Universidad de Murcia

Facultad de Matemáticas

Sobre el Problema del Isomorfismo Modular

Una recopilación de invariantes conocidos de un p-grupo determinados por su álgebra de grupo sobre un cuerpo de característica p

Diego García Lucas

Tutor: Ángel del Río Mateos

Curso 2019/2020

Declaración de originalidad

Diego García Lucas, autor del Trabajo de Fin de Máster "Sobre el Problema del Isomorfismo Modular", 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, y que la obra no infringe el copyright de ninguna persona.

En Murcia, a 21 de junio de 2020

Fdo.: Diego García Lucas.

En la Secretaría de la Facultad de Matemáticas se ha presentado una copia firmada de esta declaración.

Introduction

The Modular Isomorphism Problem ask if, given a modular group algebra $\mathbb{F}_p[G]$, where $\mathbb{F}_p$ is the field with p elements and G is a finite p-group, the isomorphism class of the group G is determined by the isomorphism class of the algebra $\mathbb{F}_p[G]$, in the following sense: if H is another group such that $\mathbb{F}_p[G]$ is isomorphic to $\mathbb{F}_p[H]$, then G must be isomorphic to H. This problem, open for more than sixty years, is the only classic variant of the Isomorphism Problem for group algebras for which there still exist expectations about a general affirmative answer, though at this moment any sort of solution, positive or negative, still seems to be a far perspective. Even if the answer came to be negative, one could always restate the problem as the question: under which circumstances is a group G determined by its modular group algebra $\mathbb{F}_p[G]$? Or, alternatively, how much information about the group G does the group algebra $\mathbb{F}_p[G]$ provide?

In this context, we have settled as purpose of the present work, and as a kind of introduction to the study of the problem, to give a non-exhaustive list of the main invariants of a p-group G determined by its modular group algebra, including almost every elaboration needed to prove that they are indeed determined, assuming only an elementary knowledge of the matter. This results (which extend over the whole Chapter 4) can be found disseminated in the bibliography on the problem, and to the best of our knowledge they had not been approached until now in a comprehensive way in a sole document (with the exception of several relevant surveys, which, as such, do not include the majority of the proofs).

This approach, consisting in searching and classifying invariants of G determined by $\mathbb{F}_p[G]$, has proven its worth, playing an indispensable role in the majority of the positive partial solutions known nowadays for the Modular Isomorphism Problem; nevertheless, generally the knowledge of this invariants does not suffice, and other and more specific ones are required, relying on the specific structure of the groups of the considered class. We will restrict our study to the first ones: this reduction of contents is justified, in an obvious way, by the impossibility of collecting in a work such as this every existing result on the subject; and the selecction of those, by their wider generality and by the fact that, from our point of view, they seem to be more likely to play a relevant role in future results about the Modular Isomorphism Problem than the second ones, even though we do not discard at all that the techniques used to prove those, or generalizations of them, could gain further relevance.

If, on the contrary, one searches for a counterexample (i.e., a pair of finite p-groups G and H such that $G \ncong H$ but $\mathbb{F}_p[G] \cong \mathbb{F}_p[H]$) it is clear that the utility of these invariants, just as the identification of the classes for which the problem has positive answer (and, therefore of every known result), is reduced to provide an easy form to dismiss possible candidates to counterexample.

Regarding to the structure of the present work, in the first chapter all the group-theoretical notions and properties that will become relevant in the main results of our work and in their proofs are presented, assuming only elementary knowledge of the matter. Firstly, nilpotent groups are defined, by means of the lower central series and the upper central series, and several properties of those are described. In particular, we consider the class of finite p-groups, and study a few of their properties. It is also described the Frattini subgroup of an arbitrary group (which is defined as the intersection of all the maximal subgroups, constituting a sort of analogue in Group Theory to the Jacobson Radical), and its alternative characterization as the subgroup made up of all the elements that "are dispensable as generators of the group". It is also presented an explicit characterization

of this subgroup for finite p-groups.

On the other hand, we introduce the so called commutator collection process, a group-theoretical technique used in the proofs of the well-known Hall-Petresco Formula and of Dark's Theorem, among other results. Next, we consider the notion of N_p-serie, and by way of example we define the Brauer-Jennings-Zassenhauss series, or simply $\mathcal{M}$-series, relative to the prime p by

$$\mathcal{M}_{p,1}(G) = G, \qquad \text{and} \qquad \mathcal{M}_{p,n}(G) = (G, \mathcal{M}_{p,n-1}(G)) \cdot \mathcal{M}_{p,i}(G)^{(p)} \qquad \text{for } n > 1,$$

i being the least integer such that $ip \geq n$, and $H^{(n)}$ denoting the subgroup of H generated by the elements of the form h^n, with $h \in H$; for each group H and each integer n. This series will turn out to be essential in the study of group algebras of p-groups over fields with characteristic p, and therefore in the study of the Modular Isomorphism Problem. It is also defined the Lazard series $\{\mathcal{L}_{p,n}(G)\}$ using the terms of the lower central series. The results obtained from the commutator collection process allow us to state a first relation between the former series: concretely, they allow us to settle the inclusion $\mathcal{L}_{p,n}(G) \subseteq \mathcal{M}_{p,n}(G)$ for each integer $n > 0$, and each prime number p. In fact, the reverse inclusion is also true, but its proof will not be performed until the third chapter.

Chapter 2, still of introductory nature, starts with the definition of group algebra $K[G]$ of a group G with coefficients in a field K. Some properties of its elements are presented too, with special attention to the ones in the center and in the subspace of the Lie commutators. It is of outstanding relevance the role of the so-called augmentation ideal of $K[G]$, denoted $\mathrm{Aug}_K(G)$. The presentation of these algebras concludes with the introduction of the group of units, and the group of normalized units of $K[G]$. At this point, we will be in a position to give an suitable introduction to the Modular Isomorphism Problem, presenting it in the context of the Isomorphism Problem and describing some of its variants.

In the third chapter, which, along with the fourth one, constitutes the kernel of our work, the structure of groups algebras of p-groups over fields with characteristic p is studied, the majority of results in that regard being due originally to S.A. Jennings. Concretely, if $K[G]$ is one of such algebras, we proof the equality of the augmentation ideal of $K[G]$ with its Jacobson Radical; it is proved that $K[G]$ is a local ring, and explicit descriptions of the group of units and the group of normalized units are given. Next, we consider the filtration of the augmentation ideal given by its powers $\{\mathrm{Aug}_K(G)^n\}_{n\geq 1}$, it is presented the notion of Jennings' basis (which is a basis of $K[G]$ as a K-vector space whose elements are of a determined form, esasily computable from the group basis G; moreover, a weight is assigned to each one of them), and it is proved that each one of these bases is adapted to the former filtration, i.e., the elements of the basis with weight $t \geq 0$ generate $\mathrm{Aug}_K(G)^t / \mathrm{Aug}_K(G)^{t+1}$ as a K-vector space. Moreover, the relation between the adapted filtrations of the augmentation ideal and the N_p-series of G is established (one can obtain an N_p-series from an adapted filtration, and vice versa); it is of special interest the fact that the N_p-series associated to the filtration $\{\mathrm{Aug}_K(G)^n\}_{n\geq 1}$, the so-called series of the dimension subgroups, coincides with both the Brauer-Jennings-Zassenhauss series and the Lazard series, which proves the equality announced in chapter one. This is one more evidence of the uselfulness of group rings in Group Theory, since this proof uses the group algebra to establish a purely group-theoretical property.

The groups of units and of normalized units of $K[G]$ are studied too, obtaining for the later a system of generators from a Jennings' basis. In the last section of the chapter we focus, in particular, in group algebras over the field of p elements $\mathbb{F}_p$: a few arithmetic results and properties regarding to augmentation ideal and some of its subrings (without one) are presented. The chapter concludes with the definition of the Zassenhauss ideals (using the so-called Lie powers of the augmentation ideal), and obtaining an easier to handle characterization for them. These ideals play a fundamental role in the majority of results regarding to the quotients of the $\mathcal{M}$-serie of Brauer-Jennings-Zassenhaus (specially in the work of S.K. Sehgal), which are elaborated in the next chapter.

Finally, in Chapter 4 the whole theoretical apparatus elaborated in the former chapter is applied to find invariants of G determined by the group algebra $K[G]$, G being an arbitrary finite p-group,

and K a field with characteristic p. In fact, we manage to give in-depth proofs of the fact that the followings invariants of G are determined by $K[G]$:

(I) The exponent of G.

(II) The isomorphism class of the factor groups $\mathcal{M}_{p,n}(G)/\mathcal{M}_{p,n+1}(G)$, for $n \geq 1$.

(III) The isomorphism class of the factor groups $\mathcal{M}_{p,n}(G')/\mathcal{M}_{p,n+1}(G')$, for $n \geq 1$.

(IV) The isomorphism class of G/G'.

(V) The isomorphism class of $\mathcal{Z}(G)$.

(VI) The isomorphism class of G', provided that G is metabelian.

(VII) The minimum number of generators of G and of G'.

(VIII) The nilpotency class of G, provided that at least one the following conditions holds:

a) the exponent of G is p;

b) G' is cyclic;

c) the nilpotency class of G is at most 2.

If, in addition, we assume that K is the field $\mathbb{F}_p$ with p elements, it is proved that the following invariants are determined by $\mathbb{F}_p[G]$:

(X) The isomorphism class of the factor groups $\mathcal{M}_{p,n}(G)/\mathcal{M}_{p,n+2}(G)$, for $n \geq 1$.

(XI) The isomorphism class of the factor groups $\mathcal{M}_{p,n}(G)/\mathcal{M}_{p,2n+1}(G)$, for $n \geq 1$.

(XII) The isomorphism class of the factor group $G/\mathcal{M}_{p,4}(G)$.

(XIII) The nilpotency class of G, provided that G' is elementary-abelian.

(XIV) The isomorphism class of the Sandling quotient $G/\gamma_2(G)^{(p)}\gamma_3(G)$, where $\gamma_i(G)$ denotes the i-th term of the lower central series of G.

As a consequence of some of these results trivial to check that the Modular Isomorphism Problem has an affirmative answer when restricted to the class of abelian groups (in fact, in this case one can omit the hypothesis $K = \mathbb{F}_p$); to the class of p-groups such that the $\mathcal{M}$-series has length 2; to the class of the p-groups, with p odd, such that the $\mathcal{M}$-series has length 3, and to the class of the central-elementary-by-abelian groups.

The chapter concludes, aiming at offering a general viewpoint of the current state of the problem, giving a list of the classes of groups for which the restriction of the Modular Isomorphism Problem has an affirmative answer, and giving sketchs of the proofs in a few cases in order to illustrate the role that the presented invariants play. Besides the considered ones, the classes of finite p-groups for which the isomorphism class of G is known to be determined by its modular group algebra are the ones composed by:

(I) 2-groups of maximal class;

(II) p-groups with center of index p^2;

(III) p-groups of maximal class, with order not greater than p^{p+1} and with a maximal subgroup which is abelian;

(IV) 2-groups of almost maximal class;

(V) metacyclic p-groups;

(VI) elementary-abelian-by-cyclic p-groups;

(VII) p-groups with a cyclic subgroup of index p^2;

(VIII) p-groups with order at most p^5;

(IX) 2-groups with order at most 2^6 (by theoretical proofs) y 2-groups with order at most 2^9 (by computational proofs).

In fact, for the two first classes in the previous list one can omit the hypothesis $K = \mathbb{F}_p$, since it suffices to assume that K is a field of characteristic p. We also present several problems that are deeply entwined with the Modular Isomorphism Problem, such as the Modular Isomorphism Problem for Groups of Units, or the Normal Complement Problem for modular group algebras.

Introducción

El Problema del Isomorfismo Modular plantea si, dada un álgebra de grupo modular $\mathbb{F}_p[G]$, donde $\mathbb{F}_p$ es el cuerpo de p elementos, y G un p-grupo finito, la clase de isomorfía del grupo G está determinada por la del álgebra $\mathbb{F}_p[G]$, en el sentido siguiente: si H es otro grupo tal que $\mathbb{F}_p[G]$ es isomorfo a $\mathbb{F}_p[H]$, entonces G ha de ser isomorfo a H. Este problema, abierto durante ya más de sesenta años, es la única variante clásica del Problema del Isomorfismo para álgebras de grupo para la que aún existen expectativas de una respuesta positiva general, aunque por el momento cualquier respuesta, negativa o afirmativa, parece ser aún una perspectiva lejana. Incluso si la respuesta llegase a ser negativa, siempre se podría replantear el problema como la cuestión: ¿bajo qué condiciones está un grupo G determinado por su álgebra de grupo modular $\mathbb{F}_p[G]$? O, alternativamente: ¿cuánta información sobre el grupo G proporciona el álgebra de grupo $\mathbb{F}_p[G]$?

En este contexto, hemos fijado como objetivo del presente trabajo, a modo de introducción al estudio del problema, dar una lista no exhaustiva de los principales invariantes de un p-grupo G determinados por su álgebra de grupo modular, incluyendo casi todos los desarrollos necesarios para demostrar que efectivamente lo están, partiendo de un nivel elemental. Estos resultados (que comprenderán todo el Capítulo 4) se encuentran, en su mayoría, dispersos por la bibliografía de la materia, y hasta ahora no abordados de forma cohesionada en un mismo documento (a excepción de varios y relevantes *surveys*, que como tales no incluyen la mayoría de las demostraciones).

Este enfoque, el de buscar y catalogar invariantes de G determinados por $\mathbb{F}_p[G]$, ha probado su utilidad, desempeñando un papel imprescindible en la mayoría de las soluciones positivas conocidas a día de hoy a restricciones del Problema del Isomorfismo Modular a algunas clases de p-grupos finitos; sin embargo, en general el conocimiento de estos invariantes no es suficiente, y se requieren otros más específicos, dependientes de la estructura específica de los grupos de la clase considerada. Nos limitaremos al estudio de los primeros: el recorte en los contenidos se justifica de manera obvia por la imposibilidad de recopilar con detalle en un trabajo como este todos los resultados existentes sobre el tema; y la elección de los mismos, por su mayor generalidad y por el hecho de que, desde nuestro punto de vista, parece más probable que representen un papel relevante en ulteriores resultados sobre el Problema del Isomorfismo que los segundos, aunque en ningún caso descartamos que las técnicas que dan lugar a éstos, o generalizaciones de las mismas, puedan llegar a cobrar relevancia.

Si, por contra, uno buscase un contraejemplo (i.e., un par de p-grupos finitos tales que $G \ncong H$ pero $\mathbb{F}_p[G] \cong \mathbb{F}_p[H]$), es obvio que la utilidad de estos invariantes, así como de la identificación de clases a las que la restricción del problema tenga respuesta positiva (y por ende de todos los resultados existentes), se ve reducida a proporcionar una forma rápida de descartar candidatos a posible contraejemplo.

En relación a la estructura del trabajo, en el primer capítulo se presentan todas las nociones y resultados de Teoría de Grupos que cobren alguna relevancia en los principales resultados del trabajo y sus demostraciones, asumiendo sólo conocimientos elementales de la materia. Se comienza definiendo la clase de los grupos nilpotentes, presentando para ello las series centrales inferior y superior, y describiendo algunas propiedades de los mismos. En particular, se considera la clase de los p-grupos finitos, y se dan algunos resultados básicos. También se describe el subgrupo de Frattini de un grupo arbitrario (que se define como la intersección de todos los subgrupos maximales, constituyendo así una suerte de análogo en Teoría de Grupos al ideal de Jacobson),

y su caracterización alternativa como subgrupo conformado por todos los elementos que "son prescindibles a la hora de generar el grupo". También se da una caracterización explícita de este subgrupo en p-grupos finitos.

Por otro lado, se introduce el llamado método de agrupación de conmutadores, una técnica (también enmarcada dentro de la Teoría de Grupos) que nos permite, entre otros resultados, demostrar la conocida Fórmula de Hall-Petresco, así como el Teorema de Dark. A continuación se define noción de N_p-serie, y como ejemplo se considera la serie Brauer-Jennings-Zassenhauss, o $\mathcal{M}$-serie, relativa al primo p, que se define recursivamente mediante

$$\mathcal{M}_{p,1}(G) = G, \qquad \text{y} \qquad \mathcal{M}_{p,n}(G) = (G, \mathcal{M}_{p,n-1}(G)) \cdot \mathcal{M}_{p,i}(G)^{(p)} \qquad \text{para } n > 1,$$

siendo i el menor entero tal que $ip \geq n$, y denotando por $H^{(n)}$ al subgrupo de H generado por todos los elementos de la forma h^n, con $h \in H$; para cada grupo H y cada entero n. Esta serie resultará ser fundamental en el estudio de álgebras de grupo de p-grupos sobre cuerpos de característica p, y por tanto en el del Problema del Isomorfismo Modular. También se define la serie de Lazard $\{\mathcal{L}_{p,n}(G)\}$ a partir de los términos de la serie central inferior. Los resultados obtenidos a partir del método de agrupación de conmutadores nos permiten establecer una primera relación entre las dos series anteriores: concretamente, permiten establecer la inclusión $\mathcal{L}_{p,n}(G) \subseteq \mathcal{M}_{p,n}(G)$ para cada entero $n > 0$, y cada primo p. De hecho, la inclusión recíproca también es cierta, pero no abordamos su demostración hasta el capítulo tercero.

En el Capítulo 2, aún de naturaleza introductoria, se define el concepto de álgebra de grupo $K[G]$, donde K y G son, respectivamente, un cuerpo y un grupo arbitrarios. También se dan algunas propiedades de sus elementos, destacándose los del centro y los del subespacio de los conmutadores de Lie. Es especialmente notable el papel del llamado ideal de aumento de $K[G]$, que denotamos por $\mathrm{Aug}_K(G)$. Se completa la presentación de estas álgebras de grupo introduciendo el grupo de unidades, y el grupo de unidades normalizadas. Estaremos ya en este punto en condiciones de dar una introducción adecuada al Problema del Isomorfismo Modular, presentándolo en el contexto del Problema del Isomorfismo y dando algunas variantes de mismo.

En el tercer capítulo, que junto con el cuarto constituye el núcleo de nuestro trabajo, se estudia la estructura de las álgebras de grupo de p-grupos finitos sobre cuerpos de característica p, estudio, en su mayor parte, desarrollado originariamente por S.A. Jennings. Más concretamente, denotando por $K[G]$ a una de estas álgebras, se identifica el ideal de aumento con el ideal de Jacobson, se deduce que $K[G]$ es un anillo local, y se identifican explícitamente el grupo de unidades y el de unidades normalizadas. A continuación, se presenta la filtración del ideal de aumento dada por sus potencias $\{\mathrm{Aug}_K(G)^n\}_{n\geq 1}$, se introduce la noción de base de Jennings (que será una base de $K[G]$ como K-espacio vectorial, cuyos elementos son de determinada forma obtenida fácilmente a partir del grupo base G; además, a cada uno de estos elementos se le asigna un peso), y se prueba que cada una de estas bases es adaptada a la filtración anterior, i.e., que los elementos de cada peso $t \geq 0$ generan $\mathrm{Aug}_K(G)^t / \mathrm{Aug}_K(G)^{t+1}$ como K-espacio vectorial. Además, también se establece la relación existente entre las filtraciones adaptadas del ideal de aumento y las N_p-series de G (a partir de una N_p-serie puede construirse una filtración adaptada, y viceversa), destacándose que la N_p-serie asociada a la filtración $\{\mathrm{Aug}_K(G)^n\}_{n\geq 1}$, que recibe el nombre de serie de los subgrupos de dimensión, coincide tanto con la serie de Brauer-Jennings-Zassenhaus como con la serie de Lazard, demostrándose así la igualdad anunciada en el primer capítulo. Esta es una muestra más de la utilidad de los anillos de grupo en Teoría de Grupos, pues esta demostración utiliza el álgebra de grupo para probar una propiedad puramente de grupos.

Se estudia también el grupo de unidades y el grupo de unidades normalizadas de $K[G]$, construyendo para el último de ellos un sistema de generadores a partir de una base de Jennings. En la última sección del capítulo se estudian, en particular, las álgebras de grupo sobre el cuerpo de p elementos $\mathbb{F}_p$: se presentan algunos resultados aritméticos, y algunas propiedades relativas al ideal de aumento, y a varios de sus subanillos (sin uno). Se completa el capítulo con la definición de los ideales de Zassenhauss (a partir de las llamadas potencias de Lie del ideal de aumento), y

obteniendo una caracterización mucho más manejable de los mismos. Estos ideales desempeñan un papel fundamental en la mayoría de los resultados relativos a los cocientes de la $\mathcal{M}$-serie de Brauer-Jennings-Zassenhaus (especialmente en el trabajo de S.K. Sehgal), que se desarrollan en el capítulo siguiente.

Finalmente, en el Capítulo 4 se aplica todo el aparato teórico desarrollado el Capítulo 3 para encontrar invariantes de G determinados por el álgebra de grupo $K[G]$, siendo G un p-grupo finito arbitrario y K un cuerpo de característica p. De hecho, se consigue dar demostraciones detalladas de que los siguientes invariantes de G están determinados por $K[G]$:

(I) El exponente de G.

(II) La clase de isomorfía de los grupos cociente $\mathcal{M}_{p,n}(G)/\mathcal{M}_{p,n+1}(G)$, para $n \geq 1$.

(III) La clase de isomorfía de los grupos cociente $\mathcal{M}_{p,n}(G')/\mathcal{M}_{p,n+1}(G')$, para $n \geq 1$.

(IV) La clase de isomorfía de G/G'.

(V) La clase de isomorfía de $\mathcal{Z}(G)$.

(VI) La clase de isomorfía de G', si G es metabeliano.

(VII) El mínimo número de generadores de G y de G'.

(VIII) La clase de nilpotencia de G, supuesta alguna de las siguientes condiciones:

a) el exponente de G es p;

b) G' es cíclico;

c) la clase de nilpotencia de G es a lo sumo 2.

Si además asumimos que K es el cuerpo de p elementos $\mathbb{F}_p$, se demuestra que están determinados por $\mathbb{F}_p[G]$ los invariantes:

(X) La clase de isomorfía de los grupos cociente $\mathcal{M}_{p,n}(G)/\mathcal{M}_{p,n+2}(G)$, para $n \geq 1$.

(XI) La clase de isomorfía de los grupos cociente $\mathcal{M}_{p,n}(G)/\mathcal{M}_{p,2n+1}(G)$, para $n \geq 1$.

(XII) La clase de isomorfía del grupo cociente $G/\mathcal{M}_{p,4}(G)$.

(XIII) La clase de nilpotencia de G, si G' es abeliano elemental.

(XIV) La clase de isomorfía del cociente de Sandling $G/\gamma_2(G)^{(p)}\gamma_3(G)$, donde $\gamma_i(G)$ denota al i-ésimo término de la serie central inferior de G.

Conociendo estos invariantes, es inmediato que el Problema del Isomorfismo Modular tiene respuesta positiva si se restringe a la clase de los grupos abelianos (de hecho, en este caso podemos omitir la hipótesis $K = \mathbb{F}_p$); a la de los p-grupos tales que la $\mathcal{M}$-serie tiene longitud 2; a la de los p-grupos, con p impar, tales que la $\mathcal{M}$-serie tiene longitud 3; y a la de los p-grupos central-elemental-por-abeliano.

Completamos el capítulo, con el fin de ofrecer una visión general del estado actual del problema, dando una lista de las clases de grupos para las que (la restricción de) el Problema del Isomorfismo Modular tiene respuesta positiva, y dando esquemas de las demostraciones de unos pocos casos, para ilustrar el papel que desempeñan en tales demostraciones los invariantes encontrados. Además de las ya consideradas, las clases de p-grupos finitos para las que la clase de isomorfía de G se sabe determinada por su álgebra de grupo modular son las de los:

(I) 2-grupos de clase maximal;

(II) p-grupos con centro de índice p^2;

(iii) p-grupos de clase maximal, orden no mayor que p^{p+1} y con un subgrupo maximal abeliano;

(iv) 2-grupos de clase casi maximal;

(v) p-grupos metacíclicos;

(vi) p-grupos abeliano-elemental-por-cíclico;

(vii) p-grupos con un subgrupo cíclico de índice p^2;

(viii) p-grupos de orden a lo sumo p^5;

(ix) 2-grupos de ordena lo summo 2^6 (con demostraciones teóricas) y 2-grupos de orden a lo sumo 2^9 (con demostraciones computacionales).

De hecho, para las dos primeras clases del listado anterior se puede omitir la hipótesis $K = \mathbb{F}_p$, siendo suficiente asumir que K es un cuerpo de característica p. También se presentan algunos problemas estrechamente relacionados con el del Isomorfismo Modular, como el Problema del Isomorfismo Modular para Grupos de Unidades, o el Problema del Complemento Normal para álgebras de grupo modulares.

Índice general

Introduction v

Introducción ix

1. Preliminares sobre grupos 1
1.1. Algunas clases de grupos 1
1.2. Conmutadores n-arios 11
1.3. Series de Lazard y de Brauer-Jennings-Zassenhaus 19

2. Álgebras de grupo 23
2.1. La noción de álgebra de grupo 23
2.2. Aplicación de aumento e ideales de aumento 28
2.3. El Problema del Isomorfismo 33

3. Álgebras de grupo sobre cuerpos de característica p 35
3.1. El ideal de aumento 35
3.2. Filtraciones del ideal de aumento y subgrupos de dimensión 37
3.3. El grupo de unidades normalizadas 46
3.4. Álgebras de grupo modulares e ideales de Zassenhaus 48

4. Invariantes determinados por el álgebra de grupo 59
4.1. Objetos determinados por un álgebra de grupo 59
4.2. Invariantes determinados por $K[G]$ 61
4.3. Invariantes determinados por $\mathbb{F}_p[G]$ 69
4.4. El Problema del Isomorfismo Modular 90

Índice alfabético 99

Bibliografía 101

Capítulo 1

Preliminares sobre grupos

Dedicamos este primer capítulo a presentar la mayor parte de los resultados de Teoría de Grupos que desempeñen algún papel relativamente central en los resultados sobre el Problema del Isomorfismo Modular que probaremos en este trabajo. Así, se comienza dando una lista de las principales clases de grupos (y sobre todo de p-grupos) que intervendrán en resultados ulteriores, así como describiendo algunas de sus propiedades. Se concluye el capítulo con la introducción de las series de Lazard y Brauer-Jennings-Zassenhaus (tercera sección), que son fundamentales en el estudio del problema que nos ocupa, así como las propiedades de las mismas que se pueden obtener eficientemente con argumentos puramente de Teoría de Grupos; estos argumentos, a su vez, se apoyan en resultados obtenidos mediante el llamado *método de agrupación de conmutadores*, que es detallado en la sección segunda.

La primera sección recoge resultados variados de [29], [16] y [9], entre otros. Las dos secciones restantes son, esencialmente, una selección de los resultados de Teoría de Grupos del Capítulo 11 de [33].

1.1. Algunas clases de grupos

En todo el texto p denotará, salvo indicación expresa, un número natural primo. Asumimos conocidas las nociones y resultados más básicos de Teoría de Grupos (e.g., los teoremas de isomorfismo, o la noción de serie de composición), para las que nos remitimos a [9] y al primer capítulo de [29]. Comenzamos enunciando el bien conocido Teorema Fundamental de los Grupos Abelianos Finitos.

