta(H, M)$, luego tenemos que

$$\mathbb{Z}(G/N) \cong \mathbb{Z}G/\Delta(G, N) \cong \mathbb{Z}H/\Delta(H, M) \cong \mathbb{Z}(H/M),$$

probando (i).

Para probar (ii), notamos que, usando el Corolario 3.3.9, tenemos que

$$\frac{N}{N'} \cong \frac{\Delta(G, N)}{\Delta(G)\Delta(G, N)} \cong \frac{\Delta(G, M)}{\Delta(H)\Delta(H, M)} \cong \frac{M}{M'}.$$

Por último, para probar (iii), resaltamos que si N es abeliano entonces $N' = 1$, así que se sigue de (ii) que $N \cong M/M'$ y, como $|N| = |M|$, se sigue que también $M' = 1$, probando que M es abeliano. □

Teorema 3.3.11 (Whitcomb)**.** *Sean G y H dos grupos finitos tales que $\mathbb{Z}G \cong \mathbb{Z}H$. Entonces,*

$$\frac{G}{G''} \cong \frac{H}{H''}.$$

Demostración. Para empezar, recordamos que $\Delta(G, G')$ puede caracterizarse como el ideal más pequeño J de $\mathbb{Z}G$ tal que $\mathbb{Z}G/J$ es un anillo conmutativo. Así, dado un isomorfismo normalizado $\theta : \mathbb{Z}G \to \mathbb{Z}H$, tenemos que $\theta(\Delta(G, G')) = \Delta(H, H')$.

Dado un elemento g de G tenemos que $\gamma = \theta(g)$ es una unidad de orden finito en $\mathbb{Z}H$. Denotemos por $\overline{\gamma}$ la imagen de γ en el anillo cociente $\mathbb{Z}H/\Delta(H, H') \cong \mathbb{Z}(H/H')$. Así, el Teorema

de Higman (2.2.4) nos muestra que $\overline{\gamma}$ es trivial. Esto es, que existe un elemento h_o en H tal que $\overline{\gamma} = \overline{h_o}$ o, en otras palabras, tal que $\gamma \equiv h_0 \pmod{\Delta(H, H')}$. Luego existen α_h en $\mathbb{Z}$ para cada $h \in H$ con

$$\gamma = h_0 + \sum_{h \in H'} \alpha_h (h-1).$$

Denotemos $a_h = \varepsilon(\alpha_h)$, que está en $\mathbb{Z}$. Entonces, podemos escribir

$$\gamma = h_0 + \sum_{h \in H'} \left(a_h(h-1) + (\alpha_h - a_h)(h-1)\right).$$

Como $(\alpha_h - a_h) \in \Delta(H)$, tenemos que

$$\gamma \equiv h_0 + \sum_{h \in H'} a_h(h-1) \pmod{\Delta(H)\Delta(H, H')},$$

luego

$$\gamma - 1 \equiv h_0 - 1 + \sum_{h \in H'} a_h(h-1) \pmod{\Delta(H)\Delta(H, H')}.$$

Usando las fórmulas 3.3.2 y 3.3.3 (resp.) podemos reescribir esta ecuación como

$$\gamma - 1 \equiv h_0 - 1 + \sum_{h \in H'} (h^{a_h} - 1) \pmod{\Delta(H)\Delta(H, H')} \equiv h_0 \prod_{h \in H'} h^{a_h} - 1 \pmod{\Delta(H)\Delta(H, H')}.$$

Así, $h_g = h_0 \prod_{h \in H'} h^{a_h}$ es un elemento de H tal que $\gamma \equiv h_g \pmod{\Delta(H)\Delta(H, H')}$. Afirmamos que a cada elemento $g \in G$ le corresponde un único elemento (módulo H''): Si h_1, h_2 son dos elementos de H tales que $h_1 \equiv h_2 \pmod{\Delta(H)\Delta(H, H')}$, entonces $h_1 h_2^{-1} \equiv 1 \pmod{\Delta(H)\Delta(H, H')}$, o sea que $h_1 h_2^{-1} \in H \cap (1 + \Delta(H)\Delta(H, H')) = H''$, por el Lema 3.3.7.