Teorema 1.1.1 (Fundamental de los Grupos Abelianos Finitos)**.** *Sea G un grupo abeliano finito. Entonces existe una única lista de enteros $(m_1, m_2, \ldots, m_k)$, todos mayores que 1, tales que*

$$|G| = m_1 m_2 \ldots m_k, \qquad y \qquad m_1 | m_2 | \ldots | m_k,$$

y $G = C_{m_1} \oplus C_{m_2} \oplus \cdots \oplus C_{m_k}$, donde cada C_{m_i} es un subgrupo cíclico de G de orden m_i, y $\oplus$ denota al producto directo de grupos.

Referencia de la demostración. Ver Teorema 8.3.1 de [9]. □

Definición 1.1.2. Sea G un grupo abeliano, y sea $(m_1, \ldots, m_k)$ la lista de enteros dada en el teorema anterior. Entonces decimos que G es de *tipo* $(m_1, \ldots, m_k)$.

Continuamos con el conocido concepto de conmutador:

Definición 1.1.3. Dados dos elementos x, y en un grupo G, se define el *conmutador* de x e y como el elemento $(x, y) = x^{-1}y^{-1}xy \in G$.

Definición 1.1.4. Dados dos subgrupos H_1, H_2 de G, denotamos por (H_1, H_2) al subgrupo de G generado por el subconjunto:

$$\{(h_1, h_2) \ : \ h_1 \in H_1, h_2 \in H_2\}.$$

En particular, el grupo $G' = (G, G)$ recibe el nombre de *subgrupo conmutador*, o *subgrupo derivado*.

Es casi inmediato observar que:

Lema 1.1.5. Sea G un grupo y N un sugrupo normal de G. Entonces

(I) G' es un subgrupo normal de G.

(II) G/G' es abeliano.

(III) G/N es abeliano si y solo si $G' \subseteq N$.

Demostración. Claramente para cada $x, y \in G$ se tiene la identidad $xy = yx(x, y)$. Si $x \in G'$, entonces $x(x, y) \in G'$, por lo que esta igualdad prueba que $G'y \subseteq yG'$ para cada $y \in G$, y como la inclusión opuesta se sigue por simetría, ya tenemos (I). La misma identidad da que G/G' es abeliano, pues para cada $x, y \in G$, los elementos $xy = yx(x, y)$ e yx coinciden en el grupo cociente. Finalmente, si $G' \subseteq N$ el mismo argumento da que G/N es abeliano; y recíprocamente, si G/N es abeliano, entonces $(x, y) = (xy)^{-1}xy \in N$ para cada $x, y \in G$, por lo que $G' \subseteq N$.

□

El grupo cociente G/G' recibe el nombre de *abelianizado* de G.

Definición 1.1.6. Un grupo G se dice *metabeliano* si tiene un subgrupo normal abeliano N tal que G/N es abeliano.

Observación 1.1.7. A la luz del Lema 1.1.5 se hace evidente que un grupo G es metabeliano si y sólo si G' es abeliano. En efecto, si hay un grupo normal N tal que G/N es abeliano, por el mencionado lema $G' \subseteq N$, y por tanto G' es abeliano; la implicación recíproca es trivial.

De forma similar, se define:

Definición 1.1.8. Un grupo G se dice *metacíclico* si tiene un subgrupo normal cíclico N tal que G/N es cíclico.

Series centrales y grupos nilpotentes

Para definir y estudiar la noción de grupo nilpotente necesitaremos considerar ciertas cadenas de subgrupos, las llamadas *serie central inferior* y *serie central superior*:

Definición 1.1.9. Dado un grupo G, se define la *serie central inferior* $\{\gamma_n(G)\}_{n\in\mathbb{N}}$ por recursión natural mediante:

(I) $\gamma_1(G) = G$;

(II) $\gamma_{n+1}(G) = (\gamma_n(G), G)$, para cada $n \geq 1$.

Definición 1.1.10. Sea G un grupo y $\{\gamma_n(G)\}_{n\in\mathbb{N}}$ su serie central inferior. Decimos que G es *nilpotente* si existe un entero c tal que $\gamma_{c+1}(G) = \{1\}$. Al menor de tales enteros c se lo denomina *clase de nilpotencia* de G, y lo denotaremos por $c(G)$.

Recordemos que el centro de un grupo G se define como el subgrupo:

$$\mathcal{Z}(G) = \{g \in G \ : \ gx = xg \text{ para cada } x \in G\}.$$

Podemos dar entonces la siguiente:

Definición 1.1.11. Dado un grupo G, se define la *serie central superior* $(\mathcal{Z}_n(G))_{n\in\mathbb{N}}$ por recursión natural mediante:

(I) $\mathcal{Z}_0(G) = \langle 1\rangle$;

(II) $\frac{\mathcal{Z}_{n+1}(G)}{\mathcal{Z}_n(G)} = \mathcal{Z}(\frac{G}{\mathcal{Z}_n(G)})$, para cada $n \geq 0$.

En otras palabras, para $n \geq 1$, $\mathcal{Z}_{n+1}$ es la imagen inversa de $\mathcal{Z}(G/\mathcal{Z}_n(G))$ por el homomorfismo canónico $G \to G/\mathcal{Z}_n(G)$. Además, todo elemento de $\mathcal{Z}_{n+1}(G)$ es central en G módulo $\mathcal{Z}_n(G)$, i.e.,

$$(\mathcal{Z}_{n+1}(G), G) \subseteq \mathcal{Z}_n(G). \tag{1.1}$$

Observación 1.1.12. Es claro que ambas series centrales consisten en subgrupos característicos de G: para la inferior, basta aplicar inducción notando que $\varphi((g,h)) = (\varphi(g), \varphi(h))$ para cada $g, h \in G$ y cada automorfismo φ de G; para la superior se puede usar también un razonamiento inductivo, teniendo en cuenta esta vez que el centro de un grupo es un subgrupo característico, y que los automorfismos de G inducen automorfismos del grupo cociente G/N, siempre que N sea un subgrupo normal característico. Nótese también que $\gamma_2(G) = (G, G) = G'$, y que $\mathcal{Z}_1(G) = \mathcal{Z}(G)$.

Lema 1.1.13. Sean H y N subgrupos de G con $N \lhd G$. Entonces para cada entero n tenemos que $\gamma_n(H) \subseteq \gamma_n(G)$ y que $\gamma_n(G/N) = \gamma_n(G)N/N$.

Si además suponemos que G es nilpotente de clase c, entonces H y G/N son nilpotentes, con $c(H) \leq c$ y $c(G/N) \leq c$. Aún más, para cada $n \leq c$ se tiene que $\mathcal{Z}_n(G) \supseteq \gamma_{c+1-n}(G)$, y por tanto $\mathcal{Z}_c(G) = G$.

Demostración. Probaremos la primera afirmación por inducción sobre n. Para $n = 1$ el resultado se tiene trivialmente, pues se reduce a las aserciones $H \subseteq G$ y $G/N = GN/N$. Supongamos la afirmación cierta para n. Entonces, de $\gamma_n(H) \subseteq \gamma_n(G)$ se sigue que

$$\gamma_{n+1}(H) = (\gamma_n(H), H) \subseteq (\gamma_n(G), G) = \gamma_{n+1}(G).$$

Veamos ahora que $\gamma_{n+1}(G/N) = \gamma_{n+1}(G)N/N$. Si denotamos con una barra superior al homomorfismo proyección $\bar{\cdot} : G \to G/N$, con $g \mapsto \bar{g} = gN$, será suficiente probar que $\gamma_{n+1}(\overline{G}) = \overline{\gamma_{n+1}(G)}$. Sean $y \in G$ y $x \in \gamma_n(G)$. Entonces $\bar{y} \in \overline{G}$, y como por hipótesis de inducción $\gamma_n(\overline{G}) = \overline{\gamma_n(G)}$, también $\bar{x} \in \gamma_n(\overline{G})$. Luego

$$\overline{(x,y)} = (\bar{x}, \bar{y}) \in (\gamma_n(\overline{G}), \overline{G}) = \gamma_{n+1}(\overline{G}).$$

Como $\gamma_{n+1}(G)$ está generado por los conmutadores de la forma (x, y), con $x \in \gamma_n(G)$ e $y \in G$, se concluye que $\overline{\gamma_{n+1}(G)} \subseteq \gamma_{n+1}(\overline{G})$. Para ver el recíproco, sean $\bar{x} \in \gamma_n(\overline{G})$, y $\bar{y} \in \overline{G}$. Entonces $\bar{y}$ ha de tener alguna imagen inversa $y \in G$, mientras que por la hipótesis de inducción también $\bar{x}$ tiene alguna imagen inversa $x \in \gamma_n(G)$. Entonces

$$(\bar{x}, \bar{y}) = \overline{(x,y)} \in \overline{\gamma_{n+1}(G)};$$

y como el grupo $\gamma_{n-1}(\overline{G})$ está generado por los conmutadores de la forma $(\bar{x}, \bar{y})$, con $\overline{x} \in \gamma_n(\overline{G})$ e $\overline{y} \in \overline{G}$, se tiene la otra inclusión $\gamma_{n+1}(\overline{G}) \subseteq \overline{\gamma_{n+1}(G)}$. Queda así probada la igualdad entre estos dos grupos, y por tanto también completo el paso inductivo.

Pasamos ahora a la segunda afirmación. Supongamos que G es nilpotente de clase c. Entonces $\gamma_{c+1}(G) = \langle 1\rangle$. Así, se sigue directamente de la primera afirmación que tanto H como G/N son ambos nilpotentes de clase a lo sumo c (pues sería $\gamma_{c+1}(H) \subseteq \langle 1\rangle$, y $\gamma_{c+1}(G/N) = \langle 1\rangle N/N = \langle 1\rangle$).

Finalmente, probaremos por inducción finita que $\mathcal{Z}_n(G) \supseteq \gamma_{c+1-n}(G)$ para $n \leq c$. El caso $n = 0$ es trivial por ser $c(G) = c$. Supongamos entonces que $\mathcal{Z}_n(G) \supseteq \gamma_{c+1-n}(G)$, con $n < c$. Entonces

$$(\gamma_{c-n}(G), G) = \gamma_{c+1-n}(G) \subseteq \mathcal{Z}_n(G),$$

y por tanto $\gamma_{c-n}(G)$ es central en G módulo $\mathcal{Z}_n(G)$, así que:

$$\frac{\gamma_{c-n}(G)\mathcal{Z}_n(G)}{\mathcal{Z}_n(G)} \subseteq \mathcal{Z}\left(\frac{G}{\mathcal{Z}_n(G)}\right) = \frac{\mathcal{Z}_{n+1}(G)}{\mathcal{Z}_n(G)},$$

y por tanto $\gamma_{c-n}(G) \subseteq \mathcal{Z}_{n+1}(G)$, lo que completa el paso inductivo. En particular, $\mathcal{Z}_c(G) = G$. □

Observación 1.1.14. En las condiciones del lema anterior, es directo que $c(G/N)$ es el menor entero n tal que $\gamma_{c+1}(G) \subseteq N$. En efecto, $\gamma_{n+1}(G/N) = \gamma_{n+1}(G)N/N$; el primer grupo es trivial si y sólo si $n \geq c(G/N)$, y el segundo es $\{1\}$ si y sólo si $\gamma_{n+1}(G) \subseteq N$, de modo que la observación se sigue.

Lema 1.1.15. Sea $c \geq 1$ un entero y G un grupo. Entoces G es nilpotente de clase c si y sólo si $\mathcal{Z}_c(G) = G$ y $\mathcal{Z}_{c-1}(G) \neq G$.

Demostración. En primer lugar, afirmamos que si $\mathcal{Z}_c(G) = G$, entonces $\gamma_{c+1}(G) = \{1\}$, de modo que $c(G) \leq c$. En efecto, basta notar $\mathcal{Z}_c(G) = G$ implica, por la ecuación (1.1), que

$$\gamma_2(G) = (\mathcal{Z}_c(G), G) \subseteq \mathcal{Z}_{c-1}(G),$$

esto a su vez implica que

$$\gamma_3(G) \subseteq (\mathcal{Z}_{c-1}(G), G) \subseteq \mathcal{Z}_{c-2}(G),$$

de modo que repitiendo el razonamiento $c-2$ veces más se llega a que $\gamma_{c+1}(G) \subseteq \mathcal{Z}_0(G) = \{1\}$.

Podemos ya probar el lema. Si G es nilpotente de clase c, por el lema anterior se tiene que $\mathcal{Z}_c(G) = G$, y si fuese $\mathcal{Z}_{c-1}(G) = G$ la afirmación inicial nos llevaría a la contradicción $c = c(G) \leq c - 1$. Recíprocamente, si $\mathcal{Z}_c(G) = G$ y $\mathcal{Z}_{c-1}(G) \neq G$ la afirmación da que $c(G) \leq c$, y si la desigualdad fuese estricta la implicación directa daría que $\mathcal{Z}_{c-1}(G) = G$.

□

Más adelante necesitaremos de los siguientes lemas auxiliares:

Observación 1.1.16. Si G es un grupo no trivial, un argumento inductivo sencillo da que $c(G') < c(G)$. En efecto, $\gamma_1(G') = G' = \gamma_2(G)$., y si suponemos que $\gamma_n(G') \subseteq \gamma_{n+1}(G)$, entonces

$$\gamma_{n+1}(G') = (\gamma_n(G'), G') \subseteq (\gamma_{n+1}(G), G') \subseteq (\gamma_{n+1}(G), G) = \gamma_{n+2}(G).$$

Por tanto, si $c = c(G)$, entonces $\gamma_c(G') \subseteq \gamma_{c+1}(G) = \{1\}$, y nuestra observación se sigue.

Lema 1.1.17. Sea G un grupo nilpotente cuyos elementos todos tienen orden finito. Si G es finitamente generado, entonces G es un grupo finito.

Demostración. Sea G un grupo como en el enunciado; procedemos por inducción sobre $c = c(G)$. Para $c = 0, 1$, G es abeliano, y por tanto $|G| \leq r \cdot s$, donde r es el número de generadores, y s el máximo de los órdenes de los elementos de G.

Supongamos entonces $c \geq 2$, y sea $\overline{G} = G/\gamma_c(G)$. Entonces, por la primera parte del Lema 1.1.13 se tiene que $\gamma_c(\overline{G}) = \{1\}$, y por tanto $c(\overline{G}) \leq c - 1$; y como $\overline{G}$ sigue siendo finitamente generado y sus elementos tienen orden finito, la hipótesis de inducción garantiza que $\overline{G}$ es finito. Pero también por la demostración del Lema 1.1.15 uno tiene que $\gamma_c(G) \subseteq \mathcal{Z}_1(G) = \mathcal{Z}(G)$ así que

$$(G : \mathcal{Z}(G)) \leq (G : \gamma_c(G)) = |\overline{G}| < \infty.$$

Sea ahora X un transversal de $\mathcal{Z}(G)$ en G, que por lo anterior será finito. Entonces cada elemento de G es de la forma zx, con $z \in \mathcal{Z}(G)$ y $x \in X$, de donde se sigue fácilmente que todos los conmutadores de G son de la forma (x, y) con $x, y \in X$; esto implica que G' es finitamente generado, de modo que (recordando la observación anterior) por la hipótesis de inducción será finito; en consecuencia, también es finito $\gamma_c(G) \subseteq G'$. Por tanto,

$$|G| = (G : \gamma_c(G)) \cdot |\gamma_c(G)| < \infty,$$

el resultado buscado.

□

Lema 1.1.18. Sea G un grupo nilpotente, y $\{1\} \neq H \trianglelefteq G$. Entonces $H \cap \mathcal{Z}(G) \neq \{1\}$.

Demostración. Sea $c = c(G)$. Como $G = \mathcal{Z}_c(G)$, existirá algún índice i que sea el menor entero positivo tal que $\mathcal{Z}_i(G) \cap H \neq \{1\}$. Se ve directamente, teniendo en cuenta que H es normal y la ecuación (1.1), que

$$(H \cap \mathcal{Z}_i(G), G) \subseteq H \cap \mathcal{Z}_{i-1}(G) = \{1\},$$

es decir, que el subgrupo $H \cap \mathcal{Z}_i(G)$ es central en G, y por tanto $H \cap \mathcal{Z}_i(G) \subseteq H \cap \mathcal{Z}(G)$. □

p-grupos finitos

Definición 1.1.19. Sea G un grupo finito. Decimos que G es un *p-grupo finito* si el orden de cada uno de sus elementos es una potencia de p.

En todo lo que sigue emplearemos la siguiente notación: dado un grupo G, y $n \geq 1$ un entero, denotaremos por

$$G^{(n)} = \langle x^n \ : \ x \in G \rangle$$

al subgrupo generado por las potencias n-ésimas de los elementos de G. Claramente, todos estos subgrupos son característicos en G.

Proposición 1.1.20. Sea G un p-grupo abeliano finito. Entonces los órdenes de los subgrupos $G^{(p^e)}$, para todo $e \geq 1$, determinan la clase de isomorfismo de G en el siguiente sentido: si H es otro grupo tal que $|H^{(p^e)}| = |G^{(p^e)}|$ para cada $e \geq 1$, entonces $G \cong H$.

Demostración. Por ser p-grupo abeliano, el Teorema Fundamental de los Grupos Abelianos Finitos (ver Teorema 1.1.1) nos permite escribir G como un producto directo de grupos cíclicos C_{p^i}, digamos $G = \bigoplus_{i=1}^{m} (C_{p^i})^{n_i}$. Claramente la clase de isomorfismo de G está determinada por los n_i. Además, para cada $e \geq 0$, se tiene que

$$G^{(p^e)} = \bigoplus_{i=e+1}^{m} (C_{p^{i-e}})^{n_i}.$$

Si llamamos $f(e)$ al entero (dependiente sólo de los ordenes de los subgrupos considerados) que verifica

$$p^{f(e)} = |G^{(p^{e-1})}|/|G^{p^e}| = p^{n_e + n_{e+1} + \cdots + n_m},$$

se sigue que $f(e) - f(e+1) = n_e$ para cada $e \geq 1$, y el resultado queda probado.

□

Usamos la siguiente observación para fijar notación:

Observación 1.1.21. Dado un grupo cualquiera G, denotaremos por $\mathrm{Cl}(G)$ al conjunto de las clases de conjugación de G; si dos elementos $g, h \in G$ son conjugados escribiremos $g \sim h$. Si además G es un grupo finito, dado que $\mathrm{Cl}(G)$ forma una partición de G, se obtiene la llamada *ecuación de clases*:

$$|G| = \sum_{C \in \mathrm{Cl}(G)} |C|,$$

de la cual se deduce fácilmente, teniendo en cuenta que un elemento está el centro $\mathcal{Z}(G)$ si y sólo si su clase de conjugación tiene un único elemento, la ecuación

$$|G| = |\mathcal{Z}(G)| + \sum_{C \in \mathrm{Cl}(G) \ : \ |C| > 1} |C|.$$

Teorema 1.1.22. *Sea G un p-grupo finito no trivial. Entonces $\mathcal{Z}(G) \neq \{1\}$.*

Demostración. Sea $|G| = p^m$ para cierto entero positivo n. Si fuese $\mathcal{Z}(G) = \{1\}$, sólo habría una clase de conjugación con un único elemento, de modo que la ecuación de clases sería de la forma:

$$p^m = |\mathcal{Z}(G)| + \sum_{C \in \mathrm{Cl}(G) \ : \ |C| > 1} |C| = 1 + \sum_{C \in \mathrm{Cl}(G) \ : \ |C| > 1} |C|,$$

y como cada $|C| > 1$ es una potencia de p, se seguiría que $p|1$, contradicción. □

Como consecuencia obtenemos los tres resultados siguientes:

Teorema 1.1.23. *Todo p-grupo finito es nilpotente.*

Demostración. Sea G un p-grupo finito. Observemos que si para algún índice i se tiene que $\mathcal{Z}_i(G) \neq G$, entonces $\mathcal{Z}_i(G) < \mathcal{Z}_{i+1}(G)$. En efecto, de $\mathcal{Z}_i(G) \neq G$ se sigue que $G/\mathcal{Z}_i(G)$ es un p-grupo no trivial, de modo que por el Teorema 1.1.22 se tendrá que

$$\{1\} \neq \mathcal{Z}\left(\frac{G}{\mathcal{Z}_i(G)}\right) = \frac{\mathcal{Z}_{i+1}(G)}{\mathcal{Z}_i(G)},$$

por lo que $\mathcal{Z}_i(G) < \mathcal{Z}_{i+1}(G)$. Entonces la serie central superior es estrictamente decreciente mientras no alcance a G, de modo que, como G es finito, $\mathcal{Z}_n(G) = G$ para algún entero $n \geq 1$, con lo que la nilpotencia de G se sigue del Lema 1.1.15. □

En las próximas demostraciones será útil la siguiente observación elemental.

Observación 1.1.24. Un grupo es abeliano si y sólo si $G/\mathcal{Z}(G)$ es cíclico. En efecto, si G es abeliano $G = \mathcal{Z}(G)$, y por tanto $G/\mathcal{Z}(G) = \{1\}$ es cíclico de orden 1. Recíprocamente, si el cociente considerado es cíclico, si $\bar{g} = g\mathcal{Z}(G)$ es un generador de $G/\mathcal{Z}(G)$, es claro que $\mathcal{Z}(G) \cup \{g\}$ es un conjunto de generadores de G, y como g conmuta con todos los elementos del centro, se deduce que G es abeliano. De hecho, en tal caso $\mathcal{Z}(G) = G$, y el cociente siempre es cíclico de orden 1.

Proposición 1.1.25. Todo grupo de orden p^2 es abeliano.

Demostración. Sea G un p-grupo de orden p^2. Por el Teorema 1.1.22 el centro de G es no trivial, por lo que o bien $|\mathcal{Z}(G)| = p^2$ o bien $|\mathcal{Z}(G)| = p$. En consecuencia, $(G : \mathcal{Z}(G))$ es o bien p o bien 1; en cualquier caso el grupo cociente $G/\mathcal{Z}(G)$ es cíclico, y el resultado se sigue de la Observación 1.1.24.

□

Proposición 1.1.26. Sea G un grupo de orden p^n y N un subgrupo normal de G de orden p^k. Entonces existe una serie normal

$$\{1\} = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_k = N \leq \cdots \leq G_n = G$$

con $G_i \trianglelefteq G$ y $(G_{i+1} : G_i) = p$ para cada i. En particular, un p-grupo finito tiene subgrupos normales de todos los órdenes posibles.

Demostración. Razonamos por inducción sobre n. Si $n = 1$ ó 2 el resultado es trivial; sea entonces $n > 2$. Supongamos primero que $N \neq 1$. Entonces por el Teorema 1.1.22 sabemos que $N \cap \mathcal{Z}(G) \neq \{1\}$. Elijamos cualquier subgrupo G_1 de $N \cap \mathcal{Z}(G)$ de orden p. Entonces es claro que G_1 es normal, G/G_1 es un p-grupo de orden p^{n-1}, y la hipótesis de inducción garantiza la existencia de una serie normal:

$$\{1\} = \frac{G_1}{G_1} \leq \frac{G_2}{G_1} \leq \cdots \leq \frac{G_k}{G_1} = \frac{N}{G_1} \leq \cdots \leq \frac{G_n}{G_1} = \frac{G}{G_1},$$

donde los cocientes de términos sucesivos tienen orden p, y los G_i son subgrupos normales de G; así, se deduce directamente que la serie

$$\{1\} = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_k = N \leq \cdots \leq G_n = G$$

verifica las condiciones del enunciado. Por otro lado, si fuese $N = \{1\}$, tomando G_1 como cualquier subgrupo de $\mathcal{Z}(G)$ de orden p, cualquier serie como la construida arriba da el resultado.

□

En particular, el resultado anterior garantiza que un p-grupo es simple si y sólo si es cíclico de orden p.

Proposición 1.1.27. Sea G un grupo de orden $p^n \geq p^2$. Entonces:

(I) La clase de nilpotencia de G es a lo sumo $n-1$.

(II) Si $c(G) = c$, entonces $(G : \mathcal{Z}_{c-1}(G)) \geq p^2$.

(III) $(G : G') \geq p^2$.

Demostración. Sea c la clase de nilpotencia de G. Probaremos primero (II). Supongamos por reducción al absurdo que $(G : \mathcal{Z}_{c-1}(G)) < p^2$. Como por el Lema 1.1.15 $G \neq \mathcal{Z}_{c-1}(G)$, necesariamente $(G : \mathcal{Z}_{c-1}(G)) = p$. Si fuese $c = 1$, lo anterior implica que $|G| = p$, lo que contradice nuestra hipótesis; podemos suponer entonces $c \geq 2$. Entonces el grupo

$$\frac{G/\mathcal{Z}_{c-2}(G)}{\mathcal{Z}\left(G/\mathcal{Z}_{c-2}(G)\right)} = \frac{G/\mathcal{Z}_{c-2}(G)}{\mathcal{Z}_{c-1}(G)/\mathcal{Z}_{c-2}(G)} \cong \frac{G}{\mathcal{Z}_{c-1}(G)}$$

es cíclico, por lo que $G/\mathcal{Z}_{c-2}(G)$ es abeliano (por la Observación 1.1.24); se sigue entonces

$$\frac{G}{\mathcal{Z}_{c-2}(G)} = \mathcal{Z}\left(\frac{G}{\mathcal{Z}_{c-2}(G)}\right) = \frac{\mathcal{Z}_{c-1}(G)}{\mathcal{Z}_{c-2}(G)},$$

por lo que $G = \mathcal{Z}_{c-1}(G)$, contradicción. Esto prueba (II). De esto, y dado que por el Lema 1.1.13 vale la inclusión $G' = \gamma_2(G) \subseteq \mathcal{Z}_{c-1}(G)$, se sigue que

$$(G : G') \geq (G : \mathcal{Z}_{c-1}(G)) \geq p^2,$$

con lo que (III) también queda probado. Finalmente, como sabemos que los cocientes $\gamma_i(G)/\gamma_{i+1}(G)$ son no triviales si $i \leq c$ (pues de lo contrario cada $\gamma_j(G) = \gamma_i(G) \neq \{1\}$ para $j > i$, y el grupo no sería nilpotente), se tiene que

$$p^n = |G| = |G/\gamma_2(G)| \cdot |\gamma_2(G)/\gamma_3(G)| \cdots |\gamma_c(G)/\gamma_{c+1}(G)|;$$

es un producto de c factores, todos potencias no triviales de p, siendo el primero de ellos $\geq p^2$. Se sigue entonces que $p^n \geq p^{c+1}$, y por tanto que $n - 1 \geq c$.

□

Corolario 1.1.28. *Sea G un p-grupo y N un subgrupo normal de G de índice $p^i \geq p^2$. Entonces $\gamma_i(G) \leq N$.*

Demostración. El grupo G/N tiene orden p^i, de modo que por el apartado (I) de la Proposición 1.1.27 sabemos que $c\,(G/N) \leq i - 1$. En consecuencia, y usando el Lema 1.1.13, vale

$$\{\overline{1}\} = \gamma_i\,(G/N) = \gamma_i(G)N/N,$$

por lo que necesariamente $\gamma_i(G) \leq N$. □

A la vista del apartado (I) de la última proposición cobran sentido las definiciones siguientes:

Definición 1.1.29. Decimos que un p-grupo finito G de orden p^n es de *clase maximal* si su clase de nilpotencia es $c(G) = n - 1$.

Definición 1.1.30. Decimos que un p-grupo finito G de orden p^n es de *clase casi maximal* si su clase de nilpotencia es $c(G) = n - 2$.

Damos unas pocas propiedades relativas a los grupos de clase maximal, aunque no profundizaremos más en esta clase de grupos.

Lema 1.1.31. Si un p-grupo G es de clase maximal, entonces $(G : G') = p^2$, y para cada $1 < i \leq c$, $(\gamma_i(G) : \gamma_{i+1}(G)) = p$. En consecuencia, $(G : \gamma_i(G)) = p^i$ para $2 \leq i \leq n$.

Demostración. Supongamos que G es un p-grupo de orden p^n y clase de nilpotencia c. Claramente podemos escribir, como en la demostración de la Proposición 1.1.27:

$$p^n = |G| = |G/\gamma_2(G)| \cdot |\gamma_2(G)/\gamma_3(G)| \cdots |\gamma_c(G)/\gamma_{c+1}(G)|;$$

siendo cada uno de estos factores es una potencia de p distinta de 1.

Si G es de clase maximal, entonces $n = c + 1$, y en la expresión anterior $p^n = p^{c+1}$ sería un producto de c potencias no triviales de p. Por tanto, la única posibilidad es que todos los factores sean p excepto uno, que tome el valor p^2. Y éste, por el apartado (III) de la Proposición 1.1.27, necesariamente es $(G : G') = |G/G'|$. Con esto, última afirmación se sigue directamente de la igualdad

$$|G| = |G/\gamma_2(G)| \cdot |\gamma_2(G)/\gamma_3(G)| \cdots |\gamma_{i-1}(G)/\gamma_i(G)| \cdot |\gamma_i(G)| = p^i \cdot |\gamma_i(G)|.$$

□

Definición 1.1.32. Sea G un grupo. De un subgrupo propio H de G decimos que es un *subgrupo maximal* si para cada subgrupo L tal que $H \leq L \leq G$ se tiene que o bien $H = L$ o bien $G = L$.

Evidentemente, si G es un grupo finito cada subgrupo propio de G está contenido en al menos un subgrupo maximal; además, es claro que cada subgrupo cuyo índice en G sea un número primo ha de ser maximal en G.

Lema 1.1.33. Sea G un p-grupo de clase maximal, con $|G| = p^n$. Entonces los únicos subgrupos normales de G son los de la serie $\{\gamma_i(G)\}_{i\geq 1}$ y los subgrupos maximales. En particular, si N es un subgrupo normal de G de índice $p^i \geq p^2$, entonces $N = \gamma_i(G)$.

Demostración. Sea N cualquier subgrupo normal de G, y escribamos $(G : N) = p^i$. Si $i = 0$ ó $i = 1$ claramente N es o bien G o bien maximal en G. Si $i \geq 2$, entonces $\gamma_i(G) \leq N$ por el Corolario 1.1.28. Pero ambos subgrupos tienen el mismo índice, por lo que necesariamente $\gamma_i(G) = N$.

□

Corolario 1.1.34. *Sea G un p-grupo de clase maximal, con $|G| = p^n$. Entonces $\gamma_{c+1-i}(G) = \mathcal{Z}_i(G)$ para $1 \leq i \leq c$.*

Demostración. Como por la demostración del Teorema 1.1.23 es sabido que los cocientes $\mathcal{Z}_{i+1}(G)/\mathcal{Z}_i(G)$ son no triviales para $i < c$, y tampoco lo es el centro por el Teorema 1.1.22, tenemos que

$$p^n = |G| = |G/\mathcal{Z}_{c-1}(G)| \cdot |\mathcal{Z}_{c-1}(G)/\mathcal{Z}_{c-2}(G)| \cdots |\mathcal{Z}_2(G)/\mathcal{Z}_1(G)| \cdot |\mathcal{Z}(G)|$$

es un producto de $c = n - 1$ factores no triviales de p, por lo que todos deben ser p excepto uno que, tomará el valor p^2. Es claro que este último debe ser $G/\gamma_2(G)$, por la Proposición 1.1.27. Con esto, se deduce también de la ecuación anterior que, para cada i,

$$|G| = |G/\mathcal{Z}_{c-1}(G)| \cdot |\mathcal{Z}_{c-1}(G)/\mathcal{Z}_{c-2}(G)| \cdots |\mathcal{Z}_{i+1}(G)/\mathcal{Z}_i(G)| \cdot |\mathcal{Z}_i(G)| = p^i \cdot |\mathcal{Z}_i(G)|.$$

Así, $(G : \mathcal{Z}_i(G)) = p^i$, y $\mathcal{Z}_i(G)$ es normal en G, de modo que la igualdad $\mathcal{Z}_i(G) = \gamma_i(G)$ se sigue de lema anterior. □

El subgrupo de Frattini

Enlazando con la definición de grupo maximal tenemos la siguiente:

Definición 1.1.35. Sea G un grupo. Llamamos *subgrupo de Frattini* de G, y denotamos por $\Phi(G)$, a la intersección de todos los subgrupos maximales de G; formalmente,

$$\Phi(G) = \bigcap_{H \text{ maximal}} H.$$

Si G no tiene subgrupos maximales, se define $\Phi(G) = G$.

Definición 1.1.36. Sea G un grupo. De un elemento $g \in G$ decimos que es un *no-generador* si para cada conjunto X de generadores de G se tiene que $X \setminus \{g\}$ sigue siendo un conjunto de generadores de G.

Equivalentemente, se puede definir un elemento no-generador como un elemento $g \in G$ tal que si $X \subseteq G$ no es un conjunto de generadores de G, entonces tampoco $X \cup \{g\}$ lo es.

Proposición 1.1.37. Sea G un grupo. Entonces

$$\Phi(G) = \{g \in G \ : \ g \text{ es un no-generador de } G\}$$

Demostración. Sea g un elemento no-generador, y H un subgrupo maximal cualquiera de G. Como claramente H no es un conjunto generador de G, tampoco $H \cup \{g\}$ lo será, y como H es maximal el subgrupo generado por este conjunto ha de ser H; en particular, $g \in H$. Esto prueba la inclusión hacia la izquierda.

Recíprocamente, sea $g \in \Phi(G)$. Sea $X \subseteq G$ un subconjunto de G que no es generador. Entonces X genera cierto subgrupo de G que estará contenido en algún subgrupo maximal H. Como $g \in H$, se tendrá que $X \cup \{g\}$ sigue generando un subgrupo de H, por lo que no es un conjunto generador de G, y el resultado se sigue. □

Dado un grupo G, denotaremos por $d(G)$ al mínimo entero $d \geq 0$ tal que existe un conjunto de generadores G de tamaño d.

Proposición 1.1.38. Sea G un grupo. Entonces $d(G) = d(G/\Phi(G))$.

Demostración. La desigualdad $d(G/\Phi(G)) \leq d(G)$ es cierta en general, pues para cada conjunto de generadores de G se tiene que la imagen de estos elementos por el homomorfismo canónico en el grupo cociente es un conjunto de generadores de $G/\Phi(G)$.

Para ver la desigualdad reciproca, sea $\overline{g_1}, \overline{g_2}, \ldots, \overline{g_n}$ un conjunto cualquiera de generadores de $G/\Phi(G)$, donde cada $g_i \in G$ es un representante de $\overline{g_i}$. Será suficiente comprobar que $\{g_1, g_2, \ldots, g_n\}$ es un conjunto de generadores de G. A este fin, supongamos por reducción al absurdo que no lo es; entonces existe un subgrupo maximal H que contiene al subgrupo de G generado por estos elementos. Si hubiese algún elemento en $G \setminus H$, claramente será de la forma hf, con $h \in H$ y $f \in \Phi(G)$. Pero por definición $\Phi(G) \subseteq H$, y por tanto $hf \in H$, contradicción.

□

Obtenemos ahora una caracterización del subgrupo de Frattini de p-grupos finitos; en su demostración será de utilidad haber fijado las siguientes nociones y resultados:

Definición 1.1.39. Sea G un grupo. Se define el *exponente* de G como el menor entero positivo n tal que $g^n = 1$ para cada $g \in G$. A este número lo denotamos por $\exp(G)$.

Definición 1.1.40. Sea G un p-grupo. Decimos G es *abeliano elemental* si es abeliano y tiene exponente p.

Observación 1.1.41. Se sigue inmediatamente del Teorema Fundamental de los Grupos Abelianos Finitos (Teorema 1.1.1) que cada grupo p-grupo abeliano elemental es isomorfo a un grupo de la forma $(C_p)^n$, donde C_p es un grupo cíclico de orden p y n un entero no negativo.

Lema 1.1.42. Sea M un subgrupo maximal de un grupo finito G de orden p^n. Entonces M es normal y $(G : M) = p$.

Demostración. Probamos que M es normal por inducción sobre n. Si $n = 1$ necesariamente $M = \{1\}$, y el resultado se tiene trivialmente. Sea entonces $n > 1$. Distinguimos dos casos. Si $\mathcal{Z}(G) \not\subseteq M$, por la maximalidad de M será $G = M\mathcal{Z}(G)$, y claramente M es normal en este grupo. Si por el contrario $\mathcal{Z}(G) \subseteq M$, como $\mathcal{Z}(G) \neq \{1\}$ por el Teorema 1.1.22, podemos aplicar la hipótesis de

inducción a $G/\mathcal{Z}(G)$ para deducir que $M/\mathcal{Z}(G) \trianglelefteq G/\mathcal{Z}(G)$, y por tanto $M \trianglelefteq G$, lo que completa el paso inductivo.

Para ver que M tiene índice p, basta notar que es posible construir una serie de subgrupos normales

$$\{1\} = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_k = M \leq \cdots \leq G_{n-1} \leq G_n = G$$

como en la Proposición 1.1.26. Así, si $(G : M) > p$ necesariamente $G_{n-1} \neq M$, y por tanto $M < G_{n-1} < G$, contradicción con la maximalidad de M.

□

Proposición 1.1.43. Sea G un p-grupo finito. Entonces $G/\Phi(G)$ es abeliano elemental, y si H es otro subgrupo normal de G tal que G/H es abeliano elemental, entonces $\Phi(G) \leq H$. En particular, $\Phi(G) = G^{(p)}G'$.

Demostración. Por el Lema 1.1.42 cada subgrupo maximal de G es normal y tiene índice p. Es decir, si M es un subgrupo maximal, entonces G/M es cíclico de orden p. Se sigue entonces (Lema 1.1.5) que $G' \leq M$ para cada grupo maximal G; en consecuencia, $G' \leq \Phi(G)$. Con esto el mencionado lema implica que $G/\Phi(G)$ es abeliano. Además, como G/M tiene orden p, para cada $x \in G$ se tiene que $(xM)^p = M$, luego $x^p \in M$, y por tanto $G^{(p)} \leq M$. Como esto ocurre para cada subgrupo maximal M, se deduce que $G^{(p)} \leq \Phi(G)$ (esto, de hecho prueba que $G^{(p)}G' \leq \Phi(G)$). Entonces cada elemento $x\Phi(G)$ de $G/\Phi(G)$ tiene orden p, y queda probado que este grupo cociente es abeliano elemental.

Recíprocamente, supongamos que G/H es abeliano elemental, digamos que de orden p^n. Entonces, este grupo está generado por n elementos de la forma x_iH, cada uno de ellos de orden p. Entonces podemos escribir

$$G/H = \langle x_1H\rangle \oplus \langle x_2H\rangle \oplus \cdots \oplus \langle x_nH\rangle.$$

Es claro que G/H tiene n subgrupos maximales H_i/H, generados por $\{x_jH \ : \ j \neq i\}$. Como el producto es directo, se tiene que

$$\bigcap_{i=1}^{n} H_i/H = \{1\},$$

de modo que $\bigcap_{i=1}^{n} H_i \subseteq H$ (donde los H_i son las imágenes inversas por el homomorfismo canónico en el grupo cociente de los H_i/H). Además estos H_i son subgrupos maximales de G, de modo que

$$\Phi(G) \subseteq \bigcap_{i=1}^{n} H_i \subseteq H,$$

y la equivalencia queda demostrada. En particular, como $G/(G^{(p)}G')$ es abeliano elemental, se tiene la inclusión $\Phi(G) \leq G^{(p)}G'$, y por tanto también la igualdad. □

Cadenas de subgrupos y grupos indescomponibles

Completamos la sección enunciando el conocido Teorema de Krull-Smith para grupos.

Definición 1.1.44. Un grupo G se dice *indescomponible* si $G \neq \{1\}$ y G no se puede expresar como el producto directo interno de dos de sus subgrupos.

Definición 1.1.45. Sea G un grupo.

(I) Decimos que G satisface la *condición de cadena ascendente* (ACC) para subgrupos normales si para cada cadena

$$G_1 \leq G_2 \leq \ldots$$

de subgrupos normales $G_i \trianglelefteq G$ existe un entero positivo n tal que $G_i = G_n$ para cada $i \geq n$.

(II) Decimos que G satisface la *condición de cadena descendente* (DCC) para subgrupos normales si para cada cadena

$$G_1 \geq G_2 \geq \dots$$

de subgrupos normales $G_i \lhd G$ existe un entero positivo n tal que $G_i = G_n$ para cada $i \geq n$.

Teorema 1.1.46 (Krull-Schmidt)**.** *Sea G un grupo que satisface ambas (ACC) y (DCC) para subgrupos normales. Entonces G admite una descomposición de la forma*

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_s$$

siendo los G_i subgrupos indescomponibles de G. Además, si existe otra descomposición

$$G = H_1 \oplus H_2 \oplus \cdots \oplus H_t,$$

con los H_j siendo subgrupos indescomponibles de G, entonces $s = t$, y es posible renombrar los índices de los H_j de forma que $G_i \cong H_i$ para cada i, y además, para cada $r \leq t$,

$$G = G_1 \oplus G_2 \oplus \dots G_r \oplus H_{r+1} \oplus \cdots \oplus H_t.$$

Demostración. Ver Teorema 3.8 de [21]. □

Es evidente que todo grupo finito satisface ambas condiciones de cadena, por lo que, en particular, podemos aplicar el Teorema de Krull-Smith a los p-grupos finitos.

1.2. Conmutadores n-arios

Introducimos en esta sección un par de fórmulas (las dadas en los Teoremas 1.2.11 y 1.2.15) que nos permiten destacar algunos elementos de los miembros de la serie central inferior, y que serán de utilidad en la próxima sección; a este fin, utilizaremos una técnica de Teoría de Grupos algo más sutil que las dadas hasta ahora, el llamado *método de agrupación de conmutadores*, cuya esencia se destila en los Lemas 1.2.9 y 1.2.10.

Conmutadores n-arios canónicos

Comenzamos dando, como generalización de la noción de conmutador, la definición de conmutador n-ario (canónico), así como algunas propiedades elementales de los mismos para $n = 3$, y aplicando estos al estudio de la serie central inferior.

Definición 1.2.1. Sea G un grupo y $x_1, x_2, \dots$ elementos de G. Entonces

(I) Decimos que (x_1, x_2) es el *conmutador 2-ario canónico* de x_1 y x_2.

(II) Si $(x_1, \dots, x_n)$ es el *conmutador n-ario canónico* de los elementos $x_1, \dots, x_n$, diremos que el elemento $((x_1, \dots, x_n), x_{n+1})$ es el conmutador $(n+1)$-ario canónico de $x_1, \dots, x_n, x_{n+1}$.

Denotaremos por $(x_1, \dots, x_n)$ al conmutador n-ario canónico de los elementos $x_1, \dots, x_n$. Además, si $H_1, H_2, \dots, H_n$ son subgrupos de G, denotaremos por $(H_1, H_2, \dots, H_n)$ al sugrupo de G generado por los elementos de la forma $(x_1, x_2, \dots, x_n)$, con $x_i \in H_i$ para cada i.

Lema 1.2.2. Sea G un grupo, y $n \geq 2$ un entero. El conjunto de los conmutadores n-arios canónicos $(x_1, \dots, x_n)$, con $x_1, \dots, x_n \in G$, genera el subgrupo $\gamma_n(G)$ módulo $\gamma_{n+1}(G)$.

Demostración. En primer lugar notemos que por la definición es obvio que, dados $x_1, \dots, x_n \in G$, se verifica $(x_1, \dots, x_n) \in \gamma_n(G)$. Para $n = 2$ el lema es inmediato a partir de la definición de $\gamma_2(G) = G'$. Supongamos el lema cierto para $n \geq 2$, y denotemos por '$\equiv$' a la identidad módulo $\gamma_{n+2}(G)$; utilizaremos frecuentemente que los elementos de $\gamma_{n+1}(G)$ conmutan con todos los elementos de G módulo $\gamma_{n+2}(G)$.

Será suficiente comprobar que los elementos de la forma (g,h), con $g \in \gamma_n(G)$ y $h \in G$, se pueden expresar como producto de conmutadores $(n+1)$-arios canónicos y de elementos de $\gamma_{n+2}(G)$. Por la hipótesis de inducción podemos escribir

$$g = c_1 \dots c_s y, \qquad \text{con} \quad c_i = (x_{i1}, \dots, x_{in}),\ x_{ij} \in G, \quad y \in \gamma_{n+1}(G).$$

Razonamos ahora por inducción sobre s. Si $s = 1$, entonces $g = c_1 y$, y así:

$$(g,h) = (c_1 y, h) \equiv (c_1, h) = (x_{11}, x_{12} \dots x_{1n}, h).$$

Supongamos válida la segunda hipótesis de inducción para $s > 1$, y sea $g = c_1 \dots c_s c_{s+1}$. Escribamos $g_1 = c_1 \dots c_s$. Entonces:

$$\begin{aligned}(g,h) = (g_1 c_{s+1} y, h) &\equiv (g_1 c_{s+1}, h)\\ &= c_{s+1}^{-1} g_1^{-1} h^{-1} g_1 c_{s+1} h\\ &= c_{s+1}^{-1} g_1^{-1} h^{-1} g_1 h c_{s+1} (c_{s+1}, h)\\ &= c_{s+1}^{-1} (g_1, h) c_{s+1} (c_{s+1}, h)\\ &\equiv (g_1, h)(c_{s+1}, h),\end{aligned}$$

que es un producto de la forma requerida, por serlo (g_1, h) en virtud de la hipótesis de inducción. Esto completa ambos pasos inductivos, y por tanto también el lema.

□

Nos centramos ahora en conmutadores 3-arios.

Lema 1.2.3. Sean $x, y, z \in G$. Entonces:

$$(x, y^{-1}, z)^y (y, z^{-1}, x)^z (z, x^{-1}, y)^x = 1.$$

Demostración. Sean $u = xzx^{-1}yx,\ v = yxy^{-1}zy,\ w = zyz^{-1}xz$. Entonces podemos reescribir

$$\begin{aligned}(x, y^{-1}, z)^y &= \big((x, y^{-1})^{-1} z^{-1} (x, y^{-1}) z\big)^y\\ &= y^{-1}(yx^{-1}y^{-1}x \cdot z^{-1} \cdot x^{-1}yxy^{-1} \cdot z)y\\ &= (x^{-1}y^{-1}xz^{-1}x^{-1})(yxy^{-1}zy)\\ &= u^{-1}v;\end{aligned}$$

análogamente se comprueba que

$$\begin{aligned}(y, z^{-1}, x)^z &= (y^{-1}z^{-1}yx^{-1}y^{-1})(zyz^{-1}xz) = v^{-1}w;\\ (z, x^{-1}, y)^x &= (z^{-1}x^{-1}zy^{-1}z^{-1})(xzx^{-1}yx) = w^{-1}u.\end{aligned}$$

Por tanto,

$$(x, y^{-1}, z)^y (y, z^{-1}, x)^z (z, x^{-1}, y)^x = u^{-1}vv^{-1}ww^{-1}u = 1.$$

□

Como consecuencia, obtenemos el siguiente resultado de P. Hall, llamado *lema de los tres subgrupos*:

Lema 1.2.4. Sean X, Y, Z tres subgrupos de G y sea $N \trianglelefteq G$. Si $(X,Y,Z) \subseteq N$ e $(Y,Z,X) \subseteq N$, entonces también $(Z,X,Y) \subseteq N$.

Demostración. Sean $x \in X$, $y \in Y$, $z \in Z$. Por las inclusiones del enunciado, y ser N normal, se tiene que $(x, y^{-1}, z)^y \in N$ y que $(y, z^{-1}, x)^z \in N$. Por tanto, el Lema 1.2.3 se deduce que $(z, x^{-1}, y)^x \in N$; lo que, de nuevo por ser N normal, implica que $(z, x^{-1}, y) \in N$.

Ahora bien, notando que (Z,X) está generado por todos los conmutadores de la forma (z, x^{-1}), el párrafo anterior afirma que y centraliza a todos los generadores de (Z,X) módulo N, y por ende que y centraliza a (Z,X) módulo N. Y como esto se tiene para cada $y \in Y$, podemos concluir que $(Z,X,Y) \subseteq N$. □

Lema 1.2.5. Sea G un grupo. Entonces $(\gamma_i(G), \gamma_j(G)) \subseteq \gamma_{i+j}(G)$ para cada i, j.

Demostración. Procedemos por inducción sobre j. Para el caso $j = 1$, como $\gamma_1(G) = G$, por definición se tiene que $(\gamma_i(G), \gamma_1(G)) = (\gamma_i(G), G) = \gamma_{i+1}(G)$ para cada i.

Supongamos ahora que $(\gamma_i(G), \gamma_{j-1}(G)) \subseteq \gamma_{i+j-1}(G)$ para cada i. Entonces se tiene que

$$(G, \gamma_i(G), \gamma_{j-1}(G)) = (\gamma_{i+1}(G), \gamma_{j-1}(G)) \subseteq \gamma_{i+j}(G)$$

y que

$$(\gamma_i(G), \gamma_{j-1}(G), G) \subseteq (\gamma_{i+j-1}(G), G) = \gamma_{i+j}(G)$$

(donde las inclusiones se obtienen aplicando la hipótesis inducción con $i+1$ e i, respectivamente).

Ahora, $\gamma_{i+j}(G)$ es un subgrupo normal de G, por lo que podemos aplicar el Lema 1.2.4 para deducir que

$$(\gamma_{j-1}(G), G, \gamma_i(G)) \subseteq \gamma_{i+j}(G),$$

siendo el término de la izquierda

$$(\gamma_{j-1}(G), G, \gamma_i(G)) = (\gamma_j(G), \gamma_i(G)) = (\gamma_i(G), \gamma_j(G)),$$

con lo que el paso inductivo queda completo. □

Conmutadores n-arios arbitrarios

Como generalización, podemos definir:

Definición 1.2.6. Sea G un grupo y $x_1, x_2, \ldots$ elementos de G. Entonces definimos por recursión:

(I) Decimos que (x_1, x_2) es un *conmutador 2-ario* de x_1 y x_2.

(II) Si y es un conmutador n-ario de los elementos $x_1, \ldots, x_n$, y z es un conmutador m-ario de los elementos $x_{n+1}, \ldots, x_{n+m}$, diremos que el elemento (y, z) es un *conmutador $(n+m)$-ario arbitrario* de los elementos $x_1, \ldots x_{n+m}$.

Denotaremos por $(x_1, x_2, \ldots, x_n)_\alpha$ a un conmutador n-ario de $x_1, x_2, \ldots, x_n$, donde asumimos que α, de alguna manera, determina cuál de ellos es exactamente, i.e., α contiene la información sobre cómo se colocan los paréntesis (por ejemplo, uno puede pensar α como una aplicación $\{1, 2, \ldots, n\} \to \{0, 1, \ldots n\} \times \{0, 1, \ldots n\}$, entendiendo que si $\alpha(i) = (j, k)$, antes del elemento x_i se abren j paréntesis, y se cierran k paréntesis; obviamente no todas las aplicaciones de este tipo determinan una disposición de paréntesis válida, pero a cada conmutador n-ario arbitrario se le puede asignar una única aplicación de este tipo).

Lema 1.2.7. Sea $x = (x_1, x_2, \ldots, x_n)_\alpha$ un conmutador n-ario de los elementos $x_i \in G$. Si $x_i \in \gamma_{k_i}(G)$ para cada i, entonces $x \in \gamma_k(G)$, donde $k = k_1 + k_2 + \cdots + k_n$. Además, si algún $x_i = 1$, entonces $x = 1$.

Demostración. Procedemos por inducción sobre n. Si $n = 2$ la primera afirmación es consecuencia inmediata del Lema 1.2.5, y la segunda es trivial. Si $n > 1$, considerando el último conmutador formado en el orden dado por α, podemos escribir $c = (c', c'')$, donde, para cierta j, $c' = (x_1, \ldots, x_j)_{\alpha'}$ y $c'' = (x_{j+1}, \ldots, x_n)_{\alpha''}$. Entonces, por hipótesis de inducción, $c' \in \gamma_{k'}(G)$ y $c'' \in \gamma_{k''}(G)$, siendo $k' = k_1 + k_2 + \cdots + k_j$, y $k'' = k_{j+1} + \cdots + k_n$; por tanto, podemos usar el Lema 1.2.5 para concluir que $c = (c', c'') \in \gamma_{k'+k''}(G) = \gamma_k(G)$.

Además, si algún $x_i = 1$, por hipótesis de inducción o bien $c' = 1$ o bien $c'' = 1$, y por tanto $c = (c', c'') = 1$. □

En particular, se obtiene la siguiente observación trivial:

Corolario 1.2.8. *Si $x = (x_1, x_2, \ldots, x_n)_\alpha$ es un conmutador n-ario, entonces $x \in \gamma_n(G)$.*

Demostración. Basta notar que los $x_i \in G = \gamma_1(G)$, y aplicar el lema anterior. □

Método de agrupación de conmutadores

Como anunciábamos antes, el método de agrupación de conmutadores se reduce esencialmente a los dos lemas siguientes. En ellos, consideraremos fijada la notación que a continuación introducimos:

Dado un entero $s > 0$, sea $\langle y_1, y_2, \ldots, y_s \rangle$ el grupo libre sobre los s generadores $y_1, y_2, \ldots, y_s$, y $X_1, \ldots, X_r$ una partición del conjunto $\{y_1, \ldots, y_s\}$. Para cada i, sea $f(i)$ el único entero que verifica $y_i \in X_{f(i)}$. Si S es cualquier subconjunto no vacío de $R = \{1, 2, \ldots, r\}$, denotamos por X_S al conjunto de todos los conmutadores (de cualquier longitud)

$$c = (y_{i_1}, y_{i_2}, \ldots, y_{i_m})_\alpha$$

tales que $S = \{f(i_1), f(i_2), \ldots, f(i_m)\}$. Es decir, todas las componentes de c están en $\bigcup_{j \in S} X_j$, y para cada $j \in S$, hay al menos un elemento de X_j que es componente de c. Notemos que $X_i \subseteq X_{\{i\}}$, pero en general no se da la igualdad.