Así, podemos definir una aplicación $\phi : G \to H/H''$ por

$$G \ni g \mapsto \overline{h_g} \in H/H'',$$

que es claramente un homomorfismo.

Ahora, sea g un elemento de $Ker(\phi)$. Entonces $\theta(g) \equiv 1 \pmod{\Delta(H)\Delta(H, H')}$. Aplicando θ^{-1} tenemos que $g \equiv 1 \pmod{\Delta(G)\Delta(G, G')}$ y aplicando de nuevo el Lema 3.3.7 obtenemos que $g \in G''$.

Así, ϕ induce un homomorfismo $\phi^* : G/G'' \to H/H''$ inyectivo. Entonces $|G/G''| \leq |H/H''|$, y aplicando de nuevo lo de arriba en la dirección opuesta obtenemos $|H/H''| \leq |G/G''|$, luego realmente son $|G/G''| = |H/H''|$ y ϕ^* es isomorfismo. □

Corolario 3.3.12. *Sean G un grupo finito metabeliano y H otro grupo tal que $\mathbb{Z}G \cong \mathbb{Z}H$. Entonces, $G \cong H$.*

Demostración. Por ser G metabeliano, $G'' = 1$. Entonces, aplicando el Teorema de Whitcomb

$$G \cong G/G'' \cong H/H'' \cong H$$

□

3.4. Grupos circulares

Al comienzo de los 40, los teóricos de anillos trabajaban en dar con una buena definición del radical de un anillo. En este contexto, S. Perlis introdujo en 1942 [18] la noción de *elemento cuasi regular* que fue muy útil para la definición del radical. Este concepto será de especial interés en esta sección.

En esta sección un anillo no será necesariamente unitario.

Definición 3.4.1. *Sea R un anillo no necesariamente unitario. Definimos una nueva operación en R por*

$$x \circ y = x + y + xy, \text{ para cada } x, y \in R.$$

Esta operación es asociativa y su identidad es el 0 de R.

Definición 3.4.2. *Sea R un anillo. Un elemento $x \in R$ es llamado **cuasi regular en R por la izquierda** si existe $y \in R$ tal que $y \circ x = 0$; llamamos a este elemento **cuasi inverso por la izquierda** de x en R. De forma similar, se dice que x es un **cuasi regular en R por la derecha** si existe $y \in R$ tal que $x \circ y = 0$. Un elemento x de R es llamado **cuasi regular en R** si lo es por ambos lados.*

Si un elemento es cuasi regular, sus inversos por ambos lados coinciden (si $x \circ y = 0 = z \circ x$, entonces $z = z \circ (x \circ y) = (z \circ x) \circ y = y$). El conjunto de todos los elementos cuasi regulares forma un grupo con la operación $\circ$.

Definición 3.4.3. *Sea R un anillo. El grupo de todos los elementos cuasi regulares de R, con la operación $\circ$ es llamado* ***grupo adjunto*** *de R.*

Definición 3.4.4. *Se dice que un anillo R es* ***radical*** *si todos sus elementos son cuasi regulares. El grupo adjunto de un anillo radical es llamado* ***grupo circular****.*

Es fácil ver que si 1 es el elemento identidad de un anillo R, entonces el elemento -1 no es cuasi regular. Así, ningún anillo unitario es radical. Además, observamos que si un elemento x en un anillo R es nilpotente, entonces x es cuasi regular. De hecho, si $x^n = 0$, entonces tenemos por cálculos directos que

$$y = -x + x^2 - \cdots + (-1)^{n-1}x^{n-1}$$

es el cuasi inverso de x.

Realmente, si un anillo R es unitario, entonces hay una conexión cercana entre el grupo adjunto de R y su grupo de unidades:

Proposición 3.4.5. *Sean R un anillo unitario y $\mathcal{U}(R)$ su grupo de unidades. Denotemos por G el grupo adjunto de R. Entonces $\mathcal{U}(R) = 1 + G$ y $\mathcal{U}(R) \cong G$.*