Consideraremos además fijado un buen orden $\prec$ sobre los subconjuntos no vacíos de R verificando que, para cada $S \neq S' \in \mathbb{P}(R) \setminus \{\emptyset\}$ con $|S| < |S'|$, se tiene que $S \prec S'$.

Lema 1.2.9. Con la notación anterior, si $\mu = y_1 y_2 \ldots y_s$, entonces

$$\mu = \prod_{\emptyset \neq S \subseteq R} \eta_S,$$

donde η_S es un producto de elementos de X_S (para cada S), y los factores aparecen en el producto en el orden determinado por $\prec$.

Demostración. La idea de la prueba no es más que la agrupación gradual de los factores, desplazándolos paso a paso hacia la derecha, para formar los η_S. Para dar un argumento detallado comenzamos notando que, en general, si u y v son elementos del grupo, v se puede desplazar hacia la izquierda sobre u usando la fórmula:

$$uv = vu(u^{-1}v^{-1}uv) = vu(u, v).$$

Sea $\{j\}$ mínimo en el orden $\prec$. Se comienza agrupando aquellos factores y_i que pertenecen a X_j. Estos factores son movidos a la izquierda uno a uno, usando la fórmula de arriba (los nuevos factores de X_j que van apareciendo a la derecha, como parte de algún conmutador, no se tienen en cuenta), de forma que los factores de X_j nunca se crucen. Claramente si $y_i \in X_j$, y $u \in X_M$ (suponiendo $M \neq \{j\}$, pues los factores de X_j nunca se cruzan), se tiene que $uy_i = y_i u(u, y_i)$, donde $(u, y_i) \in X_{M \cup \{j\}}$. Con esto, se hace evidente que una vez realizados todos estos movimientos, tendremos μ escrito como $\mu = \eta_{\{j\}} \mu'$, donde $\eta_{\{j\}}$ es un producto de elementos de X_j, y μ' es un producto de elementos de X_h con $h \neq j$ y de $X_{M \cup \{j\}}$ con $M \neq \{j\}$; es decir, μ' es un producto de elementos de $X_{M'}$, con $\{j\} \prec M'$.

Supongamos ahora que para algún conjunto $\emptyset \neq T \subseteq R$ tenemos escrito μ como:

$$\mu = \left(\prod_{S \prec T} \eta_S \right) \mu'',$$

donde μ'' es un producto de elementos de aquellos X_M tales que $T \preceq M$. Entonces el siguiente paso en este proceso de agrupación es desplazar todos los factores de X_T al comienzo de μ'' de tal modo que los factores de X_T nunca se crucen. Observemos que si $v \in X_T$ y si v es desplazado a la izquierda sobre $u \in X_M$, entonces $uv = vu(u, v)$ y $(u, v) \in X_{M \cup T}$. Como $T \prec M$ (si se diese la igualdad, se estarían cruzando dos factores de X_T), se sigue fácilmente que $|T| < |M \cup T|$ (pues o bien $|T| < |M|$, y se tiene trivialmente, o bien $|T| = |M|$ y $T \neq M$, por lo que $|T \cap M| < |M|$, y así $|T \cup M| = |T| + |M| - |T \cap M| > |T|$), y por tanto $T \prec M \cup T$. Una vez realizados todos estos

movimientos, tendremos μ'' reescrito como $\mu'' = \eta_T \mu'''$, donde μ''' es un producto de elementos pertenecientes a X_M, con $T \prec M$. Entonces podemos escribir

$$\mu = \left(\prod_{\emptyset \neq S \preceq T} \eta_S \right) \cdot \mu'''.$$

Repitiendo este proceso hasta que todos los subconjuntos de R hayan sido considerados se obtiene la expresión del enunciado. □

Lema 1.2.10. Con la misma notación, y dado $\emptyset \neq T \subseteq R$, sea μ_T el producto (en el orden de los naturales) de los y_i tales que $f(i) \in T$. Entonces

$$\mu_T = \prod_{\emptyset \neq S \subseteq T} \eta_S,$$

donde los factores aparecen en el producto en el orden determinado por $\prec$, y los η_S son los del lema anterior.

Demostración. Sea σ el endomorfismo de $\langle y_1, y_2, \ldots, y_s \rangle$ dado por

$$\sigma(y_i) = \begin{cases} y_i & \text{si } f(i) \in T \\ 1 & \text{si } f(i) \notin T. \end{cases}$$

Escribiendo $\mu = y_1 y_2 \ldots y_s$, claramente $\sigma(\mu) = \mu_T$, y por tanto el Lema 1.2.9 nos permite escribir

$$\mu_T = \sigma(\mu) = \prod_{\emptyset \neq S \subseteq R} \sigma(\eta_S). \tag{1.2}$$

Notemos ahora que si $S \subseteq T$ entonces η_S es un producto de elementos de la forma $(y_{i_1}, y_{i_2}, \ldots, y_{i_m})_\alpha \in X_S$, es decir, tales que $f(i_h) \in S \subseteq T$ para cada h. Luego cada uno de estos factores es invariante por σ, y por tanto también $\sigma(\eta_S) = \eta_S$. Por otro lado, si $S \not\subseteq T$, entonces η_S es un producto de conmutadores con al menos una componente y_{i_h} tal que $f(i_h) \notin T$; así, como $\sigma(y_{i_h}) = 1$, por el Lema 1.2.7 todo el conmutador es 1, y como esto ocurre para cada factor, también $\sigma(\eta_S) = 1$. Con esto, la fórmula (1.2) se reduce a la identidad del enunciado, y hemos terminado. □

Algunas fórmulas notables

Podemos ya, como primera aplicación del método descrito, dar el siguiente resultado:

Teorema 1.2.11 (Fórmulas de Hall-Petresco)**.** *Consideremos el grupo $G = \langle a, b \rangle$, y sean $c_1, c_2, c_3, \ldots$ los elementos del grupo definidos recursivamente por las fórmulas*

$$a^n b^n = c_1^{\binom{n}{1}} c_2^{\binom{n}{2}} \ldots c_n^{\binom{n}{n}},$$

para $n \geq 1$. Entonces $c_i \in \gamma_i(G)$ para cada i.

Demostración. Fijemos $n \geq 1$. Dado $\binom{n}{n} = 1$, es claro que la n-ésima ecuación permite expresar c_n en función de a, b, n y $c_1, \ldots, c_{n-1}$. Será suficiente probar que $c_n \in \gamma_n(G)$.

Sea $H = \langle y_1, y_2, \ldots, y_{2n} \rangle$ el grupo libre sobre $2n$ generadores. Definamos el homomorfismo $\sigma : H \to G$ dado por

$$\sigma(y_i) = \begin{cases} a & \text{si} \quad i \leq n \\ b & \text{si} \quad i \geq n+1. \end{cases}$$

Consideremos también la partición de $\{y_1, y_2, \ldots, y_{2n}\}$ conformada por los conjuntos $X_i = \{y_i, y_{n+i}\}$, con $i = 1, \ldots, n$; y ordenemos los subconjuntos no vacíos de $R = \{1, 2, \ldots, n\}$ primero por cardinalidad, y lexicográficamente[1] entre los conjuntos del mismo tamaño. Entonces por el Lema 1.2.10, y con la notación del mismo con $s = 2n$ y $r = n$, se tiene para cada $\emptyset \neq T \subseteq R$ vale

$$\mu_T = \prod_{\emptyset \neq S \subseteq T} \eta_S, \qquad \text{y por tanto} \qquad \sigma(\mu_T) = \prod_{\emptyset \neq S \subseteq T} \sigma(\eta_S). \tag{1.3}$$

Supongamos ahora que T y T' son dos subconjuntos no vacíos de R de la misma cardinalidad, digamos $|T| = |T'| = m$; usando la definición es inmediato comprobar que

$$\sigma(\mu_T) = \sigma(\mu_{T'}) = a^m b^m.$$

Además, para cada i, T y T' contienen exactamente la misma cantidad de subconjuntos de cardinal i, a saber, $\binom{m}{i}$. Con esto, una inducción sencilla da que $\sigma(\eta_T) = \sigma(\eta_{T'})$, pues si $m = 1$, entonces $\sigma(\eta_T) = \sigma(\mu_T) = \sigma(\mu_{T'}) = \sigma(\eta_{T'})$, y si la nuestra afirmación es cierta para todos los S, S' con $|S| = |S'| < m$, entonces

$$\sigma(\eta_T) = \left(\prod_{\emptyset \neq S \subsetneq T} \sigma(\eta_S) \right)^{-1} \cdot \sigma(\mu_T) = \left(\prod_{\emptyset \neq S' \subsetneq T'} \sigma(\eta_{S'}) \right)^{-1} \cdot \sigma(\mu_{T'}) = \sigma(\eta_T)$$

Podemos entonces, para $i = 1, \ldots, m$, definir elementos $d_i \in G$ mediante $d_i = \sigma(\eta_S)$ para cada S con $|S| = i$. Así, si $|T| = m$, la ecuación (1.3) se reescribe como

$$a^m b^m = \sigma(\mu_T) = d_1^{\binom{m}{1}} d_2^{\binom{m}{2}} \ldots d_m^{\binom{m}{m}};$$

como esto vale para $1 \leq m \leq n$, y por nuestra observación inicial estas ecuaciones determinan d_m, necesariamente será $d_m = c_m$ para cada $m \leq n$, y en particular $d_n = c_n$.

Finalmente, por el Lema 1.2.9 sabemos que η_R es un producto de elementos de X_R, es decir, de conmutadores de H que tienen como poco una componente en cada uno de los conjuntos $X_1, X_2, \ldots, X_n$, así que cada uno de estos conmutadores es de longitud al menos n. Esto implica que $c_n = d_n = \sigma(\eta_R)$ es un producto de conmutadores de G de longitud al menos n. Por tanto, podemos aplicar el Corolario 1.2.8 para deducir que $c_n \in \gamma_n(G)$, completando así la prueba. □

Este teorema es el punto de partida del estudio de los p-grupos regulares, los cuales, a modo de digresión, presentamos brevemente:

Definición 1.2.12. De un p-grupo G decimos que es *regular* si para cada $a, b \in G$ existen elementos $c_1, c_2, \ldots, c_k \in \gamma_2(\langle a, b \rangle)$ tales que

$$a^p b^p = (ab)^p c_1^p c_2^p \ldots c_k^p.$$

Corolario 1.2.13. *Sea G un p-grupo nilpotente de clase $c(G) < p$. Entonces G es regular.*

Demostración. Sea $s = c(G)$. Por el Teorema 1.2.11 podemos escribir

$$a^p b^p = c_1^p c_2^{\binom{p}{2}} \ldots c_p^{\binom{p}{p}},$$

donde obviamente $c_1 = ab$, y $c_i \in \gamma_i(\langle a, b \rangle)$. En particular, para $i > s$ se tiene que $c_i = 1$. Por tanto, la expresión anterior se reescribe como

$$a^p b^p = (ab)^p c_2^{\binom{p}{2}} \ldots c_s^{\binom{p}{s}},$$

y como para cada $i \leq s < p$ el número combinatorio $\binom{p}{i}$ es múltiplo de p, el resultado se sigue.

□

[1] Los subconjuntos de $\{1, 2, \ldots, n\}$ con el mismo cardinal, digamos N pueden ser identificados con los vectores $(a_1, a_2, \ldots, a_N)$ de $\mathbb{N}^N$ tales $a_i < a_{i+1}$ para cada i; y sobre estos vectores se puede considerar el orden lexicográfico usual:

$$(a_1, a_2, \ldots, a_N) < (b_1, b_2, \ldots, b_N) \qquad \text{si y solo si} \qquad \exists j (\forall i < j (a_i = b_i) \wedge (a_j < b_j)).$$

Para ilustrar la potencia del último teorema, damos además la siguiente proposición:

Proposición 1.2.14. Sea G un p-grupo nilpotente no trivial de clase $c(G) < p$. Si G está generado por elementos de orden p, entonces G tiene exponente p.

Demostración. Procedemos por inducción sobre $c(G)$. Si fuese $c(G) \leq 1$, G sería abeliano, y el resultado se sigue trivialmente. Supongamos entonces que $2 \leq c(G) < p$, y que el resultado es válido para todos los grupos de clase menor que $c(G)$.

Afirmamos primero que si x, y son dos elementos de G de orden p, entonces $(x, y)^p = 1$. Para verlo, sean x e y dos elementos tales, y consideremos el grupo

$$L = \langle x, y^{-1}xy\rangle = \langle x, x^{-1}y^{-1}xy\rangle = \langle x, (x, y)\rangle.$$

Como (x, y) es central módulo $\gamma_3(G) = (G', G)$, tenemos que el grupo $L/(L \cap \gamma_3(G))$ está generado por dos elementos, las imágenes de x y (x, y), uno de los cuales es central. Se sigue entonces que $L/(L \cap \gamma_3(G))$ es abeliano, y por tanto $\gamma_2(L) = L' \subseteq \gamma_3(G)$. Se obtiene entonces por inducción (el paso inductivo es inmediato) que $\gamma_i(L) \subseteq \gamma_{i+1}(G)$ para cada $i \geq 2$. En consecuencia, por ser $c \geq 2$ se tiene que $\gamma_c(L) \subseteq \gamma_{c+1}(G) = \langle 1\rangle$; esto prueba que $c(L) < c(G)$. Además, $L = \langle x, y^{-1}xy\rangle$ está generado por elementos de orden p, de modo que por hipótesis de inducción L tiene exponente p. En particular, $(x, y)^p = 1$, y nuestra primera afirmación queda probada.

Sea ahora N el subgrupo normal de G generado por todos los elementos de la forma $(x, y)^g$, con x e y siendo generadores de G de orden p, y con $g \in G$ arbitrario. Entonces, por lo anterior N está generado por elementos de orden p. Además, claramente $N \subseteq G'$, por lo que (Lema 1.1.13) vale $c(N) \leq c(G') < c(G)$, de manera que la hipótesis de inducción garantiza que N tiene exponente p. Ahora bien, todos los generadores de G/N conmutan, luego será $G' \subseteq N$; se deduce entonces que $G' = N$ tiene exponente p.

Finalmente, si probásemos que el conjunto H de todos los elementos de G con orden 1 o p conforma un subgrupo de G, dado que H contiene un conjunto generador de G por hipótesis, sería $H = G$, y por tanto $G = H$ tendría exponente p, con lo que la proposición quedaría demostrada. Probémoslo pues; sean $a, b \in H$, y apliquemos el Teorema 1.2.11 a los productos $a^n(b^{-1})^n$. Cuando $n = 1$, tendremos que $ab^{-1} = c_1$, y para $n = p$ se tiene que

$$1 = a^p b^{-p} = c_1^{\binom{p}{1}} c_2^{\binom{p}{2}} \dots c_p^{\binom{p}{p}}.$$

Observemos que para $2 \leq i < p$ se tiene que $p|\binom{p}{i}$, y como los c_i son productos de conmutadores de longitud al menos dos, $c_i \in G'$; combinando estos dos hechos con que $\exp(G) = p$, se deduce que $c_i^{\binom{p}{i}} = 1$. Además, $c_p = 1$, pues $c_p \in \gamma_p(G) = \langle 1\rangle$ por ser $c(G) < p$. En definitiva, la ecuación anterior se reescribe como

$$1 = a^p b^{-p} = c_1^p = (ab^{-1})^p,$$

lo que prueba que $ab^{-1} \in H$, y por ende que H es un subgrupo, con lo que también la proposición completa queda probada.

□

Y como segunda aplicación del método de agrupación de conmutadores (nótese la similitud con la prueba del Teorema 1.2.11) damos el siguiente:

Teorema 1.2.15 (Dark)**.** *Sea $G = \langle a, b\rangle$, y consideremos los elementos del grupo c_{ij}, para $i \geq 1$, $j \geq 1$ definidos recursivamente por las fórmulas*

$$(a^m, b^n) = \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} c_{ij}^{\binom{m}{i}\binom{n}{j}}$$

para $m \geq 1, n \geq 1$, donde los factores están ordenados, primero, por el parámetro $i + j$, y entre los factores cuyos índices tienen la misma suma, por el orden del parámetro i.

Entonces cada c_{ij} es un producto de conmutadores de distintas longitudes, cada uno de los cuales tiene al menos i componentes iguales a $a^{\pm 1}$, y j componentes iguales a $b^{\pm 1}$. En particular, $c_{ij} \in \gamma_{i+j}(G)$.

Demostración. Dado que $\binom{m}{m}\binom{n}{n} = 1$, es claro que la (m,n)-ésima de las ecuaciones del enunciado permite expresar c_{mn} en función de a, b, m, n y los c_{ij} con $i \leq m$, $j \leq n$ e $i + j < m + n$, de modo que c_{mn} queda determinado por ellos.

Fijemos enteros $m, n \geq 1$; sea $t = m + n$, y sea $H = \langle y_1, y_2, \ldots, y_{2n} \rangle$ el grupo libre sobre $2t$ generadores. Definamos un homomorfismo $\sigma : H \to G$ mediante

$$\sigma(y_i) = \begin{cases} a^{-1} & \text{si} \quad 1 \leq i \leq m \\ b^{-1} & \text{si} \quad m+1 \leq i \leq m+n = t \\ a & \text{si} \quad t+1 \leq i \leq t+m \\ b & \text{si} \quad t+m+1 \leq i \leq t+m+n = 2t. \end{cases}$$

Consideremos también la partición de $\{y_1, y_2, \ldots, y_{2t}\}$ conformada por los conjuntos $X_i = \{y_i, y_{t+i}\}$ con $i = 1, 2, \ldots, t$. Si S es un subconjunto de $R = \{1, 2, \ldots, t\}$, escribimos $S_a = S \cap \{1, 2, \ldots, m\}$ y $S_b = S \cap \{m, m+1, \ldots, t\}$. Ordenemos los subconjuntos S de R en primer lugar por el orden dado por la cardinalidad de S; entre los conjuntos con el mismo cardinal, por la cardinalidad de S_a, y finalmente, cuando ambos cardinales coincidan, por el orden lexicográfico. Entonces por el Lema 1.2.10, y con la notación del mismo, poniendo $s = 2t$ y $r = t$, se tiene que

$$\mu_T = \prod_{\emptyset \neq S \subseteq T} \eta_S, \qquad \text{y por tanto} \qquad \sigma(\mu_T) = \prod_{\emptyset \neq S \subseteq T} \sigma(\eta_S) \tag{1.4}$$

Supongamos ahora que T y T' son ambos subconjuntos de R con $|T_a| = |T'_a| = u$ y $|T_b| = |T'_b| = v$, y pongamos $u + v = |T| = m$. Entonces, usando la definición de μ_T es sencillo ver que

$$\sigma(\mu_T) = \sigma(\mu_{T'}) = (a^{-1})^u (b^{-1})^v a^u b^v = (a^u, b^v).$$

Además, para cada i, j, es claro que T y T' contienen exactamente la misma cantidad de subconjuntos S con $|S_a| = i$ y $|S_b| = j$, a saber, $\binom{u}{i}\binom{v}{j}$. Con esto, una inducción sencilla da que $\sigma(\eta_T) = \sigma(\eta_{T'})$, pues si $m = 1$ entonces $\sigma(\eta_T) = \sigma(\mu_T) = \sigma(\mu_{T'}) = \sigma(\eta_{T'})$, y si nuestra afirmación es cierta para todos los S, S' con $|S| = |S'| < m$, entonces

$$\sigma(\eta_T) = \left(\prod_{\emptyset \neq S \subsetneq T} \sigma(\eta_S) \right)^{-1} \cdot \sigma(\mu_T) = \left(\prod_{\emptyset \neq S' \subsetneq T'} \sigma(\eta_{S'}) \right)^{-1} \cdot \sigma(\mu_{T'}) = \sigma(\eta_T).$$

Podemos entonces, para cada $0 \leq i \leq u$, $0 \leq j \leq v$, con $i + j > 0$, definir el elemento $d_{ij} \in G$ mediante $d_{ij} = \sigma(\eta_S)$ para cualquier S con $|S_a| = i$, $|S_b| = j$. Así, si T es como arriba, la ecuación (1.4) da que

$$(a^u, b^v) = \sigma(\mu_T) = \prod_{i,j} d_{ij}^{\binom{u}{i}\binom{v}{j}},$$

donde los factores están ordenados primero por el parámetro $i + j$, y después, entres los términos con igual suma, por el parámetro i (es directo ver que este orden se corresponde con el orden sobre los subconjuntos de R en el que aparecen los factores en la ecuación (1.4)).

Observemos que la última fórmula es válida para cada $0 \leq u \leq m$, $0 \leq v \leq n$, y que los subíndices que aparecen en el producto verifican $0 \leq i \leq u$, $0 \leq j \leq v$ e $i + j > 0$. Ahora bien, como $(a^u, b^0) = 1 = (a^0, b^u)$, otra inducción sencilla da que los elementos de la forma d_{i0} y d_{0j} son 1. En efecto, si $i = 1$ está claro, pues $1 = (a^1, b^0) = d_{1,0}$; y si $d_{h0} = 1$ para cada $h < i$, entonces $1 = (a^i, b^0) = \prod_{h=1}^{i} d_{h0}^{\binom{i}{h}} = d_{h0}$. Podemos ignorar entonces estos factores, de modo que para $1 \leq u \leq m$, $1 \leq v \leq n$ se tiene la fórmula:

$$(a^m, b^n) = \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} c_{ij}^{\binom{m}{i}\binom{n}{j}},$$

con el orden especificado arriba. Además, comenzábamos observando que estas ecuaciones determinaban de forma unívoca los elementos d_{ij}, así que necesariamente $d_{ij} = c_{ij}$ para $1 \leq i \leq m$, $1 \leq j \leq n$, y en particular $d_{mn} = c_{mn}$.

Finalmente, recordemos del Lema 1.2.9 que η_R es un producto de conmutadores de H de distintas longitudes teniendo al menos una componente en cada uno de los conjuntos disjuntos $X_1, X_2, \ldots, X_m, X_{m+1}, \ldots, X_t$. En consecuencia, también $c_{mn} = d_{mn} = \sigma(\eta_R)$ es un producto de conmutadores de G con al menos m componentes iguales a $a^{\pm 1}$ y al menos n componentes iguales a $b^{\pm 1}$. Así, hemos probado que c_{mn} es un producto de conmutadores de G de longitud al menos $m + n$, por lo que el Corolario 1.2.8 da que $c_{mn} \in \gamma_{m+n}(G)$, y la prueba concluye. □

1.3. Series de Lazard y de Brauer-Jennings-Zassenhaus

Definición 1.3.1. Sea G un grupo, y p un primo. Una *N-serie* de G es una sucesión $G = G_1 \geq G_2 \geq \ldots$ de subgrupos normales de G satisfaciendo $(G_i, G_j) \subseteq G_{i+j}$ para cada i, j. Además, de una sucesión tal diremos que es una *N-serie p-restringida*, o *N_p-serie*, si además verifica la implicación: si $g \in G_i$, entonces $g^p \in G_{ip}$, para cada i.

Observación 1.3.2. Es claro por el Lema 1.2.5 que la serie central inferior $\{\gamma_i(G)\}_{i \geq 1}$ de un grupo G es una N-serie. Sin embargo, es fácil comprobar que, dado un primo p, no es en general p-restrigida.

Dedicamos esta sección a introducir un ejemplo de N_p-serie, la llamada serie de Lazard, así como la serie de Brauer-Jennings-Zassenhaus, la cual, a pesar de su aparentemente distinta definición, más adelante probaremos que coincide con la serie de Lazard (ver Sección 3.2).

La serie de Lazard

Podemos entonces dar ya la definición de esta serie:

Definición 1.3.3. Dado un grupo G, y un primo p, se define la *serie de Lazard* de G mediante:

$$\mathcal{L}_{p,n}(G) = \prod_{ip^j \geq n} \gamma_i(G)^{(p^j)},$$

donde i, j sólo toman valores enteros no negativos.

Observación 1.3.4. Notemos que:

(a) $\mathcal{L}_{p,1}(G) = G$. Para verlo, basta notar que $\mathcal{L}_{p,1}(G)$ contiene el factor $\gamma_1(G)^{(p^0)} = G$.

(b) $\mathcal{L}_{p,n}$ es el producto de sólo una cantidad finita de subgrupos $\gamma_i(G)^{(p^i)}$. En efecto, como $\mathcal{L}_{p,n}(G) \supseteq \gamma_n(G)^{(p^0)} = \gamma_n(G)$, y $\gamma_n(G)$ es una serie descendente, todos los demás factores con $i \geq n$ son redundantes.

(c) Aún más, es evidente que para $i < n$, sólo el factor $\gamma_i(G)^{(p^j)}$, siendo j el menor entero con $ip^j \geq n$, cuenta para el producto.

(d) Por ser cada $\gamma_i(G)$ normal en G es directo comprobar que los subgrupos $\mathcal{L}_{p,n}(G)$ también lo son.

(e) Finalmente, fijado un primo p, $\{\mathcal{L}_{p,n}(G)\}_{n \geq 1}$ es una serie descendente de subgrupos característicos de G, pues aumentar n disminuye la cantidad de factores en el producto, y ya vimos que los $\gamma_i(G)$ eran subgrupos característicos.

Observación 1.3.5. A modo de ejemplo, caracterizamos explícitamente los tres primeros términos de la serie de Lazard. Es claro que, para cada p, $\mathcal{L}_{p,1}(G) = G$, y $\mathcal{L}_{p,2}(G) = G^{(p)}G'$, que coincide con el subgrupo de Frattini de G cuando es un p-grupo finito. En cambio, para $n = 3$ las series ya difieren según el valor de p:

$$\mathcal{L}_{2,3}(G) = G^{(4)}\gamma_2(G)^{(2)}\gamma_3(G), \qquad \text{y} \qquad \mathcal{L}_{p,3}(G) = G^{(p)}\gamma_2(G)^{(p)}\gamma_3(G) = G^{(p)}\gamma_3(G), \quad \text{para } p > 2.$$

Para probar el próximo lema precisaremos de una observación elemental sobre los coeficientes binomiales:

Observación 1.3.6. Sea p un primo, y $n \geq 1$ un entero. Denotemos por $|n|_p$ a la *p-parte* de n, es decir, $|n|_p = p^a$, siendo $n = p^a b$ con $p \nmid b$. Consideremos el coeficiente binomial $\binom{p^a}{i}$ para $i \geq 1$.

Sea A cualquier grupo de orden p^a. Entonces A actúa sobre el conjunto subyacente A mediante la multiplicación por la derecha, y por tanto A permuta sus subconjuntos de tamaño $i \geq 1$. Si S es uno de tales subconjuntos, y B es un estabilizador de S en A, entonces claramente S es una unión de clases laterales por la izquierda de B. Por tanto, el cardinal de B divide a $i = |S|$, de modo que $|B|$ divide a $|i|_p$, y el índice $(A : B)$ es divisible entre $p^a/|i|_p$. En definitiva, todas las órbitas bajo esta acción tienen cardinal divisible entre $p^a/|i|_p$. De esto y del hecho de que la cantidad total de conjuntos que están siendo permutados es precisamente $\binom{p^a}{i}$, se deduce que $p^a/|i|_p$ divide a $\binom{p^a}{i}$. Por tanto, $\left|\binom{p^a}{i}\right|_p \geq p^a/|i|_p$, y así se llega a que

$$i \cdot \left|\binom{p^a}{i}\right|_p \geq |i|_p \cdot \left|\binom{p^a}{i}\right|_p \geq p^a.$$

Lema 1.3.7. Sea G un grupo, y sea p un primo fijo cualquiera. Entonces $\{\mathcal{L}_{p,n}(G)\}_{n\geq 1}$ es una N_p-serie de G.

Demostración. Fijemos dos enteros $n, m \geq 1$ cualesquiera. Probaremos primero que es una N-serie, es decir, que verifica la inclusión $(\mathcal{L}_{p,m}(G), \mathcal{L}_{p,n}(G)) \subseteq \mathcal{L}_{p,m+n}(G)$. Por ser el último subgrupo normal en G, probar esta inclusión es equivalente a probar que $\mathcal{L}_{p,m}(G)$ y $\mathcal{L}_{p,n}(G)$ conmutan módulo $\mathcal{L}_{p,m+n}(G)$; y para probar ésto es suficiente probar que los generadores de ambos subgrupos conmutan módulo $\mathcal{L}_{p,m+n}(G)$.

Por definición, los generadores de $\mathcal{L}_{p,m}(G)$ son los elementos de la forma x^{p^s} con $x \in \gamma_r(G)$, y $rp^s \geq m$; análogamente, los generadores de $\mathcal{L}_{p,n}(G)$ son los elementos de la forma y^{p^v} con $y \in \gamma_u(G)$ y $up^v \geq n$. Por el Teorema 1.2.15 podemos escribir:

$$(x^{p^s}, y^{p^v}) = \prod_{\substack{1 \leq i \leq p^s \\ 1 \leq j \leq p^v}} c_{ij}^{\binom{p^s}{i}\binom{p^v}{j}},$$

donde c_{ij} es un producto de conmutadores de varias longitudes, teniendo cada uno de ellos al menos i componentes iguales a $x^{\pm 1} \in \gamma_r(G)$ y j componentes iguales a $y^{\pm 1} \in \gamma_u(G)$. Así, del Lema 1.2.7, junto con el hecho de que la serie $\{\gamma_n(G)\}_{n\geq 1}$ es descendente, se sigue directamente que cada uno de estos conmutadores está en $\gamma_{ir+ju}(G)$, y en consecuencia también $c_{ij} \in \gamma_{ir+ju}(G)$. Por tanto,

$$c_{ij}^{\binom{p^s}{i}\binom{p^v}{j}} \in \gamma_{ir+ju}(G)^{\binom{p^s}{i}\binom{p^v}{j}} = \gamma_{ir+ju}(G)^{\left|\binom{p^s}{i}\right|_p \left|\binom{p^v}{j}\right|_p}.$$

Ahora bien, si ponemos $t = (ir+ju)\cdot\left|\binom{p^s}{i}\right|_p \cdot \left|\binom{p^v}{j}\right|_p$, por definición $\gamma_{ir+ju}(G)^{\left|\binom{p^s}{i}\right|_p \left|\binom{p^v}{j}\right|_p} \subseteq \mathcal{L}_{p,t}(G)$. Notando ahora que

$$t = (ir+ju)\cdot\left|\binom{p^s}{i}\right|_p \cdot \left|\binom{p^v}{j}\right|_p \geq r \cdot i \cdot \left|\binom{p^s}{i}\right|_p + u \cdot j \cdot \left|\binom{p^v}{j}\right|_p \geq$$

(dado que por la Observación 1.3.6 $i \cdot \left|\binom{p^s}{i}\right|_p \geq p^s$ y $j \cdot \left|\binom{p^v}{j}\right|_p \geq p^v$)

$$\geq r \cdot p^s + u \cdot p^v \geq m + n;$$

de que la serie de Lazard sea descendente se deduce que $\mathcal{L}_{p,t}(G) \subseteq \mathcal{L}_{p,m+n}(G)$. Finalmente, concatenando todas estas inclusiones se obtiene que

$$c_{ij}^{\binom{p^s}{i}\binom{p^v}{j}} \in \mathcal{L}_{p,m+n}(G),$$

y como esto es válido para cada i, j, se concluye que también el producto de todos ellos $(x^{p^s}, y^{p^v}) \in \mathcal{L}_{p,m+n}(G)$. Esto prueba que los conmutadores considerados conmutan módulo $\mathcal{L}_{p,m+n}(G)$, y por tanto la serie en cuestión es una N-serie.

Queda ver que es p-restringida. A este fin, fijemos un $n \geq 1$ arbitrario y escribamos $H = \mathcal{L}_{p,n}(G)$ y $\overline{H} = H/\mathcal{L}_{p,np}(G)$. Será suficiente probar que para cada $g \in \mathcal{L}_{p,n}(G)$ se tiene que $g^p \in \mathcal{L}_{p,np}(G)$, o equivalentemente, que el grupo $\overline{H}$ tiene exponente divisor de p.

Un razonamiento inductivo sencillo nos lleva a que $\gamma_i(H) \subseteq \mathcal{L}_{p,ni}(G)$ para cada i; en efecto, en el caso $i = 1$ se da la igualdad, y si la tesis vale para i, entonces

$$\gamma_{i+1}(H) = (\gamma_i(H), H) \subseteq (\mathcal{L}_{p,ni}(G), H) \subseteq \mathcal{L}_{p,n(i+1)}(G),$$

donde la primera inclusión se tiene por hipótesis de inducción, mientras que la segunda vale por formar los $\mathcal{L}_{p,n}(G)$ una N-serie. En particular, hemos probado que $\gamma_p(H) \subseteq \mathcal{L}_{p,np}(G)$, de modo que por el Lema 1.1.13 obtenemos que $\gamma_p(\overline{H}) = \langle 1 \rangle$, y por tanto que $\overline{H}$ tiene clase de nilpotencia estrictamente menor que p.

Ahora, los generadores de H son de la forma $h = x^{p^j}$, con $x \in \gamma_i(G)$ e $ip^j \geq n$; por tanto $h^p = x^{p^{j+1}}$ e $ip^{j+1} \geq np$, y en consecuencia $h^p \in \mathcal{L}_{p,np}(G)$. Esto prueba que $\overline{H}$ está generado por elementos de orden p; entonces, como por el párrafo anterior $c(\overline{H}) < p$, podemos aplicar la Proposición 1.2.14 para deducir que $\overline{H}$ tiene exponente divisor p, y la prueba queda completa. □

Serie de Brauer-Jennings-Zassenhaus

Definición 1.3.8. Dado un grupo G, y un primo p, se define la *$\mathcal{M}$-serie de Brauer-Jennings-Zassenhaus* de G mediante:

(I) $\mathcal{M}_{p,1}(G) = G$;

(II) $\mathcal{M}_{p,n}(G) = (\mathcal{M}_{p,n-1}(G), G) \cdot \mathcal{M}_{p,i}(G)^{(p)}$, para $n \geq 2$, donde i es el menor entero verificando $ip \geq n$.

Es sencillo comprobar, por inducción, que se trata de una serie descendente de subgrupos característicos. Además, se tiene la siguiente relación evidente con la serie central inferior:

Observación 1.3.9. Notando que $(\mathcal{M}_{p,n-1}(G), G) \subseteq \mathcal{M}_{p,n}(G)$, un argumento inductivo obvio da que $\gamma_n(G) \subseteq \mathcal{M}_{p,n}(G)$ para cada n. En efecto, $\mathcal{M}_{p,1}(G) = G = \gamma_1(G)$, y si $\gamma_{n-1}(G) \subseteq \mathcal{M}_{p,n-1}(G)$, entonces $\gamma_n(G) = (\gamma_{n-1}(G), G) \subseteq (\mathcal{M}_{p,n-1}(G), G) \subseteq \mathcal{M}_{p,n}(G)$.

Observación 1.3.10. También es de destacar que para un grupo G cualquiera, el cociente de los dos primeros términos de la serie

$$\frac{\mathcal{M}_{p,1}(G)}{\mathcal{M}_{p,2}(G)} = \frac{G}{G'G^{(p)}}$$

es un grupo abeliano elemental.

Además, se tiene la siguiente relación trivial entre esta serie y la anterior:

Lema 1.3.11. Sea G un grupo, p un primo y $n \geq 1$ un entero. Entonces

$$\mathcal{L}_{p,n}(G) \subseteq \mathcal{M}_{p,n}(G).$$

Demostración. Para cada i, por la Observación 1.3.9 sabemos que $\gamma_i(G) \subseteq \mathcal{M}_{p,i}(G)$. Además, fijo i, por inducción sobre j se deduce fácilmente vale $\mathcal{M}_{p,i}(G)^{(p^j)} \subseteq \mathcal{M}_{p,ip^j}(G)$. En efecto, para $j = 1$ por definición es claro que $\mathcal{M}_{p,i}(G)^{(p)} \subseteq \mathcal{M}_{p,ip}(G)$, y si la tesis es cierta para j, entonces

$$\mathcal{M}_{p,i}(G)^{(p^{j+1})} \subseteq \left(\mathcal{M}_{p,i}(G)^{(p^j)}\right)^{(p)} \subseteq \mathcal{M}_{p,ip^j}(G)^{(p)} \subseteq \mathcal{M}_{p,ip^{j+1}}(G).$$

(la primera inclusión es directa, la segunda es la hipótesis de inducción, y la tercera se debe a la definición de $\mathcal{M}_{p,ip^{j+1}}(G)$, pues ip^j es el menor entero tal que $ip^j \cdot p \geq ip^{j+1}$). En resumen, hemos probado la cadena de inclusiones

$$\gamma_i(G)^{(p^j)} \subseteq \mathcal{M}_{p,i}(G)^{(p^j)} \subseteq \mathcal{M}_{p,ip^j}(G),$$

y como $\{\mathcal{M}_{p,n}(G)\}_{n\geq 1}$ es una serie descendente, se concluye que $\mathcal{M}_{p,n}(G)$ contiene a todos los subgrupos $\gamma_i(G)^{(p^j)}$ con $ip^j \geq n$, y por tanto también su producto $\mathcal{L}_{p,n}(G) \subseteq \mathcal{M}_{p,n}(G)$.

□

Para demostrar la inclusión recíproca, haremos uso de otra caracterización la misma serie, la de los *subgrupos de dimensión* de G, noción *a priori* también dependiente de algún cuerpo de característica p; por ello, con el fin poder introducir antes todos estos conceptos retrasaremos la demostración hasta el Capítulo 3.

Capítulo 2

Álgebras de grupo

Presentamos en este breve capítulo la noción de álgebra de grupo, tras lo cual se introducen algunos de los objetos que de forma más básica intervienen en el estudio de su estructura, entre los que se destaca el ideal de aumento, sobre cuya estructura a su vez profundizaremos, para cierto caso de especial interés, en el capitulo subsiguiente. Se completa el capítulo describiendo el Problema del Isomorfismo para álgebras de grupo (tanto en su versión general como en la modular). Además, para facilitar la fluidez del texto asumimos conocidos a partir de ahora los rudimentos de las teorías de anillos, módulos y álgebras (sólo las definiciones y las propiedades más elementales), para los que nos remitimos a [1] y al segundo Capítulo de [29].

Las dos primeras secciones se basan en los primeros capítulos de [33] y en el Capítulo 2 de [29]; la última sección se apoya en la estructura y los resultados del Capítulo 14 de [33].

2.1. La noción de álgebra de grupo

Hacemos notar que en la mayoría de definiciones y resultados en esta sección, y en una parte de los resultados posteriores, es posible sustituir el cuerpo K por cualquier anillo conmutativo con uno R, y en algunos casos incluso por anillos con uno arbitrarios (en este sentido, véase [39]). Sin embargo, y dado que para los objetivos de este trabajo sólo son de relevancia las álgebras de grupo sobre cuerpos (de hecho, sólo sobre cuerpos de característica p, con p primo) sacrificamos con [33] esa tan amplia generalidad, obteniendo a cambio unas pruebas y desarrollos algo más sencillos y agradables de leer. En todo el capítulo. salvo indicación K denotará a un cuerpo cualquiera, y G a un grupo.

Definición 2.1.1. Sea G un grupo y K un cuerpo. Se define el *álgebra de grupo* $(K[G], +, \cdot)$, o simplemente $K[G]$, como la K-álgebra asociativa que tiene por base a los elementos de G, y con la multiplicación '$\cdot$' definida distributivamente usando la multiplicación en el grupo.

Más concretamente, $K[G]$ será el conjunto de todas las sumas formales de la forna

$$\alpha = \sum_{g \in G} a_g g,$$

con $a_g \in K$ para cada g, tales que sólo hay una cantidad finita de coeficientes a_g no nulos. Si $\beta = \sum_{g \in G} b_g g$ es otro elemento de $K[G]$, las operaciones vienen dadas por

$$\alpha + \beta = \sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g,$$

y

$$\alpha\beta = \left(\sum_{g \in G} a_g g \right) \left(\sum_{g \in G} b_g g \right) = \sum_{g,h \in G} a_g b_h \cdot gh = \sum_{x \in G} c_x x,$$

siendo

$$c_x = \sum_{gh=x} a_g b_h = \sum_{g\in G} a_b b_{g^{-1}x} = \sum_{h\in G} a_{xh^{-1}} b_h;$$

y la multiplicación por escalares, para cada $a \in K$, viene dada por

$$a\alpha = a\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G}(aa_g)g.$$

Es un ejercicio sencillo ver que en efecto estas operaciones dotan a $K[G]$ con estructura de K-álgebra asociativa, e identificando cada elemento $g \in G$ con $g \cdot 1 \in K[G]$, podemos considerar G como un subconjunto de $K[G]$, que claramente forma una base del mismo.

Proposición 2.1.2 (Propiedad universal)**.** Sea G un grupo y K un cuerpo. Dado cualquier K-álgebra A, y cualquier aplicación $f : G \to A$ tal que $f(gh) = f(g)f(h)$ para cada $g, h \in G$, existe un único homomorfismo de K-álgebras $f^* : K[G] \to A$ tal que conmuta el diagrama:

$$\begin{array}{ccc} G & \xrightarrow{\ i\ } & K[G] \\ & \searrow^{f} & \downarrow{\scriptstyle f^*} \\ & & A \end{array}$$

donde $i : G \to K[G]$ es la inclusión.

Demostración. Dada una aplicación $f : G \to A$ como en el enunciado, consideremos $f^* : K[G] \to A$ definida mediante

$$f^*\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g f(g).$$

Que $f^* \circ i = f$ es evidente, y ver tanto que f^* es en efecto un homomorfismo de K-álgebras como que es el único en estas condiciones es de comprobación directa. □

De hecho, se comprueba fácilmente que todas las K-álgebras que verifican las condiciones sobre $K[G]$ en la proposición anterior son isomorfas, lo que constituye una definición alternativa de álgebra de grupo. Además, a partir de esta proposición se deduce fácilmente que:

Corolario 2.1.3. *Sean $f : G \to H$ un homomorfismo de grupos y K un cuerpo. Entonces existe un único homomorfismo de K-álgebras $\tilde{f} : K[G] \to K[H]$ tal que $\tilde{f}(g) = f(g)$ para cada $g \in G$. Además, si f es un epimorfismo (resp. monomorfismo), entonces $\tilde{f}$ también es un epimorfismo (resp. monomorfismo).*

Elementos de un álgebra de grupo

Definición 2.1.4. Sean $K[G]$ un álgebra de grupo, y $\alpha = \sum_{g\in G} a_g g \in K[G]$. Se define el *soporte* de α, $\mathrm{Sop}(\alpha)$, mediante:

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

Es inmediato que $\mathrm{Sop}\,\alpha$ es un subconjunto finito de G, y que es vacío si y sólo si $\alpha = 0$.

Observación 2.1.5. Destacamos la siguiente propiedad evidente de $\mathrm{Sop}(\alpha)$: si $\alpha \neq 0$ y $g \in G$, entonces $\mathrm{Sop}(g\alpha) = g\,\mathrm{Sop}(\alpha)$, y $\mathrm{Sop}(\alpha g) = \mathrm{Sop}(\alpha)g$. En particular, si $x \in \mathrm{Sop}(\alpha)$, entonces $1 \in \mathrm{Sop}(x^{-1}\alpha)$, y $1 \in \mathrm{Sop}(\alpha x^{-1})$.

Sea ahora H un subgrupo de G. Entonces el K-subespacio vectorial generado por los elementos de $H \subseteq G \subseteq K[G]$ es claramente el subespacio subyacente de $K[H]$. Es entonces inmediato que

$$K[H] = \{\alpha \in K[G] \ : \ \mathrm{Sop}(\alpha) \subseteq H\}.$$

Además, hay una proyección natural $\pi_H : K[G] \to K[H]$, dada por

$$\pi_H\left(\sum_{g\in G} a_g g\right) = \sum_{g\in H} a_g g.$$

Es decir, si $\alpha \in K[G]$, entonces $\alpha = \pi_H(\alpha) + \alpha'$, donde $\mathrm{Sop}(\alpha') \cap H = \emptyset$, y $\mathrm{Sop}(\alpha - \alpha') \subseteq H$. Es inmediato que π_H es un homomorfismo de espacios vectoriales, pero no es en general un homomorfismo de K-álgebras.

Lema 2.1.6. Sea H un subgrupo de un grupo G, y sea Y un transversal por la izquierda de H en G. Entonces cada elemento $\alpha \in K[G]$ se puede expresar de forma única como una suma finita de la forma

$$\alpha = \sum_{y\in Y} y\alpha_y, \qquad \text{con } \alpha_y \in K[H].$$

En otras palabras, Y es una base de $K[G]$ como $K[H]$-módulo por la izquierda.

Demostración. Sea $\alpha \in K[G]$. Por ser $\mathrm{Sop}\,\alpha$ finito, está contenido en una cantidad finita de clases laterales por la izquierda de H, digamos $y_1H, y_2H, \ldots, y_nH$ con $y_i \in Y$. Podemos entonces escribir

$$\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_n, \qquad \text{siendo} \qquad \alpha_i = \sum_{x\in y_iH} a_x x.$$

Observando ahora que de $x \in y_iH$ se sigue que $y_i^{-1}x \in H$, se deduce que también $y_i^{-1}\alpha_i \in K[H]$; por tanto, la expresión

$$\alpha = \sum_{i=1}^{n} y_i(y_i^{-1}\alpha_i)$$

es como la buscada. Para ver la unicidad, sea $\alpha = \sum_{y\in Y} y\alpha_y$ como en el enunciado, y sea $y_0 \in Y$. Entonces $y_0^{-1}\alpha = \sum_{y\in Y} y_0^{-1}y\alpha_y$, de modo que, teniendo en cuenta la equivalencia "$y_0^{-1}y \in H$ si y sólo si $y = y_0$" para cada $y \in Y$, se deduce que

$$\pi_H(y_0^{-1}\alpha) = y_0^{-1}y_0\alpha_{y_0} = \alpha_{y_0};$$

como esto vale para cada $y_0 \in Y$, la expresión del enunciado ha de ser única. □

Observación 2.1.7. Notemos que G actúa sobre $K[G]$ por conjugación. En efecto, para cada $g \in G$, se considera la aplicación $(\cdot)^g : K[G] \to K[G]$ dada por $\alpha^g = g^{-1}\alpha g$ para cada $\alpha \in K[G]$; la aplicación asociada a $1 \in G$ es la identidad, y además esta asignación es compatible con la operación de G, puse para cada $g, h \in G$:

$$(\alpha^g)^h = h^{-1}\alpha^g h = h^{-1}g^{-1}\alpha gh = (gh)^{-1}\alpha gh = \alpha^{gh}.$$

Aún más, cada una de estas aplicaciones $(\cdot)^g$ es un homomorfismo de K-álgebras, pues para cada $\alpha, \beta \in K[G]$ y cada $a \in K$ valen:

$$(\alpha + \beta)^x = x^{-1}(\alpha + \beta)x = x^{-1}\alpha x + x^{-1}\beta x = \alpha^x + \beta^x,$$

$$(\alpha\beta)^x = x^{-1}\alpha\beta x = x^{-1}\alpha x x^{-1}\beta x = \alpha^x\beta^x,$$

y

$$(a\alpha)^x = x^{-1}a\alpha x = ax^{-1}\alpha x = a\alpha^x.$$

Finalmente, notemos que estos homomorfismos han de ser automorfismos, pues $(\cdot)^g$ es el homomorfismo inverso de $(\cdot)^{g^{-1}}$.

El centro de un álgebra de grupo

Estudiamos también cómo son los elementos del centro de un álgebra de grupo:

Teorema 2.1.8. *Sea G un grupo y K un cuerpo. Entonces el conjunto de los elementos de la forma*

$$\sigma_C = \sum_{g \in C} g,$$

donde C es una clase de conjugación de G, forma una base de $\mathcal{Z}(K[G])$, el centro del álgebra de grupo $K[G]$.

Demostración. Sea C una clase de conjugación cualquiera. En primer lugar probaremos que $\sigma_C \in \mathcal{Z}(K[G])$. En efecto, dado un $x \in G$ cualquiera, se tiene que

$$(\sigma_C)^x = \sum_{g \in C} x^{-1} g x = \sum_{g \in C_i} g = \sigma_C,$$

por lo que será $x\sigma_C = \sigma_C x$, por lo que σ_C es central.

En segundo lugar, vemos que los σ_C son linealmente independientes. Si hubiese una relación de dependencia lineal de la forma

$$\sum_{C \in \mathrm{Cl}(G)} a_C \sigma_C = 0,$$

casi todos los a_C nulos, podríamos escribir

$$\sum_{C \in \mathrm{Cl}(G)} a_C \sum_{g \in C} g,$$

y como las distintas sumas de clase tienen soportes disjuntos, la independencia lineal de los elementos de G garantiza que $a_C = 0$ para cada C.

Finalmente, comprobamos que los σ_C generan $\mathcal{Z}(K[G])$. Sea $\alpha = \sum_{g \in G} a_g g \in \mathcal{Z}(K[G])$. Sea $h \in \mathrm{Sop}(\alpha)$, y $x \sim h$ cualquier conjugado de h en G, digamos $x = y^{-1}hy$, con $y \in G$. Entonces, como α es central,

$$\sum_{g \in G} a_g g = \alpha = \alpha^y = \sum_{g \in G} a_g y^{-1} g y,$$

de modo que, como el coeficiente que acompaña a x ha de ser el mismos en ambos lados de la igualdad, ha de ser $a_x = a_h$. Como esto ocurre para cada $x \sim h$, se deduce que los coeficientes de α son constantes sobre las clases de conjugación, de modo que, escribiendo $a_C = a_g$ si $g \in C$, podemos escribir:

$$\alpha = \sum_{C \in \mathrm{Cl}(G)} a_C \sigma_C.$$

□

Equivalentemente, la prueba del teorema anterior da que:

Corolario 2.1.9. *Sean G un grupo y K un cuerpo. Dado un elemento $\alpha = \sum_{g \in G} a_g g \in K[G]$, se verifica la equivalencia: $\alpha \in \mathcal{Z}(K[G])$ si y sólo si $a_g = a_h$ para cada $g \sim h$, i.e., para cada h conjugado de g en G.*

Conmutadores de Lie

Definición 2.1.10. Sea A un álgebra sobre un cuerpo K. Un *conmutador de Lie* será un elemento de la forma $[\alpha, \beta] = \alpha\beta - \beta\alpha$, con $\alpha, \beta \in A$. Se define el subespacio conmutador de A, al que denotamos por $[A, A]$, como el K-subespacio vectorial de A conformado por todos los conmutadores de Lie.

Que en efecto es un espacio vectorial es claro, pues para cada $x \in K$, y cada $\alpha, \beta \in A$ se tiene que

$$x[\alpha, \beta] = x(\alpha\beta - \beta\alpha) = x\alpha\beta - \beta x\alpha = [x\alpha, \beta] \in [A, A].$$

Además, se define recursivamente el conmutador de Lie de n elementos mediante $[\alpha_1, \alpha_2, \ldots, \alpha_n] = [[\alpha_1, \ldots, \alpha_{n-1}], \alpha_n]$. Dados subconjuntos $S_1, S_2, \ldots, S_n$ de A, denotaremos por $[S_1, S_2, \ldots, S_n]$ al subespacio vectorial generado por los conmutadores de Lie de la forma $[s_1, s_2, \ldots, s_n]$, con $s_i \in S_i$.

Si además exigimos que el cuerpo K sea de característica p, obtenemos que:

Lema 2.1.11. Sea A un álgebra sobre un cuerpo K de característica $p > 0$. Sean $\alpha_1, \alpha_2, \ldots, \alpha_m \in A$, y $n > 0$ un entero; escribamos además $q = p^n$. Entonces existe un elemento $\beta \in [A, A]$ tal que:

$$(\alpha_1 + \alpha_2 + \cdots + \alpha_m)^q = \alpha_1^q + \alpha_2^q + \cdots + \alpha_m^q + \beta.$$

Demostración. Observemos que

$$(\alpha_1 + \alpha_2 + \cdots + \alpha_m)^q = \alpha_1^q + \alpha_2^q + \cdots + \alpha_m^q + \beta,$$

donde β es la suma de todos los elementos de la forma $\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_q}$ con al menos dos subíndices distintos, elementos que podemos ver como palabras sobre el alfabeto $\alpha_1, \alpha_2, \ldots \alpha_m$. Si dadas dos palabras, ω_1 y ω_2, una es una permutación cíclica de la otra, i.e., si

$$\omega_1 = \alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_q}, \qquad \omega_2 = \alpha_{i_j}\alpha_{i_{j+1}}\ldots\alpha_{i_q}\alpha_{i_1}\ldots\alpha_{i_{j-1}},$$

entonces es claro que $\omega_1 - \omega_2 = \gamma\delta - \delta\gamma \in [A, A]$, siendo

$$\gamma = \alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_{j-1}}, \qquad \delta = \alpha_{i_{j+1}}\ldots\alpha_{i_q}.$$

Por tanto, fijada una palabra ω cualquiera, todas sus permutaciones cíclicas son equivalentes módulo $[A, A]$. Consideremos la acción del grupo cíclico C_1 de orden q sobre el conjunto de las permutaciones cíclicas de ω. Se ve fácilmente que el número de permutaciones formalmente distintas de ω que aparecen en β es el tamaño de una órbitacon más de un elemento, y por tanto es divisible por p; en consecuencia, su suma se anula módulo $[A, A]$. Como esto ocurre para cada palabra ω que aparezca en β, y la relación de "ser una permutación cíclica" es de equivalencia, también β sea anula módulo $[A, A]$. □

Finalmente, restringiéndonos al caso en que $A = K[G]$ se trata de un álgebra de grupo arbitraria, tenemos que:

Lema 2.1.12. Sea K un cuerpo y G un grupo. Se verifica:

(I) $[K[G], K[G]]$ es el subespacio vectorial de $K[G]$ generado por todos los conmutadores de Lie de la forma $[g, h]$, con $g, h \in G$.