Demostración. Sea $g \in G$ y tomemos $h \in G$ el cuasi inverso de g. Entonces $g \circ h = h \circ g = 0$, así que tenemos que

$$(1 + g)(1 + h) = 1 + g + h + gh = 1 + g \circ h = 1.$$

De forma similar, se sigue que $(1+h)(1+g) = 1$, mostrando que $1+g \in \mathcal{U}(R)$. Recíprocamente, si $u \in \mathcal{U}(R)$, un argumento similar muestra que $u - 1$ está en G. Así, es claro que la aplicación $\varphi : G \to \mathcal{U}(R)$ dada por $\varphi(g) = 1 + g$ es una biyección, así que solo queda mostrar que es homomorfismo. Para ello tomamos g y h en G y tenemos

$$\varphi(g \circ h) = 1 + g \circ h = 1 + g + h + gh = (1 + g)(1 + h) = \varphi(g)\varphi(h).$$

□

Veamos un ejemplo de un grupo circular *(Ejemplo 3.4.6)*:

- Sea $T(n, K)$ el conjunto de las matrices triangulares superiores con coeficientes en K:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & a_{22} & a_{23} & \cdots & a_{2n} \\ 0 & 0 & a_{33} & \cdots & a_{3n} \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & a_{nn} \end{bmatrix}$$

- Denotamos por $T_0(n, K)$ el conjunto de matrices en $T(n, K)$ que tienen solo ceros en la diagonal principal. Es fácil comprobar que $T_0(n, K)$ es cerrado bajo sumas y productos. Todos los elementos de $T_0(n, K)$ son nilpotentes, así que se sigue que es un anillo radical. Luego $T_0(n, K)$, con la operación $\circ$, es un grupo circular.

- Además, nótese que si denotamos por $T_1(n, K)$ el conjunto de todas las matrices en $T(n, K)$ con solamente unos en la diagonal principal, entonces $1 + T_0(n, K) = T_1(n, K)$, y se sigue de la Proposición 3.4.5 que $T_0(n, K)$, con la operación $\circ$, es un grupo isomorfo a $T_1(n, K)$.

Mostraremos ahora que un grupo adjunto G de un anillo R puede ser caracterizado en términos de su anillo de grupo entero. Definimos un homomorfismo de grupos aditivos $\theta : \mathbb{Z}G \to R$ por

$$\theta\left(\sum_{g\in G} a(g)g\right) = \sum_{g\in G} a(g)g \tag{3.4.7}$$

Recordamos que el elemento identidad de G (que denotaremos por 1_G) es el 0 de R, o sea que un elemento de la forma $g - 1_G \in \mathbb{Z}G$ va por la aplicación a $g \in R$.

Afirmamos que la restricción de θ al ideal de aumento $\Delta(G)$ es un homomorfismo de anillos. Para probar lo afirmado, hemos de mostrar que θ es un homomorfismo multiplicativo al restringirse a $\Delta(G)$:

$$\theta((g - 1_G)(h - 1_G)) = \theta(g \circ h - g - h + 1_G) = g \circ h - g - h = g + h + gh - g - h = gh,$$

luego $\theta(\Delta(G))$ es un subanillo de R.

Teorema 3.4.8. *Un grupo G es el grupo adjunto de un anillo si y solo si es el grupo adjunto de un anillo cociente de $\Delta(G)$ (salvo isomorfismos).*

Demostración. La suficiencia es trivial así que probaremos solo la necesidad. Asumamos que G es el grupo adjunto de cierto anillo R. Sea $\theta : \Delta(G) \to R$ el homomorfismo de anillos construido arriba. Entonces:

$$\Delta(G)/Ker(\theta) \cong \theta(\Delta(G)).$$

Ahora, $\theta(\Delta(G))$ es un subanillo de R que contiene a G, así que G es el grupo adjunto de $\theta(\Delta(G))$, luego es también por la fuerza el grupo adjunto de $\Delta(G)/Ker(\theta)$. □

Podemos caracterizar los grupos circulares de forma similar.

Teorema 3.4.9. *Sea G un grupo finito. Entonces G es un grupo circular si y solo si existe un ideal J de $\mathbb{Z}G$, contenido en $\Delta(G)$, de forma que:*

(i) El índice aditivo de J en $\Delta(G)$ es igual a $|G|$

(ii) $(1_G + J) \cap G = 1$.