(II) Sea $\gamma = \sum_{g\in G} c_g g \in K[G]$. Entonces $\gamma \in [K[G], K[G]]$ si y sólo si $\sum_{h\sim g} c_h = 0$ para cada $g \in G$. En particular, $c_g = 0$ para cada $g \in \mathcal{Z}(G)$.

Demostración.

(I) Sean $\alpha = \sum_{g\in G} a_g g$ y $\beta = \sum_{g\in G} b_g g$ dos elementos de $K[G]$. Entonces

$$[\alpha, \beta] = \left[\sum_{g\in G} a_g g, \sum_{g\in G} b_g g\right] = \sum_{g,h\in G} a_g b_h [g, h];$$

por los tanto, los elementos de la forma $[g, h]$ con $g, h \in G$ también generan $[K[G], K[G]]$.

(II) Sea $\gamma = \sum_{g\in G} c_g g \in [K[G], K[G]]$. Entonces por el apartado anterior γ es una combinación K-lineal de elementos de la forma $gh - hg$, siendo $hg = g^{-1}ghg$ un conjugado de gh. Como la propiedad considerada obviamente cerrada para combinaciones K-lineales, se sigue que $\sum_{h\sim g} c_h = 0$ para cada $g \in G$. Recíprocamente, si γ verifica esta propiedad para los coeficientes, es sencillo comprobar que habrá de ser combinación lineal de elementos de la forma $g - g^h$; y como estos elementos son conmutadores de Lie, pues

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

el resultado se sigue.

□

2.2. Aplicación de aumento e ideales de aumento

Si en el Corolario 2.1.3 partimos de un epimorfismo $G \to \{1\}$, obtenemos obtenemos un epimorfismo $K[G] \to K$, que resulta ser central en el estudio de las álgebras de grupo: la llamada aplicación de aumento.

Definición 2.2.1. Sea K un cuerpo y G un grupo. Llamamos *aplicación de aumento* del álgebra de grupo $K[G]$ al homomorfismo $\varepsilon : K[G] \to K$ dado por

$$\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g.$$

Además, llamaremos a su núcleo *ideal de aumento* de $K[G]$, y lo denotamos por $\mathrm{Aug}_K(G)$.

Además, dado un elemento $\alpha \in K[G]$, llamamos *aumento de* α al valor $\varepsilon(\alpha) \in K$.

Observación 2.2.2. Es evidente que el ideal $\mathrm{Aug}_K(G)$ es bilátero, por ser el núcleo de un homomorfismo; y maximal, pues por ser ϵ un epimorfismo, $K[G]/\mathrm{Aug}_K(G) \cong K$.

Proposición 2.2.3. El conjunto $\{g-1 \ : \ g \in G, g \neq 1\}$ es una base de $\mathrm{Aug}_K(G)$ como K-espacio vectorial.

Demostración. Dado un elemento $\alpha = \sum_{g\in G} a_g g \in \mathrm{Aug}_K(G) = \ker(\varepsilon)$ se tiene que $0 = \varepsilon(\alpha) = \sum_{g\in G} a_g = 0$, de modo que se puede reescribir α de la forma

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

Como claramente todos los elementos de la forma $g - 1$ están en $\mathrm{Aug}_K(G)$, ya tenemos que el conjunto del enunciado es un conjunto generador de este subespacio. Finalmente, notando que estos elementos son linealmente independientes (pues cualquier relación de dependencia K-lineal entre ellos implicaría una relación de dependencia K-lineal entre los elementos de la base G) se obtiene el resultado. □

La proposición anterior da pie a la siguiente generalización de la noción de ideal de aumento:

Definición 2.2.4. Dado un subgrupo H de G, denotamos por $\mathrm{Aug}_K(G, H)$ al ideal por la derecha de $K[G]$ generado por el conjunto $\{h - 1 \ : \ h \in H\}$, esto es,

$$\mathrm{Aug}_K(G, H) = \left\{\sum_{h\in H} \alpha_h(h-1) \ : \ \alpha_h \in K[G]\right\} = K[G] \cdot \mathrm{Aug}_K(H).$$

Es ciertamente una generalización, pues:

Lema 2.2.5. Sea H un subgrupo de un grupo G, y sea S un conjunto de generadores de H. Entonces el conjunto $C = \{s - 1 \ : \ s \in S\}$ es un conjunto de generadores de $\mathrm{Aug}_K(G, H)$ como ideal por la derecha de $K[G]$.

Demostración. Sea B el subconjunto de elementos de $h \in H$ tales que $h-1$ está en el ideal generado por C. Es evidente que $S \subseteq B$, y que además B es un subgrupo, pues dados $x, y \in B$, se tiene que

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

está en el ideal generado por C, y por tanto $xy^{-1} \in B$. Por tanto, necesariamente será $B = H$. Esto prueba que el ideal generado por C contiene al conjunto $\{h - 1 \ : \ h \in H\}$, que es generador de $\mathrm{Aug}_K(G, H)$, y por tanto C también genera a este ideal.

□

Proposición 2.2.6. Sea H un subgrupo de G, y $X = \{q_i\}_{i \in I}$ un transversal por la izquierda de H en G que contenga a 1. Entonces el conjunto:

$$B_H = \{q(h - 1) \ : \ q \in X, h \in H, h \neq 1\}$$

es una base de $\mathrm{Aug}_K(G, H)$ como K-espacio vectorial.

Demostración. Veamos primero la independencia lineal. Supongamos que existe una combinación lineal

$$\sum_{i,j} a_{ij} q_i (h_j - 1) = 0, \qquad \text{con } a_{ij} \in K;$$

entonces podemos escribir

$$\sum_{i,j} a_{ij} q_i h_j - \sum_i \left(\sum_j a_{ij} \right) q_i = 0.$$

Notando que en la expresión anterior los elementos del grupo $q_i h_j$ y q_i no se repiten por ser Xun transversal, la independencia lineal de los elementos de G da que necesariamente $a_{ij} = 0$ para cada par de índices i, j.

Por otro lado, es inmediato que los elementos de la forma $g(h - 1)$ con $g \in G$, $h \in H$, generan $\mathrm{Aug}_K(G, H)$ como K-espacio vectorial, de modo que para probar que B_H es un conjunto generador es suficiente probar que cualquier elemento $g(h - 1)$ de tal forma puede ser escrito como una combinación lineal de elementos de B_H. Y esto es sencillo, pues escribiendo $g = q_i h_j$, para ciertos $q_i \in X$, $h_j \in H$, se tiene que

$$g(h - 1) = q_i h_j (h - 1) = q_i (h_j h - 1) - q_i (h_j - 1).$$

□

Este ideal es de especial interés cuando H es un subgrupo normal de G. En tal caso,el homomorfismo canónico $\rho_H : G \to G/H$ puede ser extendido a un epimorfismo (que denotamos de la misma manera) $\rho_H : K[G] \to K[G/H]$ en virtud del Corolario 2.1.3; más concretamente, esta aplicación será la dada por:

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

Proposición 2.2.7. Sea H un subgrupo normal de un grupo G. Con la notación de arriba,

$$\mathrm{Ker}(\rho_H) = \mathrm{Aug}_K(G, H).$$

Demostración. Sea de nuevo X un transversal de H en G que contiene a 1. Entonces cada elemento $\alpha \in K[G]$ puede escribirse como una suma finita de elementos de la forma

$$\alpha = \sum_{i,j} a_{ij} q_i h_j, \qquad \text{con } a_{ij} \in K,\ q_i \in X,\ \text{y } h_j \in H.$$

Si denotamos por $\overline{q_i}$ a la clase de q_i en el grupo cociente G/H, tenemos que

$$\rho_H(\alpha) = \sum_i \left(\sum_j a_{ij} \right) \overline{q_i},$$

siendo las clases $\overline{q}_i$ distintas. Se tiene entonces que $\alpha \in \mathrm{Ker}(\rho_H)$ si y sólo si $\sum_j a_{ij} = 0$ para cada i. Así, si $\alpha \in \mathrm{Ker}(\rho_H)$ podemos escribir:

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

Esto prueba que $\mathrm{Ker}(\rho_H) \subseteq \mathrm{Aug}_K(G,H)$; como la inclusión recíproca se tiene trivialmente, hemos terminado. □

Observación 2.2.8. Además, si repetimos las dos últimas proposiciones intercambiando izquierda y derecha, si H es un subgrupo normal de G también se obtiene

$$\mathrm{Aug}_K(H) \cdot K[G] = \mathrm{Ker}(\rho_H) = K[G] \cdot \mathrm{Aug}_K(H).$$

De esta proposición también se sigue directamente el próximo:

Corolario 2.2.9. *Sea H un subgrupo normal de un grupo G. Entonces $\mathrm{Aug}_K(G,H)$ es un ideal bilátero de $K[G]$ y*

$$\frac{K[G]}{\mathrm{Aug}_K(G,H)} \cong K[G/H].$$

Proposición 2.2.10. Sea H un subgrupo de un grupo G, y K un cuerpo. Entonces

$$G \cap (1 + \mathrm{Aug}_K(G,H)) = H.$$

Demostración. Supongamos que g está en la intersección. Entonces $g - 1 \in \mathrm{Aug}_K(G,H)$, de modo que por la Proposición 2.2.6 se puede escribir en la forma:

$$g - 1 = \sum_{q \in X, h \in H} a_{qh} q(h-1),$$

siendo X un transversal de H en G que contiene a 1, y $a_{qh} \in K$. Como 1 aparece en el miembro izquierdo de la igualdad, ha de haber un sumando de la forma $r_{1h}(1-h) = (1-h)$ en el lado derecho de la igualdad; y como los elementos de G que aparecen como sumandos en el lado derecho son distintos dos a dos, ha de ser $g = h \in H$. Esto prueba la inclusión hacia la derecha; la recíproca es trivial. □

Concluimos por el momento el estudio de estos ideales observando cómo se comportan sus potencias, y los conmutadores de Lie de sus elementos.

Proposición 2.2.11. Sea H un subgrupo normal de un grupo G y $n \geq 1$ un entero. Entonces

$$\mathrm{Aug}_K(G,H)^n = \mathrm{Aug}_K(H)^n \cdot K[G].$$

Demostración. Procedemos por inducción sobre n. El caso $n = 1$ se tiene por definición. Supongamos la propiedad cierta para $n \geq 1$. La inclusión

$$\mathrm{Aug}_K(G,H)^{n+1} \supseteq \mathrm{Aug}_K(H)^{n+1} \cdot K[G]$$

es cierta trivialmente, pues $\mathrm{Aug}_K(H) \subseteq \mathrm{Aug}_K(G,H)$ se conserva si tomamos potencias.

Para ver el contenido recíproco, sea xy un generador del ideal $\mathrm{Aug}_K(G,H)^{n+1}$, con $x \in \mathrm{Aug}_K(G,H)^n$ e $y \in \mathrm{Aug}_k(G,H)$. Por la hipótesis de inducción x es combinación $K[G]$-lineal de elementos de $x_i \in \mathrm{Aug}_K(H)^n$, mientras que por el caso base y es combinación $K[G]$-lineal de elementos $y_j \in \mathrm{Aug}_K(H)$. Así, usando la Observación 2.2.8 es fácil ver que el producto xy es combinación $K[G]$-lineal de los elementos $x_i y_j \in \mathrm{Aug}_K(H)^{n+1}$. Esto prueba que $xy \in \mathrm{Aug}_K(H)^{n+1} \cdot K[G]$. □

Notemos que en la proposición previa no se usa en ningún momento la estructura del álgebra de grupo, ni del ideal de aumento; por tanto, la misma demostración nos permite deducir una propiedad mucho más general: si R es un anillo cualquiera, S un subanillo de R e I un ideal de R tal que $I \cdot R = R \cdot I$, entonces $I \cdot R$ es un ideal bilátero de R, e $(I \cdot R)^n = I^n \cdot R$.

Ahora, generalizando la Proposición 2.2.6 tenemos que:

Proposición 2.2.12. Sea H un subgrupo normal de un grupo G y $n \geq 1$ un entero. Si B es una base de $\mathrm{Aug}_K(H)^n$ como K-espacio vectorial y X un transversal de H en G que contenga a 1, entonces

$$C = \{qb \ : \ q \in X, \ b \in B\}$$

es una base de $\mathrm{Aug}_K(G,H)^n$.

Demostración. Veamos primero la independencia lineal. Si hubiese una relación de dependencia lineal entre ellos, digamos

$$\sum_{q \in X, b \in B} a_{qb} = 0, \qquad \text{con } a_{qb} \in K,$$

ésta se puede reescribir como:

$$\sum_{q \in X} q \left(\sum_{b \in B} a_{qb} b \right) = 0;$$

como cada $b \in \mathrm{Aug}_K(H)^n$, es claro que los sumandos $q \sum_{b \in B} a_{qb} b$ tienen soporte disjunto, por lo que habrá de ser

$$\sum_{b \in B} a_{qb} b = 0$$

para cada $q \in X$, y como los elementos de B son linealmente independientes, necesariamente será $a_{qb} = 0$ para cada $q \in X$, $b \in B$.

Veamos ahora que C es un conjunto generador. Es inmediato que los elementos de la forma gb con $g \in G$, $b \in B$, generan $\mathrm{Aug}_K(G,H)^n$ como K-espacio vectorial, de modo que para probar que C es un conjunto generador es suficiente probar que cualquier elemento gb de dicha forma puede ser escrito como una combinación lineal de elementos de C. Y esto es sencillo, pues escribiendo $g = qh$, para ciertos $q \in X$, $h \in H$, se tiene que $b = qhb$, y como $hb \in \mathrm{Aug}_K(H)^n$, es combinación lineal de elementos de B, digamos $hb = \sum_i a_i b_i$, con $a_i \in K$, $b_i \in B$; por tanto,

$$gb = \sum_i a_i q b_i$$

es una combinación lineal de elementos de C, con lo que concluye la prueba. □

Corolario 2.2.13. *Sea K un cuerpo, G un grupo y H un subgrupo normal de G. Entonces vale la igualdad:*

$$\dim_K \left(\mathrm{Aug}_K(G,H)^t \right) = (G : H) \cdot \dim_K (\mathrm{Aug}_K(H)^t).$$

Demostración. Si B es una base de $\mathrm{Aug}_K(H)^t$ y X es un transversal de H en G que contiene a 1, por la Proposición 2.2.12 $\mathrm{Aug}_K(G,H)^t$ tiene una base de la forma

$$C = \{qb \ : \ q \in X, b \in B\},$$

por lo que

$$\dim_K \left(\mathrm{Aug}_K(G,H)^t\right) = |C| =$$
$$|X| \cdot |B| = (G:H) \cdot \dim_K(\mathrm{Aug}_K(H)^t).$$

□

Relacionando las nociones de conmutador y de ideal de aumento, damos un último lema:

Lema 2.2.14. Sea K un cuerpo, G un grupo, y H, L dos subgrupos de G. Entonces

$$[K[H], K[L]] \subseteq \mathrm{Aug}_K\left(G, (H,L)\right)$$

(donde, recordemos, (H,L) denota al subgrupo generado por los conmutadores).

Demostración. Se comprueba directamente (ver la prueba de la primera parte del Lema 2.1.12) que los elementos de la forma $[h,l]$ con $h \in H$ y $l \in L$ generan $[\mathbb{F}_p[H], \mathbb{F}_p[L]]$, por lo que será suficiente probar que éstos están en $\mathrm{Aug}_K\left(G,(H,L)\right)$. Y en efecto:

$$[h,l] = hl - lh = (hlh^{-1}l^{-1} - 1)lh = ((h^{-1},l^{-1}) - 1)lh \in \mathrm{Aug}_K\left(G,(H,L)\right).$$

□

Isomorfismos normalizados y grupos de unidades

Dado un anillo arbitrario R, denotaremos por $\mathcal{U}(R)$ al grupo de las unidades de R. Particularizando al caso en que $R = K[G]$ es un álgebra de grupo, es obvio que todos los elementos de G son unidades; sin embargo, el recíproco no es cierto. Además, es inmediato que ningún elemento $\alpha \in \mathcal{U}(K[G])$ puede tener aumento 0, pues en tal caso sería $\epsilon(1) = 0$, y por tanto habría de ser $K = \{0\}$, y por convenio no admitimos cuerpos con un solo elemento. Por tanto,

$$\mathcal{U}(K[G]) \subseteq K[G] \setminus \mathrm{Aug}_K(G).$$

Observación 2.2.15. Se observa también fácilmente que si $K[G]$ y $K[H]$ son dos álgebras de grupo, dado cualquier isomorfismo de álgebras de θ de $K[G]$ a $K[H]$, la restricción de este a $\mathcal{U}(K[G])$ da un isomorfismo entre los respectivos grupos de unidades.

Se define también el *Grupo de unidades normalizadas* de $K[G]$ como:

$$V(K[G]) = \{\alpha \in \mathcal{U}(K[G]) \ : \ \epsilon(\alpha) = 1\}.$$

Aunque la Observación 2.2.15 no se puede extender directamente a este nuevo grupo de unidades (pues la imagen de una unidad de aumento 1 es necesariamente una unidad, pero no hay garantías de que tenga aumento 1) aún podemos obtener una versión análoga si nos restringimos a cierta clase de isomorfismos.

Definición 2.2.16. Sea θ un isomorfismo entre dos álgebras de grupo, $\theta : K[G] \to K[H]$. Denotemos por ε_G y ε_H a las respectivas aplicaciones de aumento en $K[G]$ y en $K[H]$. Decimos que θ *preserva el aumento* si se tiene que $\varepsilon_G = \varepsilon_H \circ \theta$, i.e., si conmuta el diagrama:

$$\begin{array}{ccc} K[G] & \xrightarrow{\theta} & K[H] \\ & \searrow^{\varepsilon_G} & \downarrow{\scriptstyle \varepsilon_H} \\ & & K \end{array}$$

En este caso también decimos que θ es un *isomorfismo normalizado.*

Además, si existe un isomorfismo cualquiera, el siguiente lema garantiza que también existe uno normalizado.

Lema 2.2.17. Sea $\theta : K[G] \to K[H]$ un isomorfismo entre álgebras de grupo. Entonces existe un isomorfismo normalizado $\tilde{\theta} : K[G] \to K[H]$.

Demostración. Basta definir $\tilde{\theta}$ mediante

$$\tilde{\theta}\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} \frac{a_g}{(\varepsilon_H \circ \theta)(g)}\theta(g), \qquad \text{para cada } \sum_{g\in G} a_g g \in K[G].$$

Es claro que está bien definida, pues por ser $g \in G$ unidad en $K[G]$ también lo es $\theta(g)$, y por lo visto arriba necesariamente $\varepsilon_H(\theta(g)) \neq 0$; el resto de comprobaciones también son rutinarias. □

Por tanto, y como es claro que la restricción a $V(K[G])$ de cualquier isomorfismo normalizado de $K[G]$ a $K[H]$ da lugar a un isomorfismo de grupos, hemos obtenido un análogo a la Observación 2.2.15. Profundizaremos más sobre este hecho en el Capítulo 4.

2.3. El Problema del Isomorfismo

Definición 2.3.1. Sea K un cuerpo y G un grupo. Decimos que G está *determinado* por el álgebra de grupo $K[G]$ si, para cada grupo H vale al implicación:

$$K[G] \cong K[H] \qquad \Rightarrow \qquad G \cong H.$$

Es entonces natural preguntarse, cuando uno estudia álgebras de grupo, si dados un grupo G y un cuerpo K, es cierto que G está determinado por su álgebra de grupo $K[G]$. Esta pregunta se explicita el denominado *Problema del Isomorfismo* para álgebras de grupo, que abreviamos por **(IP)**, y formulamos como sigue:

Problema 1 (IP). *Sea G un grupo y K un cuerpo arbitrario. ¿Está G determinado por el álgebra de grupo $K[G]$?*

No es demasiado difícil deducir que este problema tiene respuesta negativa en general. En efecto, sea G un grupo abeliano finito de orden n. Entonces se puede comprobar que[1]

$$\mathbb{C}[G] \cong \underbrace{\mathbb{C} \oplus \mathbb{C} \oplus \cdots \oplus \mathbb{C}}_{n \text{ veces}},$$

i.e., $\mathbb{C}[G]$ es isomorfo (como $\mathbb{C}$-álgebra) a n copias de $\mathbb{C}$. Por tanto, para cualquier otro grupo abeliano finito H de orden n se tiene que $\mathbb{C}[G] \cong \mathbb{C}[H]$, aunque H no sea isomorfo a G.

Aún más, el siguiente resultado de D.S. Passman garantiza que, incluso limitándonos a la clase de los p-grupos finitos el Problema del Isomorfismo tiene respuesta negativa en general; de hecho, el resultado da respuesta negativa para todos los cuerpos con característica distinta de p.

Teorema 2.3.2. *Para $n \geq 23$ existe un conjunto de*

$$p^{\frac{2}{27}(n^3-23n^2)}$$

p-grupos no isomorfos de orden p^n que tienen álgebras de grupo isomorfas sobre todos los cuerpos con característica distinta de p.

[1] La prueba es ciertamente directa (se sigue del Teorema de Wedderburn-Artin, en particular del Corolario 3.4.10 de [29]) utilizando la semisimplicidad de $\mathbb{C}[G]$; sin embargo, dado que en este trabajo no se utilizará tal noción (por no ser las álgebras de grupo que nos interesarán a partir de ahora –de p-grupos finitos sobre cuerpos de característica p– semisimples, de acuerdo con el recíproco del Teorema de Maschke; véase, por ejemplo, el Corolario 3.4.8 de [29]), nos remitimos a la introducción de Capítulo 14 de [33].

Demostración. Ver Teorema 14.1.11 de [33]. □

Por tanto, sólo sigue teniendo sentido dar una respuesta positiva a **(IP)** si las álgebras de grupo consideradas se toman sobre cuerpos de característica p, cuando el grupo considerado es un p-grupo. Y cuando el grupo considerado no es un p-grupo, incluso en la limitada clase de los grupos metacíclicos se pueden encontrar contraejemplos al Problema del Isomorfismo: en efecto, en [12] E.C. Dade describe dos grupos metabelianos finitos no isomorfos cuyas álgebras de grupo sobre todos los cuerpos posibles son isomorfas.

Adquiere entonces obvia relevancia la siguiente restricción de **(IP)**, que llamamos *Problema del Isomorfismo Modular Amplio*, y abreviamos por **(WMIP)**:

Problema 2 (**WMIP**)**.** *Sea G un p-grupo finito y K un cuerpo de característica p. ¿Está G está determinado por el álgebra de grupo $K[G]$?*

A la hora de estudiar este problema, en muchas ocasiones es mucho más sencillo trabajar sobre el cuerpo primo de p elementos $\mathbb{F}_p$; de hecho, la mayoría de los resultados conocidos hasta ahora (y por tanto también la mayoría de resultados que presentamos en este trabajo) sobre este problema se limitan a considerar el caso particular de las álgebras de grupo modulares $\mathbb{F}_p[G]$. Este es el llamado *Problema del Isomorfismo Modular*, o abreviadamente, **(MIP)**:

Problema 3 (**MIP**)**.** *Sea G un grupo p-grupo finito y $\mathbb{F}_p$ el cuerpo de p elementos. ¿Está G está determinado por el álgebra de grupo modular $\mathbb{F}_p[G]$?*

En otro orden de cosas, y haciendo una pequeña digresión en la línea de nuestro trabajo, es de destacar que, si permitimos en la definición de álgebra de grupo sustituir el cuerpo K por un anillo conmutativo con unidad R cualquiera (es evidente que tal definición sigue siendo válida), podemos replantear el Problema 1 como:

Problema 4 (**IP'**)**.** *Sea G un grupo y R un anillo conmutativo con uno. ¿Está G está determinado por el álgebra de grupo $R[G]$?*

Los mismos argumentos y resultados anteriores muestran que este problema, más amplio, sigue teniendo respuesta negativa en general. Sin embargo, durante algún tiempo se conjeturó que en el caso en que $R = \mathbb{Z}$, el anillo de los enteros, era cierto que cada grupo G estaba determinado por su álgebra de grupo $\mathbb{Z}[G]$. Sin embargo M. Hertweck da en [18] un contraejemplo a esta conjetura, de modo que, incluso en esta versión del Problema del Isomorfismo, el planteamiento restringido de **(WMIP)**, y en particular el de **(MIP)**, sigue siendo la única restricción razonable del problema sobre la que existen expectativas de una solución general positiva.

Por todo esto, dedicamos el presente trabajo a recopilar algunos resultados conocidos concernientes a los problemas **(WMIP, MIP)**. Para ello, es imprescindible haber estudiado previamente la estructura de las álgebras de grupo sobre cuerpos de característica p, y en particular sobre el cuerpo de p elementos; éste es el objetivo del capítulo próximo.

Capítulo 3

Álgebras de grupo sobre cuerpos de característica p

Iniciamos en este capítulo un estudio algo más profundo de la estructura de las álgebras de grupo $K[G]$, prestando especial atención a aquellas en las que K es un cuerpo de característica p y G es un p-grupo finito.

Para esta última situación (aunque no en todos los resultados exigimos que G sea un p-grupo finito), en la primera sección obtenemos una caracterización del ideal de aumento $\mathrm{Aug}_K(G)$ únicamente en términos de la estructura de anillo de $K[G]$ (de hecho, será el ideal de Jacobson); en la segunda se introduce la noción de filtración graduada del ideal de aumento, y su estrecha relación con la de N_p-serie de G (podemos obtener N_p-series a partir de filtraciones graduadas, y viceversa), lo que nos permite definir una en principio nueva N_p-serie de G, la llamada *serie de los subgrupos de dimensión* $\{D_{K,n}\}_{n\geq 1}$ a partir de la filtración natural del ideal de aumento (i.e., la de sus potencias). Además, probaremos que esta serie coincide tanto con la serie de Lazard como con la de Brauer-Jennings-Zassenhaus, lo que justifica nuestro comentario tras el Lema 1.3.11. Finalmente, utilizamos las dos últimas secciones para estudiar en mayor profundidad la estructura de las álgebras de grupo modulares (i.e., sobre cuerpos de p elementos) mediante los *ideales de Zassenhaus* de $K[G]$ y ciertas potencias de los ideales de aumento, y para identificar ciertos subgrupos del grupo de las unidades normalizadas.

La principal referencia del capítulo es [33], y en menor medida [39]. Más concretamente, las dos primeras secciones están basadas en [33]: la primera toma resultados de los Capítulos 3 y 8, y para la segunda seguimos mayormente el Capítulo 3 y parte del Capítulo 11; a su vez, estos capítulos se apoyan en los resultados originales de [23]. En la tercera utilizamos resultados de fuentes diversas, que iremos citando según se presenten. Finalmente, en la cuarta y última de ellas reorganizamos libremente algunos resultados del Capítulo III de [39], ligeramente inspirados por la introducción de [20].

3.1. El ideal de aumento

En esta breve sección simplemente establecemos la nilpotencia del ideal de aumento, obteniendo a partir de ella su caracterización como el ideal de Jacobson, y, como consecuencia, caracterizaciones explícitas de los grupos de unidades. Comenzamos recordando la noción de ideal nilpotente, así como la de ideal de Jacobson, y algunas de sus propiedades.

Definición 3.1.1. Sea R un anillo. Un elemento $r \in R$ se dice *nilpotente* si existe un entero $n > 0$ tal que $r^n = 0$. Un ideal I de R se dice *nilpotente* si existe un entero $n > 0$ tal que $I^n = \{0\}$.

Es claro que todo elemento de un ideal nilpotente es nilpotente; en cambio el recíproco, i.e., la afirmación "un ideal cuyos elementos todos son nilpotentes es nilpotente", no es cierta en general.

Definición 3.1.2. Un ideal I en un anillo R se dice *maximal* si para cada ideal J con $I \subseteq J \subseteq R$ se tiene que o bien $I = J$, o bien $I = R$.

Con la ayuda del Lema de Zorn se puede probar que todo anillo contiene al menos un ideal maximal (ver Lema 2.4.3 de [29]).

Definición 3.1.3. Sea R un anillo. Se define el *ideal de Jacobson* de R como la intersección de todos los ideales maximales (por la izquierda) de R. Denotamos a este ideal por $J(R)$, o simplemente JR.

De hecho, es un resultado conocido que el ideal de la definición anterior también coincide con la intersección de todos los ideales maximales (por la derecha) de R. También es bien conocida la siguiente caracterización de $J(R)$:

Lema 3.1.4. Sea R un anillo, y $a \in R$. Entonces $a \in J(R)$ si y sólo si $1 - ab$ es una unidad para cada $b \in R$.

Referencia de la demostración. Ver Teorema 15.3 de [1]. □

Lema 3.1.5. Sea I un ideal nilpotente de un anillo R. Entonces $I \subseteq J(R)$.

Demostración. Por el lema anterior es suficiente probar que $1-ab$ es una unidad para cada $a \in I$ y cada $b \in R$. Como $ab \in I$, en particular es nilpotente, digamos que $(ab)^n = 0$. Entonces el elemento $x = (1 + ab + (ab)^2 + \cdots + (ab)^{n-1})$ claramente verifica $x(1 - ab) = (1 - ab)x = 1$. □

Proposición 3.1.6. Sea G un p-grupo finito, y K un cuerpo con característica p. Entonces el ideal $\mathrm{Aug}_K(G)$ es nilpotente.

Demostración. Escribimos $|G| = p^e$, y procedemos por inducción sobre e. El caso $|G| = 1$ es trivial, pues sería $G = \langle 1 \rangle$, y por tanto $\mathrm{Aug}_K(G) = 0$.

Sea ahora $|G| = p$. Entonces $G = \langle x \rangle$ es cíclico de orden p. Entonces $\mathrm{Aug}_K(G) = \langle x - 1 \rangle$, el ideal principal generado por $x-1$. En efecto, por la Proposición 2.2.3 sabemos que $\mathrm{Aug}_K(\langle x \rangle)$ está generado por elementos de la forma $x^i - 1$, y cada uno de estos elementos está en $\langle x-1 \rangle$, en virtud de la igualdad

$$x^i - 1 = (x - 1)(1 + x + \cdots + x^{i-1});$$

la inclusión recíproca es evidente. Y entonces $\mathrm{Aug}_K(\langle x \rangle)^p = \{0\}$, pues $K[\langle x \rangle]$ es conmutativo, y $(x - 1)^p = x^p - 1 = 1 - 1 = 0$.

Finalmente, sea G un p-grupo con orden $|G| = p^e$, $e > 1$, y supongamos la proposición cierta para $e - 1$. Sea H un subgrupo normal de orden p (que de hecho será central, por el Lema 1.1.18). Entonces, dado que $|G/H| = p^{e-1}$, por la hipótesis de inducción tenemos que existe un entero positivo n tal que $\mathrm{Aug}_K(G/H)^n = \{0\}$. Además, es claro que

$$\rho_H(\mathrm{Aug}_K(G)) \subseteq \mathrm{Aug}_K(G/H) \quad \Rightarrow \quad \rho_H(\mathrm{Aug}_K(G)^n) \subseteq \mathrm{Aug}_K(G/H)^n = \{0\},$$

de modo que

$$\mathrm{Aug}_K(G)^n \subseteq \mathrm{Ker}(\rho_H) = \mathrm{Aug}_K(G, H),$$

donde la igualdad se debe a la Proposición 2.2.7. Ahora bien, como por el caso cíclico de orden p existe un entero m tal que $\mathrm{Aug}_K(H)^m = \{0\}$, tenemos que

$$\mathrm{Aug}_K(G)^{nm} \subseteq \mathrm{Aug}_K(H, G)^m = \mathrm{Aug}_K(H)^m K[G] = \{0\}.$$

donde la primera igualdad se tiene por la Proposición 2.2.11.

□

De hecho, el recíproco del resultado anterior también es cierto, es decir, dado un grupo no trivial G y un cuerpo K, si $\mathrm{Aug}_K(G)$ es nilpotente entonces G es un p-grupo finito y $\mathrm{char}\, K = p$; (cf. Lema 3.1.6 de [33]); sin embargo, no entraremos en la prueba de este hecho, por no ser necesario para nuestros objetivos.

Lema 3.1.7. Sea G un p-grupo finito, y K un cuerpo de característica p. Entonces el ideal de Jacobson $JK[G]$ coincide con el ideal de aumento $\mathrm{Aug}_K(G)$.

Demostración. Dado que sabemos por la Observación 2.2.2 que $\mathrm{Aug}_K(G)$ es un ideal maximal de $K[G]$, claramente $JK[G] \subseteq \mathrm{Aug}_k(G)$. Recíprocamente, basta notar como $\mathrm{Aug}_K(G)$ es nilpotente por la Proposición 3.1.6, estará contenido en el ideal de Jacobson (ver Lema 3.1.5). □

Definición 3.1.8. De un anillo R decimos que es un *anillo local* si tiene un único ideal maximal por la izquierda.

Se puede comprobar (ver Proposición 15.15 de [1]) que en un anillo local R, el complementario del grupo de las unidades $\mathcal{U}(R)$ es precisamente el único ideal maximal por la izquierda, que será $J(R)$. Es decir, $R \setminus J(R) = \mathcal{U}(R)$.

Corolario 3.1.9. *Sea G un p-grupo finito y K un cuerpo de característica p. Entonces $K[G]$ es un anillo local.*

Demostración. Trivial; el ideal de Jacobson (que es la intersección de todos los ideales maximales) es un ideal maximal, por lo que es el único de estos ideales. □

Dado un par de subconjunto S y T de un álgebra de grupo $K[G]$, denotamos por $T + S$ al conjunto de los elementos de $K[G]$ de la forma $t + s$ con $s \in S$ y $t \in T$. En particular, cuando $T = \{1\}$ escribiremos $T + S = 1 + S$. Se obtienen entonces las siguientes caracterizaciones de los grupos de unidades:

Corolario 3.1.10. *Sea G un p-grupo y K un cuerpo de característica p. Entonces*

(I) $\mathcal{U}(K[G]) = \mathcal{U}(K) + \mathrm{Aug}_K(G)$.

(II) $V(K[G]) = 1 + \mathrm{Aug}_K(G)$.

Demostración. En primer lugar, notemos que por ser el anillo local el grupo de sus unidades será precisamente el complementario de $JK[G] = \mathrm{Aug}_K(G)$ en $K[G]$. Ahora, es claro que $\{1\} \cup \{g - 1 : g \in G,\ g \neq 1\}$ es una base de $K[G]$, siendo la segunda componente de la unión una base de $\mathrm{Aug}_k(G)$. Por tanto, cada elemento de $K[G]$ admite una (única) expresión de la forma $a + \alpha$, con $a \in K$ y $\alpha \in \mathrm{Aug}_K(G)$; tal elemento obviamente tiene aumento a. Se sigue entonces que el grupo de unidades es el de los elementos con $a \neq 0$; y el grupo de unidades normalizadas, el de los elementos con $a = 1$. □

3.2. Filtraciones del ideal de aumento y subgrupos de dimensión

Definición 3.2.1. Sea R un anillo arbitrario, e I un ideal bilátero de R. Por una *filtración* de I entendemos una serie decreciente $I = E_1 \supseteq E_2 \supseteq \ldots$ de ideales biláteros de R. Además, decimos que la filtración es *graduada* si $E_i E_j \subseteq E_{i+j}$ para cada i, j.

En este trabajo nos limitaremos a tratar filtraciones graduadas del ideal $\mathrm{Aug}_K(G)$ en el álgebra de grupo $K[G]$; más concretamente, nuestro estudio se centrará en la filtración natural del ideal de aumento dada por sus potencias, i.e., $\{\mathrm{Aug}_k(G)^n\}_{n \geq 1}$, que evidentemente es graduada.

De filtraciones a N-series

El resultado siguiente da una manera de obtener N-series a partir de filtraciones del ideal de aumento:

Proposición 3.2.2. Sea G un grupo y K un cuerpo. Sea $\{E_i\}_{i \in \mathbb{N}}$ una filtración del ideal $\mathrm{Aug}_R(G)$. Definamos $G_i = G \cap (1 + E_i)$, para cada i. Entonces:

(I) $G = G_1 \geq G_2 \geq \cdots \geq G_n \geq \ldots$ es una sucesión decreciente de grupos normales de G.

(II) Si la filtración $\{E_i\}_{i\geq 1}$ es graduada, entonces $\{G_i\}_{i\geq 1}$ es una N-serie. Si además $\mathrm{char}(K)$ es un primo p, entonces $\{G_i\}_{i\geq 1}$ es una N_p-serie.

Demostración.

(I) Claramente $G_1 = G \cap (1 + \mathrm{Aug}_K(G)) = G$, y $G_i \supseteq G_{i+1}$ para cada i. Además, si $x, y \in G_i$ y $z \in G$, entonces

$$xy^{-1} - 1 = ((x-1) - (y-1))y^{-1} \in E_i,$$

luego $xy^{-1} \in G_i$, lo que prueba que G_i es un subgrupo; y

$$z^{-1}xz - 1 = z^{-1}(x-1)z \in E_i,$$

luego $z^{-1}xz \in G_i$, lo que prueba que G_i es normal en G.

(II) Sean $x \in G_i$, $y \in G_j$. Entonces $(x-1) \in E_i$ e $(y-1) \in E_j$; y por ser la filtración graduada se tiene que $(x-1)(y-1), (y-1)(x-1) \in E_{i+j}$. En consecuencia,

$$(x,y) - 1 = xyx^{-1}y^{-1} - x^{-1}y^{-1} =$$

$$= x^{-1}y^{-1}\left((x-1)(y-1) - (y-1)(x-1)\right) \in E_{i+j},$$

y por lo tanto $(x,y) \in 1 + E_{i+j}$. Esto prueba que $(G_i, G_j) \leq G_{i+j}$, y por tanto que los G_i forman una N-serie.

Asumamos ahora que la característica de K es p. Entonces para cada $x \in K[G]$ vale la identidad $(x-1)^p = x^p - 1$. Así, si $x \in G_i$, entonces $x - 1 \in E_i$, de modo que por ser la filtración graduada $x^p - 1 = (x-1)^p \in E_{ip}$. Esto da que $x^p \in 1 + E_{ip}$, y por tanto $x^p \in G_{ip}$.

□

De N_p-series a filtraciones

En esta subsección, K denotará a un cuerpo de característica $p > 0$, y G a un p-grupo. En ella estableceremos una suerte de recíproco del lema precedente, en una situación algo más restringida: obtendremos filtraciones graduadas del ideal de aumento de $K[G]$ a partir de N_p-series del grupo G.

Lema 3.2.3. Sean K un cuerpo de característica p; sea también G un grupo con $|G| = p^n$. Sea $G = H_1 \rhd H_2 \rhd \cdots \rhd H_{n+1} = \langle 1 \rangle$ una serie de subgrupos tales que $|H_i/H_{i+1}| = p$ para cada $i \geq 1$. Para cada $i \geq 1$, tomemos un elemento $x_i \in H_i \setminus H_{i+1}$. Entonces los elementos:

$$\eta(a_1, \ldots, a_n) = (x_1 - 1)^{a_1}(x_2 - 1)^{a_2} \ldots (x_n - 1)^{a_n},$$

con $0 \leq a_i < p$, forman una base de $K[G]$ como K-espacio vectorial. Además, estos elementos sin $\eta(0, 0, \ldots, 0) = 1$ forman una base de $\mathrm{Aug}_K(G)$.

Demostración. Comenzamos notando que para $i = 0, \ldots, p-1$, y $x \in G$, vale:

$$x^i = ((x-1)+1)^i = \sum_{j=0}^{i} \binom{i}{j} (x-1)^j. \tag{3.1}$$

Dado que hay exactamente $p^n = |G|$ elementos de la forma $\eta(a_1, \ldots, a_n)$, basta probar que forman un conjunto generador de $K[G]$. Procederemos por inducción sobre n, pero antes hacemos un par de observaciones.

Como G/H_2 es cíclico de orden p se tiene que $|H_2| = p^{n-1}$; además como G/H_2 está generado por la imagen de x_1, se deduce que $\{1, x_1, x_1^2, \ldots, x_1^{p-1}\}$ es un transversal de H_2 en G, de manera que cada elemento α de $K[G]$ puede reescribirse de la forma

$$\alpha = \sum_{i=0}^{p-1} x_1^i \alpha_i, \qquad \text{con } \alpha_i \in R[H_2]. \tag{3.2}$$

Realizamos ahora el razonamiento inductivo. Si $n = 1$, necesariamente $H_2 = \langle 1 \rangle$ y $K[H_2] \cong K$, de modo que por las fórmulas (3.1) y (3.2) cualquier elemento $\alpha \in K[G]$ puede escribirse como combinación K-lineal de elementos de la forma $\eta(a_1)$.

Sea ahora $n > 1$, y la hipótesis de inducción cierta para exponentes menores. En particular ésta se verifica para H_2, por lo que los elementos de la forma

$$\eta(0, a_2, \ldots, a_n) = (x_2 - 1)^{a_2} \ldots (x_n - 1)^{a_n}$$

generan $K[H_2]$. Así, de nuevo considerando las ecuaciones (3.1) y (3.2), también se deduce que cualquier elemento $\alpha \in K[G]$ se puede escribir como K-combinación lineal de elementos de la forma $\eta(a_1, \ldots, a_n)$, y la primera afirmación del lema queda probada.

Para la afirmación sobre $\mathrm{Aug}_K(G)$, notemos que cada uno de estos elementos $\eta(a_1, \ldots, a_n)$, con los a_i no todos nulos, están en $\mathrm{Aug}_K(G)$, pues la aplicación de aumento verifica:

$$\varepsilon((x_1 - 1)^{a_1} \ldots (x_n - 1)^{a_n}) = (\varepsilon(x_1) - 1)^{a_1} \ldots (\varepsilon(x_n) - 1)^{a_n} = 0.$$

La prueba concluye notando que, por lo ya probado, estos elementos son K-linealmente independientes, y además generan todo $\mathrm{Aug}_K(G)$, pues cualquier elemento

$$\alpha = \sum_{a_1, \ldots, a_n} r_{a_1, \ldots, a_n} \eta(a_1, \ldots, a_n) \in \mathrm{Aug}_K(G)$$

verifica

$$0 = \varepsilon(\alpha) = \sum_{a_1, \ldots, a_n} r_{a_1, \ldots, a_n} \varepsilon(\eta(a_1, \ldots, a_n)) = r_{0, \ldots, 0}.$$

□

Sea G un p-grupo finito, supongamos dada una N_p-serie de G,

$$G = G_1 \geq G_2 \geq \cdots \geq G_d \geq G_{d+1} = \langle 1 \rangle.$$

Entonces, para cada $g \in G$, se define la *altura* de g como $\nu(g) = \sup\{m \in \mathbb{N} \ : \ g \in G_m\}$. Notemos que $\nu(1) = \infty$ (pues en realidad se trata de una serie infinita, con $G_i = \langle 1 \rangle$ para cada $i \geq d + 1$), y para $g \neq 1$, $\nu(g) = m$ si y solo si $G \in G_m \setminus G_{m+1}$.

Para cada entero $i \geq 1$, sea $E_i \subseteq K[G]$ el conjunto de todas las combinaciones K-lineales de todos los productos de la forma:

$$(g_1 - 1)(g_2 - 1) \ldots (g_k - 1)$$

para algún k con $\nu(g_1) + \nu(g_2) + \ldots \nu(g_k) \geq i$. Es fácil ver que E_i es un ideal de $K[G]$, pues es cerrado bajo multiplicación por 1 y cualquier $g - 1$, y por tanto por cualquier $g \in G$. Además, es de comprobación directa que

$$\mathrm{Aug}_K(G) = E_1 \supseteq E_2 \supseteq \ldots E_i \supseteq \ldots$$

y que $E_i E_j \subseteq E_{i+j}$ para cada i, j. Por tanto, $\{E_i\}_{i \geq 1}$ es una filtración graduada del ideal de aumento. Decimos que esta es la *filtración graduada de* $\mathrm{Aug}_K(G)$ *determinada por la serie* $\{G_i\}$.

Dada ahora una N_p-serie $\{G_i\}$, podemos refinarla (quitando previamente los posibles términos repetidos) a una serie de composición

$$G = H_1 > H_2 > \ldots > H_{n+1} = \langle 1 \rangle,$$

de modo que, tomando elementos $x_i \in H_{i+1} \setminus H_i$, por el Lema 3.2.3 se obtiene una base de $K[G]$. Llamamos a cualquier base así obtenida una *base de Jennings generalizada de* $K[G]$ *obtenida de la* N_p*-serie* $\{G_i\}$. Además, a cada uno de los elementos de tal base,

$$\eta = \eta(a_1, \ldots, a_n) = (x_1 - 1)^{a_1} \ldots (x_n - 1)^{a_n},$$

con $0 \leq a_i < p$, le asociamos un *peso*

$$w(\eta) = a_1\nu(x_1) + a_2\nu(x_2) + \cdots + a_n\nu(x_n).$$

Lema 3.2.4. Con la notación anterior, los elementos de la base de Jennings generalizada de la forma $\eta(a_1, \ldots, a_n)$ que verifican $w(\eta) = t$ generan E_t módulo E_{t+1}.

Demostración. Observemos que, por las definiciones de $w(\eta)$ y E_i es inmediato que si $w(\eta) \geq t$, entonces $\eta \in E_t$. Para probar que estos elementos generan E_t módulo E_{t+1}, debemos probar la siguiente:

Tesis: "Cada producto $\pi = (g_1 - 1)(g_2 - 1) \ldots (g_k - 1)$ con $\nu(g_1) + \nu(g_2) + \cdots + \nu(g_n) \geq t$ puede reescribirse como una combinación K-lineal de η's de peso t más un término en E_{t+1}".

Simplificará considerablemente esta tarea la afirmación siguiente:

- Afirmación 1: "Para demostrar la tesis, es suficiente hacerlo para productos de la forma $\pi' = (x_{i_1} - 1)(x_{i_2} - 1) \ldots (x_{i_k} - 1)$, con $\nu(x_{i_1}) + \nu(x_{i_2}) + \cdots + \nu(x_{i_k}) \geq t$".

  Para verlo, tomemos un factor particular $g_i - 1$ de π, de modo que $\pi = \alpha(g_i - 1)\beta$. Escribamos $\nu(g_i) = v$; así, $g_i \in G_v$. Por ser la serie $\{H_s\}_{s \geq 1}$ un refinamiento de $\{G_s\}_{s \geq 1}$, se tiene que $G_v = H_r > H_{r+1} > \ldots > H_{n+1} = \langle 1 \rangle$. Entonces, por el Lema 3.2.3 $g_i - 1$ es una combinación K-lineal de elementos de la forma

  $$\eta' = (x_r - 1)^{a_r}(x_{r+1} - 1)^{a_{r+1}} \cdots (x_n - 1)^{a_n},$$

  donde los a_i no son todos nulos. Pero cada $x_s \in H_s \subseteq G_v$, por lo que $\nu(x_s) \geq v = \nu(g_i)$; por lo que, claramente podemos escribir

  $$g_i - 1 = \sum_{\nu(x_s) = v} b_s(x_s - 1) + \gamma,$$

  para ciertos $b_s \in K$, $\gamma \in E_{v+1}$. Por tanto,

  $$\pi = \alpha(g_i - 1)\beta = \sum_{\nu(x_s) = v} b_s\alpha(x_s - 1)\beta + \alpha\gamma\beta \equiv \sum_{\nu(x_s) = v} b_s\alpha(x_s - 1)\beta \mod E_{t+1}.$$

  En consecuencia, probar la tesis para π es equivalente a probarla para $\sum_{\nu(x_s)=v} b_s\alpha(x_s - 1)\beta$, de modo que es suficiente hacerlo para elementos de la forma $\alpha(x_s - 1)\beta$ (que verifiquen la condición sobre las alturas). Aplicando este argumento reiteradamente a cada factor $(g_i - 1)$ (de los restantes, en α y β), queda probada la Afirmación 1.

Ahora probaremos la tesis por inducción sobre k: si $k = 1$, por la Afirmación 1 podemos limitarnos a $\pi' = (x_j - 1)$ para cierto j con $\nu(x_j) \geq t$. En tal caso, π' es un elemento η de la base, de peso $\geq t$. Si fuese $w(t) = t$, hemos terminado, y si es $w(\eta) > t$, por nuestra observación inicial $\eta \in E_{t+1}$, y por tanto es la combinación lineal nula, módulo E_{t+1}.

Supongamos ahora que la tesis es cierta para todos los productos π' con menos de k factores. Para dar el paso inductivo necesitaremos la siguiente:

- Afirmación 2: "Para probar la tesis en el caso en que π tiene k factores es suficiente hacerlo para productos de la forma $\pi'' = (x_1-1)^{b_1}(x_1-1)^{b_2}\dots(x_n-1)^{b_n}$, con $0 \leq b_i$, $b_1+b_2+\dots+b_n = k$ y $\sum_{i=1}^n b_i\nu(x_i) \geq t$".

  En efecto, por la Afirmación 1 podemos limitarnos a productos de la forma $\pi' = (x_{i_1}-1)(x_{i_2}-1)\dots(x_{i_k}-1)$; aislemos dos factores adyacentes de π', de modo que $\pi' = \alpha(x_i-1)(x_j-1)\beta$. Escribamos $r = \nu(x_i)$ y $s = \nu(x_j)$, y consideremos la identidad

$$(x_i-1)(x_j-1) = (x_j-1)(x_i-1) + (x_i^{-1}x_j^{-1}x_ix_j-1) + (x_jx_i-1)(x_i^{-1}x_j^{-1}x_ix_j-1).$$

  Pongamos por comodidad $h = x_i^{-1}x_j^{-1}x_ix_j$; entonces por estar $x_i \in G_r$ y $x_j \in G_s$, tenemos que $h \in (G_r, G_s) \subseteq G_{r+s}$. Por tanto, $\nu(h) \geq r+s$, y de ahí que $(x_jx_i-1)(h-1) \in E_{r+s+1}$. Se sigue entonces que

$$\pi' = \alpha(x_i-1)(x_j-1)\beta \equiv \alpha(x_j-1)(x_i-1)\beta + \alpha(h-1)\beta \mod E_{t+1}$$

  Notemos que $\alpha(h-1)\beta$ es un producto de, a lo sumo, $k-1$ factores, pero con altura total no menor que t. Entonces por hipótesis de inducción es una combinación lineal de η's de peso t; de modo que para probar que π' lo es es suficiente probarlo para $\alpha(x_j-1)(x_i-1)\beta$. Esto prueba que, en lo que a la tesis respecta, no importa el orden en que aparezcan los (x_i-1) en el producto; podemos entonces reeordenarlos en el orden natural para obtener una expresión de la forma de π'', y la Afirmación 2 queda también probada.

Podemos limitarnos a llevar a cabo la demostración para productos de la forma π'' (i.e., como en la afirmación precedente). Distinguimos entonces dos posibilidades. Si todos los b_i son menores que p, entonces

$$\pi'' = (x_1-1)^{b_1}(x_2-1)^{b_2}\dots(x_n-1)^{b_n} = \eta(b_1,\dots,b_n) = \eta,$$

y $w(\eta) \geq t$, y por tanto la tesis se sigue, argumentando como en el caso $k=1$.

Si por el contrario, para algún i vale $b_i \geq p$, entonces $(x_i-1)^p = (x_i^p-1)$ es un factor de π'', por lo que podemos escribir

$$\pi'' = \alpha(x_i-1)^p\beta = \alpha(x^p-1)\beta,$$

que es un producto con menos de k factores. Además, si $\nu(x_i) = s$, entonces $x_i \in G_s$, de forma que $x_i^p \in G_{sp}$ y en consecuencia $\nu(x_i^p) \geq sp$. Por tanto, la suma de las alturas de los factores en esta nueva representación de π'' sigue siendo mayor o igual que t, la tesis se sigue por la hipótesis de inducción, y el paso inductivo queda completo. □

Lema 3.2.5. Con la misma notación, los elementos de la base de Jennings generalizada $\eta(a_1, a_2, \dots, a_n)$ con $w(\eta) \geq t$ forman una base de E_t.

Demostración. Ya sabemos que $w(\eta) \geq t$ implica que $\eta \in E_t$; así como que los η's son linealmente independientes (Lema 3.2.3). Por tanto, bastará probar que estos η's generan E_t. Ahora bien, aplicando repetidamente el Lema 3.2.4 se comprueba que el conjunto de los η's con $s \geq w(\eta) \geq t$ genera E_t módulo E_{s+1} para cada $s \geq t$. Por tanto, será suficiente probar que $E_{s+1} = 0$ para algún s lo suficientemente grande.

A este fin, recordemos por el Lema 3.1.6 que $\mathrm{Aug}_K(G)$ es nilpotente, por lo que existe un $k > 0$ tal que $\mathrm{Aug}_K(G)^k = 0$. Ahora bien, $G_{d+1} = \langle 1 \rangle$, por lo que todos los elementos de la forma

$$\pi = (g_1-1)(g_2-1)\dots(g_k-1)$$

verifican $\nu(g_1)+\nu(g_2)+\dots+\nu(g_k) \leq dk$; esto prueba que todo producto con menos de k factores no puede estar en E_{dk} , y por tanto $E_{dk} \subseteq \mathrm{Aug}_K(G)^k = 0$. Por tanto, $E_{dk} = 0$, y hemos terminado. □

Llamaremos *base adaptada a la filtración del ideal de aumento* $\{E_t\}_{t\geq 1}$ a cualquiera base $\mathscr{B}$ de $K[G]$ que contenga a 1, con un peso asociado w (i.e., una función $w : \mathscr{B} \to \mathbb{N}$) tal que para cada $t \geq 1$ los elementos de peso t generen E_t módulo E_{t+1}.

En particular, dada una N_p-serie $\{G_t\}_{t\geq 1}$ y la filtración del ideal de aumento $\{E_t\}_{t\geq 1}$ obtenida a partir de ella como arriba, el Lema 3.2.4 garantiza que cualquier base de Jennings generalizada $\mathscr{B}$ obtenida a partir de $\{G_t\}_{t\geq 1}$ es adaptada a la filtración $\{E_t\}_{t\geq 1}$.