En este caso, tenemos que

$$G \cong 1 + \frac{\Delta(G)}{J}$$

Demostración. Probaremos primero que las condiciones son necesarias. Asumamos que G es el grupo circular de cierto anillo radical R. Sea $\theta : \Delta(G) \to R$ el homomorfismo de anillos construido en (3.4.7). Tomamos $J = Ker(\theta)$. Como R es un anillo radical, es claro que θ es suprayectivo. Así,

$$\Delta(G)/J \cong \theta(\Delta(G)) = R.$$

De forma que la condición (i) del teorema se deduce inmediatamente.

Para probar (ii) tomamos $x \in (1_G + J) \cap G$. Entonces, $x - 1_G \in J$, luego $\theta(x - 1_G) = 0$. Como $x \in G$, tenemos que $\theta(x - 1_G) = x$, luego se sigue que $x = 0$ en R. Como el elemento 0 de R es el elemento identidad 1_G del grupo circular G, se sigue que $x = 1_G$, como se deseaba.

Mostraremos ahora que las condiciones son también suficientes. Consideramos la aplicación $\phi : G \to 1 + \Delta(G)/J$ dada por

$$\phi : x \mapsto 1 + (x - 1_G) + J.$$

Mostraremos que ϕ es un homomorfismo de grupos. De hecho, tomamos $g, h \in G$. Entonces,

$$\begin{aligned}\phi(g)\phi(h) &= (1 + (g - 1_G) + J)(1 + (h - 1_G) + J) \\ &= 1 + (gh - 1_G) + J = \phi(gh),\end{aligned}$$

luego ϕ es un homomorfismo.

Afirmamos además que es una biyección. Como $|G| = |\Delta(G)/J| = |1+\Delta(G)/J|$, es suficiente probar que ϕ es inyectiva. Así, asumamos $g \in G$ de forma que $\phi(g) = 1$. Entonces $g - 1_G \in J$, luego $g \in (1_G + J) \cap G = 1$ como queríamos. □

Lema 3.4.10. *Sean G y H dos grupos finitos y $\phi : \mathbb{Z}G \to \mathbb{Z}H$ un isomorfismo normalizado. Sea J un ideal de $\mathbb{Z}G$ tal que $(1+J)\cap G = 1$. Entonces también $(1+\phi(J))\cap H = 1$*

Demostración. Asumamos que $M = (1 + \phi(J)) \cap H$ es no trivial. Por ser J ideal bilátero, también lo es $\phi(J)$ y se sigue que M es un subgrupo normal de H. Además, como $M = \{h \in H : h - 1 \in \phi(J)\}$, es claro que $\Delta(M) \subseteq \phi(J)$. Sea $N = \widehat{\phi}^{-1}(M)$ el subgrupo normal de G que corresponde a M como en el Teorema 3.2.2. Entonces $|N| = |M|$, luego N es no trivial y $\phi^{-1}(\Delta(M)) = \Delta(N) \subseteq J$. Esto implica que $N \subseteq (1 + J) \cap G$, una contradicción. □

Siguiendo el mismo desarrollo que R. Sandling [23], usaremos estas ideas para probar que los grupos circulares finitos, los grupos finitos adjuntos y los grupos de unidades de anillos finitos están todos determinados por sus anillos de grupo enteros.

Teorema 3.4.11. *Un grupo circular finito está determinado por su anillo de grupo entero.*

Demostración. Sea G un grupo circular finito. Se sigue del Teorema 3.4.9 que existe un ideal $J \subseteq \Delta(G)$ tal que $(1 + J) \cap G = 1$ y $G \cong 1 + \Delta(G)/J$. Sea H otro grupo tal que $\mathbb{Z}G \cong \mathbb{Z}H$ y sea $\phi : \mathbb{Z}G \to \mathbb{Z}H$ un homomorfismo normalizado. Entonces $\phi(J)$ es un ideal de $\mathbb{Z}H$ contenido en $\Delta(H)$ y, como se ha mostrado en el Lema 3.4.10, es tal que $(1 + \phi(J)) \cap H) = 1$.

Como $\phi(\Delta(G)) = \Delta(H)$, se sigue que $[\Delta(H) : \phi(J)] = [\Delta(G) : J] = |G| = |H|$, luego por el Teorema 3.4.9, H es un grupo circular y es isomorfo a $1 + \Delta(H)/\phi(J)$. Así, tenemos que

$$G \cong 1 + \frac{\Delta(G)}{J} \cong 1 + \frac{\Delta(H)}{\phi(J)} \cong H,$$

como se pedía. □

Como consecuencia inmediata tenemos:

Corolario 3.4.12. *Sea K un cuerpo finito de característica p. Entonces los p-subgrupos de Sylow del grupo general lineal $GL(n, K)$ están determinados por su anillo de grupo entero.*

Demostración. Vimos en el ejemplo (3.4.6) que $T_1(n, K)$ es isomorfo a $T_0(n, K)$, el grupo circular de un anillo radical. Puede verse[3] que $T_1(n, K)$ es un subgrupo p-Sylow de $GL(n, K)$. Así, todos los subgrupos p-Sylow de $GL(n, K)$ son isomorfos a $T_0(n, K)$. Así, el Teorema 3.4.11 nos muestra que están todos determinados por el anillo de grupo entero. □

Más resultados:

- Los grupos circulares de anillos finitos son nilpotentes.
- Los grupos nilpotentes finitos están determinados por su anillo de grupo entero. Es otra forma de demostrar el Teorema 3.4.11, pero la prueba se sale del nivel del trabajo. Puede consultarse en [25].
- Los grupos nilpotentes de clase 2 son grupos circulares [23].
- No todos los grupos nilpotentes son circulares, de hecho esto no es cierto ni para p-grupos. Los grupos de orden como mucho p^3 sí son circulares, pero un grupo de orden p^4 es circular si y solo si su clase de nilpotencia es como mucho 2 [14].

Vamos a demostrar un lema y lo usaremos para demostrar que el grupo de unidades de un anillo finito está determinado por su anillo de grupo.

Lema 3.4.13. *Sea J un ideal de un anillo de grupo entero $\mathbb{Z}G$ tal que $(1 + J) \cap G = 1$. Entonces G es isomorfo a un subgrupo del grupo de unidades del grupo cociente $\mathbb{Z}G/J$.*

Demostración. Como en el Teorema 3.4.9, consideramos la aplicación $\phi : G \to 1+(\Delta(G)+J)/J$ dada por

$$\phi : x \mapsto 1 + (x - 1_G) + J.$$

Como ya hemos mostrado que esta aplicación es un monomorfismo de grupos se sigue que G es isomorfo a $\phi(G)$, que es un subgrupo del grupo de unidades de $\mathbb{Z}G/J$, como pedíamos. □

[3] No lo veremos, porque no hemos introducido la noción de grupos de Sylow y porque la prueba se basa simplemente en calcular los cardinales de $GL(n, K)$ y $T_1(n, K)$

Teorema 3.4.14. *El grupo de unidades de un anillo finito está determinado por su anillo de grupo entero.*

Demostración. Sea G el grupo de unidades de un anillo finito R. Sustituyendo R por el subanillo generado por G, podemos asumir, sin pérdida de generalidad, que R es generado por G como anillo. Definimos una aplicación $\theta : \mathbb{Z}G \to R$ por $\sum_{g\in G} a(g)g \mapsto \sum_{g\in G} a(g)g$. Como el producto en G es también el producto de R, se sigue que θ es un homomorfismo de anillos y que $\theta(\mathbb{Z}G) = R$. Denotamos $J = Ker(\theta)$; entonces $R = \theta(\mathbb{Z}G) \cong \mathbb{Z}G/J$. Sea H otro grupo tal que $\mathbb{Z}G \cong \mathbb{Z}H$ y pongamos $\phi : \mathbb{Z}G \to \mathbb{Z}H$ un isomorfismo normalizado cualquiera. Entonces $\mathbb{Z}G/J \cong \mathbb{Z}H/\phi(J)$.

Como $(1 + J) \cap G = 1$, el Lema 3.4.10 muestra que $(1 + \phi(J)) \cap H = 1$. Se sigue del Lema 3.4.13 que H es isomorfo a un subgrupo del grupo de unidades de $\mathbb{Z}H/\phi(J) \cong \mathbb{Z}G/J \cong R$. Como el grupo de unidades de R es precisamente G, se sigue que H es isomorfo a un subgrupo de G y, como ambos grupos tienen el mismo orden, $G \cong H$. □

Corolario 3.4.15. *Sea K un cuerpo finito. Entonces el grupo general lineal $GL(n, K)$ está determinado por su anillo de grupo entero.*

Demostración. Como $GL(n, k)$ es el grupo de unidades de $M_N(k)$ y es finito, el resultado se deduce inmediatamente a partir del Teorema 3.4.14. □

El resultado anterior es de hecho una versión más fuerte del Corolario 3.4.12.

Corolario 3.4.16. *Todo grupo finito está contenido en un grupo finito determinado por su anillo de grupo entero.*

Demostración. Sean G un grupo finito de orden n y K cualquier cuerpo finito. Tomando la representación regular $\rho : G \to GL(n, K)$ vemos que G es isomorfo a un subgrupo de $GL(n, K)$. El resultado se sigue del Corolario 3.4.15. □

3.5. Resultados posteriores

En esta sección daremos un breve recuento de desarrollos posteriores en el Problema del Isomorfismo para anillos de grupo enteros. Un avance importante en el problema fue un resultado de Roggenkamp y Scott[21] en el que se demuestra que si G es un p-grupo y $\mathbb{Z}G \cong \mathbb{Z}H$, entonces $G \cong H$. Más adelante, A. Weiss probó un resultado más fuerte [27]:

Teorema 3.5.1. *Sea G un grupo finito nilpotente. Entonces:*

$$\mathbb{Z}G \cong \mathbb{Z}H \Longrightarrow G \cong H$$

Una consecuencia es resultado de Sehgal-Sehgal-Zassenhaus [26]:

Teorema 3.5.2. *Supongamos que G es un grupo finito que es una extensión de un grupo abeliano A por un grupo nilpotente B. Supóngase que $(|A|, |B|) = 1$. Entonces, $\mathbb{Z}G \cong \mathbb{Z}H \Longrightarrow G \cong H$.*

Roggenkamp y Scott anunciaron el resultado anterior sin asumir la hipótesis $(|A|, |B|) = 1$ [21]. Puede consultarse la demostración en [22]

Ahora, a partir de la clasificación de los grupos simples finitos, es bien sabido salvo por algunas excepciones que grupos simples distintos tienen distintos órdenes. Se sigue entonces que el siguiente resultado (demostración en[23]):

Teorema 3.5.3. *Sea G un grupo simple finito. Entonces, $\mathbb{Z}G \cong \mathbb{Z}H \Longrightarrow G \cong H$.*

En 1997, Martin Hertweck anunció un resultado negativo al Problema del Isomorfismo, que no se publicó hasta 2001 [9]. Damos un resumen de las cuentas a continuación:

- Sea X un producto semidirecto $Q \rtimes P$ con un 97-subgrupo de Sylow normal Q y P un 2-subgrupo de Sylow de X. P es un producto semidirecto:

  $$P = (\langle u \rangle \times \langle v \rangle \times \langle w \rangle) \rtimes (\langle a \rangle \times \langle b \rangle \times \langle c \rangle),$$

  donde u, v, w, a, b y c tienen órdenes 32, 4, 8, 128, 2 y 8 respectivamente.

  - La acción de a está dada por $u^a = u$, $v^a = u^{16}v$, $w^a = u^4 w$.

  - La acción de los elementos b y c está dada por $x^b = x^{-1}$ y $x^c = x^5$, para cualquier $x \in \langle u, v, w\rangle$.

- Sea $D = (\langle z\rangle \times \langle y\rangle) \rtimes \langle x\rangle \cong C_{97}^{(2)} \rtimes C_{97}$ con $y^x = zy$ y $z^x = z$. Definimos un automorfismo $\delta \in Aut(D)$ de orden 64 por $z^\delta = z^{-19}$, $y^\delta = x$ y $x^\delta = y^{19}$. Sean $R = D^{(2)}$ y $\rho \in Aut(R)$ con $(d_1, d_2)\rho = (d_2, d_1\delta)$ un automorfismo de orden 128. Sea M un grupo abeliano elemental de orden 97^4. M puede verse como el grupo aditivo del cuerpo finito $\mathbb{F}_{97^4}$.

- Definimos el grupo Q como el producto directo de $R^{(4)}$ y M. Los elementos u, v, w, b, c, centralizan M y a actúa como el producto por una raíz de la unidad (fija) de orden 128 en el cuerpo.

- La acción de P con $R^{(4)}$ está dada por: u, v centralizan $R^{(4)}$ y

$$\begin{aligned}(r_1, r_2, r_3, r_4)^a &= (r_1\rho, r_2\rho, r_3\rho, r_4\rho),\\ (r_1, r_2, r_3, r_4)^w &= (r_4\rho^{64}, r_1, r_2, r_3),\\ (r_1, r_2, r_3, r_4)^b &= (r_1, r_4\rho^{64}, r_3\rho^{64}, r_2\rho^{64}),\\ (r_1, r_2, r_3, r_4)^c &= (r_1, r_2\rho^{64}, r_3, r_4\rho^{64}).\end{aligned}$$

- Escribimos $G = Q \rtimes (\langle u\rangle \times \langle v\rangle \times \langle w\rangle) \rtimes (\langle a\rangle \times \langle b\rangle)$. Entonces $X = G \rtimes \langle c\rangle$.

Tenemos el siguiente teorema:

Teorema 3.5.4 (M. Hertweck). *(a) Existen un automorfismo de G no interno τ y una unidad $t \in \mathcal{V}(\mathbb{Z}G)$ de forma que $g \overset{\tau}{\mapsto} g^t$, para todo $g \in G$.*

(b) En $\mathbb{Z}X$, el elemento c invierte t.

(c) El subgrupo $Y = \langle G, tc\rangle$ de $\mathcal{V}(\mathbb{Z}X)$ es un grupo base de $\mathbb{Z}X$ pero no es isomorfo a X.

(d) El orden de X es $2^{21} \cdot 97^{28}$. El grupo X tiene un 97-subgrupo de Sylow y la longitud derivada de X es 4.

Así, $\mathbb{Z}X \cong \mathbb{Z}Y$ pero $X \ncong Y$

¿Por qué este teorema contradice el Problema del Isomorfismo? Para entenderlo hay que saber lo que es un grupo base: Un grupo base de $\mathbb{Z}X$ es un grupo de unidades de $\mathbb{Z}X$ de modo que a su vez es una base de $\mathbb{Z}X$ sobre $\mathbb{Z}$. Por ejemplo, X es un grupo base de $\mathbb{Z}X$. Ahora, como

se tiene que $\mathbb{Z} \subseteq \mathcal{Z}(\mathbb{Z}X)$, si Y es un grupo base de $\mathbb{Z}X$, podemos aplicar la propiedad universal de los anillos de grupo y tenemos que $\mathbb{Z}X \cong \mathbb{Z}Y$.

En conclusión, el teorema nos está dando dos grupos X e Y de forma que $\mathbb{Z}X \cong \mathbb{Z}Y$ pero $X \ncong Y$, luego se incumple la versión fuerte del Problema del Isomorfismo.

Bibliografía

La referencia principal usada a lo largo del trabajo es [20]. Gran parte de las referencias históricas se han sacado de una introducción no publicada a la investigación en anillos de grupo, realizada por César Polcino Milies: https://www.ime.usp.br/~polcino/group_rings/. También se han consultado de forma continua los apuntes de las asignaturas Álgebra No Conmutativa y, en menor medida, Álgebra Conmutativa, ambos del curso 2017/2018 y realizados por el profesor Jose Luis García Hernández, miembro del Departamento de Matemáticas de la Universidad de Murcia.

Para el trabajo en látex se han consultado de forma continua páginas como Share Latex, TeX StackExchange y la propia wiki de LaTeX; así como específicamente la documentación de `mdframed` [6].

La lista completa se detalla a continuación:

Referencias

[1] **Berman, S. D.** "*On the equation $x^n = 1$ in an integral group ring*". En: *Ukrain. Math. Zh* 7 (*1955*), págs. 253-261.

[2] **Cayley, Arthur**. "*VII. On the theory of groups, as depending on the symbolic equation $\theta^n = 1$*". En: *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* 7.42 (*1854*), págs. 40-47.

[3] **Coleman, D. B.** "*Finite groups with isomorphic group algebras*". En: *Transactions of the American Mathematical Society* 105.1 (*1962*), págs. 1-8.

[4] **Curtis, C.W.** y **Reiner, I.** *Representation Theory of Finite Groups and Associative Algebras*. AMS Chelsea Publishing Series. Interscience, *1966*.

[5] **Dade, Everett C.** "*Deux groups finis distincts ayant la meme algèbre de groupe sur tout corps.*" En: *Mathematische Zeitschrift* 119 (*1971*), págs. 345-348.

[6] **Daniel, Marco** y **Schubert, Elke**. "*The mdframed package*". En: (Abril de *2012*). URL: https://tools.ietf.org/doc/texlive-doc/latex/mdframed/mdframed.pdf.

[7] **Deskins, W. E.** "*Finite Abelian groups with isomorphic group algebras*". En: *Duke Mathematical Journal* 23.1 (mar. de *1956*), págs. 35-40.

[8] **Goodaire, Edgar G.**, **Jespers, Eric** y **Milies, César Polcino**. *Alternative Loop Rings*. North-Holland Mathematics Studies. Elsevier Science, *1996*.

[9] **Hertweck, Martin**. "*A Counterexample to the Isomorphism Problem for Integral Group Rings*". En: *Annals of Mathematics* 154.1 (*2001*), págs. 115-138.

[10] **Higman, Graham**. "*The Units of Group-Rings*". En: *Proceedings of the London Mathematical Society* s2-46.1 (*1940*), págs. 231-248.

[11] **Higman, Graham**. *Units of Group-Rings*. University of Oxford: D.Phil. Thesis, *1940*.

[12] **Hurley, Ted**. "*Group rings for communications*". En: *International Journal of Group Theory* 4.4 (*2015*), págs. 1-23.

[13] **Kaplansky, Irving**. "*"Problems in the Theory of RingsRevisited*". En: *The American Mathematical Monthly* 77.5 (*1970*), págs. 445-454.

[14] **Kruse, R. L.** "*On the Circle Group of a Nilpotent Ring*". En: *The American Mathematical Monthly* 77.2 (*1970*), págs. 168-170.

[15] **Passman, Donald S.** "*Isomorphic groups and group rings*". En: *Pacific Journal of Mathematics* 15.2 (*1965*), págs. 561-583.

[16] **Passman, Donald S.** "*The group algebras of groups of order p^4 over a modular field*". En: *Michigan Math. J.* 12.4 (dic. de *1965*), págs. 405-415.

[17] **Passman, Donald S.** *The algebraic structure of group rings*. Wiley-Interscience, *1977*.

[18] **Perlis, Sam**. "*A characterization of the radical of an algebra*". En: *Bull. Amer. Math. Soc.* 48.2 (feb. de *1942*), págs. 128-132.

[19] **Perlis, Sam** y **Walker, Gordon L.** "*Abelian Group Algebras of Finite Order*". En: *Transactions of the American Mathematical Society* 68.3 (mayo de *1950*), págs. 420-426.

[20] **Polcino Milies, César** y **Sehgal, Sudarshan K.** *An Introduction to Group Rings*. Springer Netherlands, *2002*.

[21] **Roggenkamp, Klaus** y **Scott, Leonard**. "*Isomorphisms of p-adic Group Rings*". En: *Annals of Mathematics* 126.3 (*1987*), págs. 593-647.

[22] **Roggenkamp, K.W.** y **Taylor, M.J.** *Group rings and class groups*. DMV Seminar. Birkhäuser Verlag, *1992*.

[23] **Sandling, Robert**. "*Group rings of circle and unit groups*". En: *Mathematische Zeitschrift* 140.3 (oct. de *1974*), págs. 195-202. ISSN: 1432-1823.

[24] **Scott, L. L.** "*On a conjecture of Zassenhaus and beyond*". En: *Contemp. Math.* 131.1 (*1989*), págs. 325-343.

[25] **Sehgal, Sudarshan K.** *Units in Integral Group Rings*. John Wiley & Sons Canada, Limited, *1993*.

[26] **Sehgal, Sudarshan K.**, **Sehgal, Surinder K.** y **Zassenhaus, Hans J.** "*Isomorphism of integral group rings of abelian by nilpotent class two groups*". En: *Communications in Algebra* 12.19 (*1984*), págs. 2401-2407.

[27] **Weiss, Alfred**. "*Rigidity of p-adic p-Torsion*". En: *Annals of Mathematics* 127.2 (*1988*), págs. 317-332.