Teorema 3.2.6 (Jennings)**.** *Sea K un cuerpo de característica $p > 0$ y sea G un p-grupo finito. Supongamos que*

$$G = G_1 \geq G_2 \geq \cdots \geq G_d \geq G_{d+1} = \langle 1 \rangle.$$

es una N_p-serie con $|G_t/G_{t+1}| = p^{e_t}$. Sea $\{E_i\}_{i\geq 1}$ la filtración de $\mathrm{Aug}(KG)$ *determinada por $\{G_i\}$, y escribamos $E_0 = KG$.*

*(*I*) Sea $m = \sum_{t=1}^{d}(p-1)e_t$. Entonces $E_m \neq 0$, pero $E_{m+1} = 0$.*

*(*II*) Si $f_t = \dim E_t/E_{t+1}$, entonces el polinomio $\sum_{t=0} f_t\zeta^t \in \mathbb{Z}[\zeta]$, donde ζ es una indeterminada, viene dado por*

$$\sum_{t=0} f_t\zeta^t = \prod_{i=1}^{d} \Phi_p(\zeta^i)^{e_i},$$

siendo $\Phi_p(\zeta) = 1 + \zeta^2 + \zeta^3 + \cdots + \zeta^{p-1}$ es el p-ésimo polinomio ciclotómico.

*(*III*) Sea $t \geq 1$. Si $x \in G$, entonces $x - 1 \in E_t$ si y sólo si $x \in G_t$.*

Demostración. Notemos que es posible que algunos de los e_i's sean 0. Notemos también que dada una serie de composición $\{H_i\}_{i\geq 1}$ que sea un refinamiento de $\{G_i\}_{i\geq 1}$, y elegidos $x_i \in H_i \setminus H_{i+1}$, entonces la cantidad de x_i's de altura j es precisamente e_j (por ser la cantidad de H_i's con $G_j \geq H_i > G_{j+1}$).

(I) Sea $\eta(a_1, \ldots, a_n) = (x_1 - 1)^{a_1}(x_2 - 1)^{a_2} \ldots (x_n - 1)^{a_n}$ un elemento de la base de $K[G]$ dada en el Lema 3.2.3. Entonces el mayor peso posible de η se da cuando todos los $a_i = p - 1$, y en tal caso

$$w(\eta) = (p-1)\sum_{i=1}^{n} \nu(x_i) = (p-1)\sum_{t=1}^{d} te_t = m,$$

porque por nuestra observación inicial la cantidad de $x_i's$ con altura t es exactamente e_t. Entonces $E_m \neq 0$, pues por el Lema 3.2.5 $\eta(p-1, p-1, \ldots, p-1) \in E_m$. El mismo lema da que $E_{m+1} = 0$, pues no hay elementos de altura mayor que m.

(II) De nuevo por el Lema 3.2.5, es claro que f_t es precisamente el número de η's de peso t (que son los elementos de una base de E_t/E_{t+1}). Ahora, el peso de $\eta(a_1, \ldots, a_n)$ es

$$w(\eta) = a_1\nu(x_1) + a_2\nu(x_2) + \cdots + a_n\nu(x_n),$$

de modo que f_t es el número de formas de escoger $0 \leq a_i \leq p - 1$ de tal forma que $w(\eta) = t$. Por otro lado, es evidente que para cada $i = 1, \ldots, d$ hay exactamente e_i elementos de $\{x_1, x_2, \ldots, x_n\}$ con altura i, de modo que

$$\prod_{i=1}^{d} \Phi_p(\zeta^i)^{e_i} = \prod_{j=1}^{n} \Phi_p(\zeta^{\nu(x_j)}) = \prod_{i=1}^{n} \left(1 + \zeta^{\nu(x_i)} + \zeta^{2\nu(x_i)} + \cdots + \zeta^{(p-1)\nu(x_i)}\right).$$

Así, se ve que en el desarrollo del último producto aparecen tantos sumandos de la forma ζ^t como formas posibles hay escoger $0 \leq a_i \leq p - 1$ de forma que

$$\zeta^{a_1\nu(x_1)+a_2\nu(x_2)+\cdots+a_n\nu(x_n)} = \zeta^t,$$

i.e., hay f_t de ellos. Como esto ocurre para cada t, queda demostrado que

$$\sum_{t=0} f_t \zeta^t = \prod_{i=1}^{d} \Phi_p(\zeta^i)^{e_i}.$$

(III) Una implicación es trivial: si $x \in G_t$, entonces $\nu(x) \geq t$, así que $x-1 \in E_t$ por definición de E_t. Recíprocamente, sea $x \in G$ tal que $x \notin G_t$. Entonces $\nu(x) < t$. Sea también $\{H_s\}_{s\geq 1}$ una serie de composición, refinamiento de $\{G_i\}_{i\geq 1}$. Por ser $x \neq 1$, existe un $j \geq 1$ tal que $x \in H_j \setminus H_{j+1}$, y a la hora de escoger un generador $x_j \in H_j/H_{j+1}$ como en el Lema 3.2.3, siempre podemos forzar $x_j = x$. Entonces tenemos un elemento de la base $\eta = x_j - 1 = x - 1$ con peso $w(\eta) = \nu(x) < t$. Por tanto, como el Lema 3.2.5 los η's con $w(\eta) \geq t$ forman una base de E_t, y por el Lema 3.2.3 todos los η's forman una base de $K[G]$, ha de ser $\eta \notin E_t$. Por tanto, $x - 1 \notin E_t$, y el teorema queda probado.

□

Subgrupos de dimensión

Estudiaremos en esta subsección la filtración graduada natural del ideal de aumento, es decir, la dada por las potencias de $\mathrm{Aug}_K(G)$, junto con la N-serie asociada a ella, la de los llamados *subgrupos de dimensión*:

Definición 3.2.7. Sea G un grupo, y K un cuerpo. Para cada $n \geq 1$, se define el *n-ésimo subgrupo de dimensión de G sobre K* como:

$$D_{K,n}(G) = \{x \in G \ : \ x - 1 \in \mathrm{Aug}_K(G)^n\}.$$

Observación 3.2.8. Se hace evidente, a la luz de la Proposición 3.2.2, y dado que por definición $D_{K,n}(G) = G \cap (1 + \mathrm{Aug}_K(G)^n)$, que la sucesión $\{D_{K,n}(G)\}_{n\geq 1}$ es una N-serie; y que, si $\mathrm{char}(K) = p$, además es una N_p serie.

Definición 3.2.9. Sea K un cuerpo con característica p, y G un p-grupo finito. Sea $\{H_s\}_{s\geq 1}$ una serie de composición que sea un refinamiento de la N_p-serie $\{D_{K,t}(G)\}_{t\geq 1}$. Llamamos *base de Jennings* a cualquier base de Jennings generalizada obtenida a partir de esta serie de composición.

Dado G un grupo, consideremos el orden en el conjunto de todas las N_p-series de G determinado por, dadas dos N_p-series $\{G_i\}_{i\geq 1}$, $\{Hi\}_{i\geq 1}$ de G:

$$\{G_i\}_{i\geq 1} \geq \{H_i\}_{i\geq 1} \qquad \text{si y solo si} \qquad G_i \supseteq H_i \text{ para cada } i \geq 1.$$

Teorema 3.2.10 (Jennings)**.** *Sea K un cuerpo con característica p, y G un p-grupo finito. Entonces la serie $\{D_{K,t}(G)\}_{t\geq 1}$ de subgrupos de dimensión es la mínima N_p-serie de G, respecto al orden $\leq$ dado arriba. Además, la filtración de $\mathrm{Aug}_K(G)$ determinada por $\{D_{K,t}(G)\}_{t\geq 1}$ es precisamente $\{\mathrm{Aug}_K(G)^t\}_{t\geq 1}$, las potencias del ideal de aumento.*

Demostración. Por la Observación 3.2.8 $\{D_{K,t}\}_{t\geq 1}$ es una N_p-serie. Además, por el Lema 3.1.6 $\mathrm{Aug}_K(G)$ es nilpotente, por lo que para cierto entero d se tiene que $\mathrm{Aug}_K(G)^{d+1} = (0)$, y por tanto $D_{K,d+1}(G) = \langle 1 \rangle$.

Consideremos una N_p-serie de G cualquiera $\{\tilde{G}_t\}_{t\geq 1}$. Poniendo $G_t = \tilde{G}_t \cap D_{K,t}(G)$ para cada t, es inmediato comprobar que $\{G_t\}_{t\geq 1}$ es una N_p-serie, que además es menor o igual que $\{D_{K,t}(G)\}_{t\geq 1}$ en el orden dado arriba. Sea $\{E_t\}_{t\geq 1}$ la filtración de $\mathrm{Aug}_K(G)$ determinada por $\{G_t\}_{t\geq 1}$. Fijemos un entero $t \geq 1$ cualquiera. Por ser $\mathrm{Aug}_K(G) = E_1$ y la filtración graduada se tiene que:

$$\mathrm{Aug}_K(G)^t = (E_1)^t \subseteq E_t.$$

Por otro lado, sea

$$(g_1 - 1)(g_2 - 1)\dots(g_k - 1)$$

un elemento cualquiera de entre los que por definición generan E_t; entonces verifica

$$\nu(g_1) + \nu(g_2) + \dots + \nu(g_k) \geq t.$$

Por tanto, para cada i, vale $g_i \in G_{\nu(g_i)} \subseteq D_{K,\nu(g_i)}(G)$, de modo que $g_i - 1 \in \mathrm{Aug}_K(G)^{\nu(g_i)}$. En consecuencia,

$$(g_1 - 1)(g_2 - 1)\dots(g_k - 1) \in \mathrm{Aug}_K(G)^{\nu(g_1)+\nu(g_2)+\dots+\nu(g_k)} \subseteq \mathrm{Aug}_K(G)^t.$$

Esto prueba que $E_t \subseteq \mathrm{Aug}_K(G)^t$, y por tanto también la igualdad. Ahora, por el apartado (III) del Teorema 3.2.6 sabemos que

$$G_t = \{x \in G \ : \ x - 1 \in E_t\},$$

mientras que por definición

$$D_{K,t}(G) = \{x \in G \ : \ x - 1 \in \mathrm{Aug}_K(G)^t\};$$

se sigue entonces que $G_t = D_{K,t}(G)$, y por tanto que $D_{K,t}(G) \leq \tilde{G}_t$. Como esto es válido para cada t, el primer resultado queda probado. Además, por lo que acabamos de ver $\{\mathrm{Aug}_K(G)^t\}_{t\geq 1} = \{E_t\}_{t\geq 1}$ es la filtración graduada determinada por la serie $\{G_t\}_{t\geq 1} = \{D_{K,t}(G)\}_{t\geq 1}$, lo que da la afirmación restante.

□

En definitiva, el teorema anterior, por un lado, da una caracterización estrictamente dentro de la Teoría de Grupos los subgrupos de dimensión (como la mínima N_p-serie), mientras que por otro nos permite aplicar el Teorema 3.2.6 a la filtración de las potencias del ideal de aumento.

Lema 3.2.11. Sea K un cuerpo arbitrario, y G un grupo finito. Sean H, N subgrupos de G, con $N \lhd G$. Entonces para cada entero n se tiene que $\mathrm{Aug}_K(H)^n \subseteq \mathrm{Aug}_K(G)^n$, y $D_{K,n}(H) \subseteq D_{K,n}(G)$. Además,

$$\rho_N(\mathrm{Aug}_K(G)^n) = \mathrm{Aug}_K(G/N)^n. \tag{3.3}$$

Finalmente, si $N \subseteq D_{K,n}(G)$, entonces $D_{K,n}(G/N) = D_{K,n}(G)/N$.

Demostración. Como la inclusión $\mathrm{Aug}_K(H) \subseteq \mathrm{Aug}_K(G)$ es inmediata, se deduce que $\mathrm{Aug}_K(H)^n \subseteq \mathrm{Aug}_K(G)^n$, y por tanto también que $D_{K,n}(H) \subseteq D_{K,n}(G)$.

Además, como $\mathrm{Aug}_K(G)$ está generado por los elementos de la forma $g-1$ con $g \in G$, sabemos que $\mathrm{Aug}_K(G)^n$ está generado por elementos de la forma $(g_1-1)(g_2-1)\dots(g_n-1)$, con los $x_i \in G$. Y la imagen por ρ_N de estos elementos está en $\mathrm{Aug}_K(G/N)^n$ (pues o bien tiene n factores, o es nula); además cada generador de $\mathrm{Aug}_K(G/N)^n$ es imagen de uno de ellos, por lo que se da la igualdad $\rho_N(\mathrm{Aug}_K(G)^n) = \mathrm{Aug}_K(G/N)^n$.

Finalmente, supongamos que $N \subseteq D_{K,n}(G)$. Entonces $x \in N$ implica que $x \in D_{K,n}(G)$, y por tanto que $x - 1 \in \mathrm{Aug}_K(G)^n$. En consecuencia, tenemos que

$$\mathrm{Aug}_K(G, N) = \mathrm{Ker}(\rho_N) \subseteq \mathrm{Aug}_K(G)^n; \tag{3.4}$$

se sigue entonces que para cada $g \in G$ se tiene la equivalencia:

$$g - 1 \in \mathrm{Aug}_K(G)^n \qquad \text{si y sólo si} \qquad \rho_N(g-1) \in \mathrm{Aug}_K(G/N)^n$$

(en efecto, la implicación hacia la derecha se sigue directamente de (3.3), mientras que para la recíproca basta notar que si $\rho_N(g-1) \in \mathrm{Aug}_K(G/N)^n$ entonces $\rho_N^{-1}(g-1) = g - 1 + \mathrm{Ker}(\rho_N) \subseteq \mathrm{Aug}_K(G)^n$, lo que por (3.4) da el resultado). Y de esta equivalencia se sigue directamente que $D_{K,n}(G)/N = D_{K,n}(G/N)$. □

El siguiente lema da una relación trivial entre estas series y los subgrupos de dimensión sobre cuerpos de característica p:

Lema 3.2.12. Sea K un cuerpo de característica p, y G un grupo. Entonces para cada entero $n \geq 1$,

$$D_{K,n}(G) \supseteq \mathcal{M}_{p,n}(G) \supseteq \mathcal{L}_{p,n}(G).$$

Demostración. La segunda inclusión viene dada por el Lema 1.3.11. Así, podemos limitarnos a probar la inclusión $D_{K,n}(G) \supseteq \mathcal{M}_{p,n}(G)$; lo haremos por inducción sobre n. El resultado es claro para $n = 1$, pues $D_{K,1}(G) = G$. Supongamos entonces que $n \geq 2$, y que el resultado es cierto para todo subíndice menor que n. Recordemos que, por la Observación 3.2.8, se tiene que $\{D_{K,i}(G)\}_{i\geq 1}$ es una N_p-serie de G. Como por hipótesis de inducción $\mathcal{M}_{p,n-1}(G) \subseteq D_{K,n-1}(G)$, se sigue que

$$(\mathcal{M}_{p,n-1}(G), G) \subseteq (D_{K,n-1}(G), G) \subseteq D_{K,n}(G). \tag{3.5}$$

(donde la última inclusión se tiene porque los subgrupos de dimensión forman una N_p-serie de G).

Además, si i el menor entero tal que $ip \geq n$, entonces $i \leq n-1$ (pues en caso contrario $i \geq n$, y por tanto $(i-1)p \geq (n-1)p \geq (n-1)\cdot 2 \geq n$, contradicción). Entonces, de nuevo por la hipótesis de inducción, $\mathcal{M}_{p,i}(G) \subseteq D_{K,i}(G)$, y en consecuencia

$$\mathcal{M}_{p,i}(G)^{(p)} \subseteq D_{K,i}(G)^{(p)} \subseteq D_{K,n}(G) \tag{3.6}$$

(la última inclusión, de nuevo por formar los subgrupos de dimensión una N_p-serie). Así, de las inclusiones dadas por (3.5) y (3.6) se sigue directamente que

$$\mathcal{M}_{p,n}(G) = (\mathcal{M}_{p,n-1}(G), G)\mathcal{M}_{p,i}(G)^{(p)} \subseteq D_{K,n}(G),$$

y el paso inductivo queda completo.

□

Observación 3.2.13. Notemos que del lema previo y la Proposición 3.1.6 se sigue directamente que la $\mathcal{M}$-serie de Brauer-Jennings-Zassenhaus tiene longitud finita, pues

$$\mathcal{M}_{p,n}(G) - 1 \subseteq D_{K,n}(G) - 1 \subseteq \mathrm{Aug}_K(G)^n = \{0\}$$

para algún entero positivo n.

El siguiente resultado, objetivo de esta sección, resuelve el llamado *Problema de los Subgrupos de Dimensión* en característica p, es decir, permite afirmar que la serie de los subgrupos de dimensión de un grupo G sobre un cuerpo K depende solamente de la característica de K (y del propio G), y que además coincide con la serie de Larzard y con la de Brauer-Jennings-Zassenhaus. Podrá el lector comprobar que, con lo ya probado, la prueba de este hecho en el caso en que G es un p-grupo finito (el único caso que será de relevancia más adelante) es casi trivial; sin embargo, unos pocos cálculos adicionales permiten generalizar el resultado a cualquier grupo:

Teorema 3.2.14 (Jennings-Lazard)**.** *Sea G un grupo, y K un cuerpo de característica p. Entonces se verifican las igualdades:*

$$D_{K,n}(G) = \mathcal{M}_{p,n}(G) = \mathcal{L}_{p,n}(G).$$

Demostración. Por el Lema 3.2.12 sabemos que

$$D_{K,n}(G) \supseteq \mathcal{M}_{p,n}(G) \supseteq \mathcal{L}_{p,n}(G)$$

para cada $n \geq 1$, de modo que será suficiente probar la inclusión $D_{K,n}(G) \subseteq \mathcal{L}_{p,n}$. Fijemos un entero arbitrario $n \geq 1$.

Supongamos primero que G es un p-grupo finito. Entonces, dado que por el Lema 1.3.7 se tiene que $\{\mathcal{L}_{p,n}\}_{n\geq 1}$ es una N_p-serie de G, y que por el Teorema 3.2.10 se sabe que $\{D_{K,i}(G)\}_{i\geq 1}$ es la N_p-serie mínima de G, podemos concluir que $D_{K,n}(G) \subseteq \mathcal{L}_{p,n}(G)$ en este caso.

Supongamos ahora que G es finitamente generado, y escribamos $N = \mathcal{L}_{p,n}(G)$. Entonces, como ya sabemos que $N \subseteq D_{K,n}(G)$, el Lema 3.2.11 garantiza que $D_{K,n}(G/N) = D_{K,n}(G)/N$. Ahora bien, el Lema 1.1.13 junto con el hecho de que $\gamma_n(G) \subseteq N$ dan que $\gamma_n(G/N) = \gamma_n(G)N/N = \langle 1 \rangle$; esto prueba que G/N es nilpotente. Además, por la definición de serie de Lazard, es claro que para j lo suficientemente grande vale $N \supseteq \gamma_1(G)^{(p^j)} = G^{(p^j)}$, por lo que G/N es un p-grupo; es más, tendrá exponente $\leq p^j$, por lo que también ha de ser finito por el Lema 1.1.17, pues es finitamente generado por serlo G. Así, del párrafo anterior aplicado al p-grupo finito G/N se sigue que

$$D_{K,n}(G)/N = D_{K,n}(G/N) = \mathcal{L}_{p,n}(G). \tag{3.7}$$

Sea $ip^j \geq n$. Si consideramos el epimorfismo canónico

$$\pi : \gamma_i(G) \to \gamma_i(G)/N = \gamma_i(G/N),$$

donde la igualdad de nuevo se tiene por el Lema 1.1.13, es claro que la restricción $\pi' : \gamma_i(G)^{(p^j)} \to \gamma_i(G/N)^{(p^j)}$ sigue siendo un epimorfismo. Pero $\gamma_i(G)^{(p^j)} \subseteq \mathcal{L}_{p,n}(G) = N$, de modo que $\langle 1 \rangle = \pi(\gamma_i(G)^{(p^j)}) = \mathrm{Im}(\pi')$; por tanto, necesariamente $\gamma_i(G/N)^{(p^j)} = \langle 1 \rangle$. Así, se deduce que $\mathcal{L}_{n,p}(G/N) = \langle 1 \rangle$, pues cada uno de sus factores es trivial. Esto y la ecuación (3.7) dan que $D_{K,n}(G) = N = \mathcal{L}_{p,n}(G)$, y el resultado queda también probado en este caso.

Finalmente, sea G un grupo arbitrario. Tomemos un $x \in D_{K,n}(G)$ arbitrario. Entonces $x - 1 \in \mathrm{Aug}_K(G)^n$, de modo que podemos escribir $x - 1$ como combinación K-lineal de elementos de la forma:

$$(x-1) = \sum_{s=1}^{m} k_i (x_{s1} - 1)(x_{s2} - 1) \dots (x_{sn} - 1),$$

con $k_i \in K$, $x_{si} \in G$. Entonces existe un subgrupo H de G finitamente generado (por los x_{si} y por x), y con $x \in H$, $x - 1 \in \mathrm{Aug}_K(H)^n$. Por esto último, $x \in D_{K,n}(H)$. Pero H es finitamente generado, de modo que por el caso anterior podemos afirmar que $D_{K,n}(H) = \mathcal{L}_{p,n}(H)$, y por tanto que $x \in \mathcal{L}_{p,n}(H)$. Para cada par i, j con $ip^j \geq n$ se tiene (Lema 1.1.13) que $\gamma_i(H) \subseteq \gamma_i(G)$, y por tanto que $\gamma_i(H)^{(p^j)} \subseteq \gamma_i(G)^{(p^j)}$. En consecuencia, se también se tiene la inclusión entre los productos $\mathcal{L}_{p,n}(H) \subseteq \mathcal{L}_{p,n}(G)$. Esto prueba que $x \in \mathcal{L}_{p,n}(G)$, de donde se deduce la inclusión buscada $D_{K,n}(G) \subseteq \mathcal{L}_{n,p}(G)$. □

3.3. El grupo de unidades normalizadas

Volviendo al estudio del grupo de unidades normalizadas del álgebra de grupo $K[G]$, obtenemos un conjunto generador de este grupo a partir de una base de Jennings dada, y se destacan ciertos subgrupos de dicho grupo. A continuación, se da un resultado relativo a estos grupos de unidades normalizados en álgebras de grupo modulares conmutativas.

Lema 3.3.1. Sea G un p-grupo finito y K un cuerpo de característica p. Entonces hay un isomorfismo de grupos natural:

$$\frac{\mathrm{Aug}_K(G)^n}{\mathrm{Aug}_K(G)^{n+1}} \cong \frac{1 + \mathrm{Aug}_K(G)^n}{1 + \mathrm{Aug}_K(G)^{n+1}},$$

siendo el primero un grupo aditivo, y el segundo multiplicativo.

Demostración. Consideramos la aplicación

$$\lambda : \mathrm{Aug}_K(G)^n \longrightarrow \frac{1 + \mathrm{Aug}_K(G)^n}{1 + \mathrm{Aug}_K(G)^{n+1}}, \qquad \lambda(\alpha) = (1+\alpha)(1 + \mathrm{Aug}_K(G))^{n+1}.$$

Es claro que es un homomorfismo, pues si $\alpha, \beta \in \mathrm{Aug}_K(G)^n$, se tiene que

$$(1+\alpha)(1+\beta) = (1+\alpha+\beta) + \alpha\beta = (1+\alpha+\beta)\left(1 + (1+\alpha+\beta)^{-1}\alpha\beta\right),$$

donde claramente $\alpha\beta \in \mathrm{Aug}_K(G)$, y el inverso existe por el Corolario 3.1.10. Se sigue entonces que $\lambda(\alpha)\lambda(\beta) = \lambda(\alpha+\beta)$. Que es suprayectivo es inmediato. Además, $\alpha \in \mathrm{Ker}(\lambda)$ si y sólo si $1+\alpha \in 1+\mathrm{Aug}_K(G)^{n+1}$, i.e., si y sólo si $\alpha \in \mathrm{Aug}_K(G)^{n+1}$. Queda así probado que $\mathrm{Ker}(\lambda) = \mathrm{Aug}_K(G)^{n+1}$, y por tanto que λ induce un isomorfismo como en el enunciado. □

Tomamos el siguiente lema de [36]:

Lema 3.3.2. Sea G un p-grupo finito y K un cuerpo de característica p. Para cada $n \geq 1$, sea B_n un subconjunto de $\mathrm{Aug}_K(G)^n$ tal que el conjunto imagen por el homomorfismo canónico en el cociente

$$\frac{\mathrm{Aug}_K(G)^n}{\mathrm{Aug}_K(G)^{n+1}}$$

genera dicho cociente como grupo aditivo. Sea $B = \bigcup_{n\geq 1} B_n$. Entonces $1+B$ es un conjunto generador de $V(K[G])$.

Demostración. Considerando el isomorfismo del Lema 3.3.1, como B_n genera $\mathrm{Aug}_K(G)^n$ módulo $\mathrm{Aug}_K(G)^{n+1}$, es claro que $1+B_n$ genera $1+\mathrm{Aug}_K(G)^n$ módulo $1+\mathrm{Aug}_K(G)^{n+1}$ para cada n. Aplicando esta propiedad repetidamente, se deduce fácilmente que $1+\bigcup_{n=1}^{m} B_n$ genera $V(K[G]) = 1+\mathrm{Aug}_K(G)$ módulo $1+\mathrm{Aug}_K(G)^{m+1}$. Como $\mathrm{Aug}_K(G)$ es nilpotente, existirá un entero $m>0$ tal que $1+\mathrm{Aug}_K(G)^{m+1} = \{1\}$, y el resultado se sigue. □

Por tanto:

Corolario 3.3.3. *Sea G un p-grupo finito, K un cuerpo de característica p, y $\mathscr{B}$ una base de de $K[G]$ adaptada a la filtración $\{\mathrm{Aug}_{\mathbb{F}_p}(G)\}_{n\geq 1}$. Entonces el conjunto*

$$1+(\mathscr{B}\setminus\{1\}) = \{1+\eta \ : \ \eta \in \mathscr{B}\setminus\{1\}\}$$

es un conjunto de generadores de $V(K[G])$

Demostración. Por definición los conjuntos $\mathscr{B}_n$ de elementos de la base adaptada de peso n generan $\mathrm{Aug}_K(G)^n$ módulo $\mathrm{Aug}_K(G)^{n+1}$, por lo que $\mathscr{B}\setminus\{1\} = \bigcup_{n\geq 1}\mathscr{B}_n$ está en las condiciones del lema anterior, que da el resultado. □

En particular, obtenemos un conjunto de generadores de $V(K[G])$ a partir de una base de Jennings:

Corolario 3.3.4. *Sea G un p-grupo finito, K un cuerpo de característica p y $\mathscr{B}$ una base de Jennings de $K[G]$. Entonces $1+(\mathscr{B}\setminus\{1\})$ es un conjunto de generadores de $V(K[G])$*

Demostración. Por el Lema 3.2.4 toda base de Jennings es en particular una base adaptada a la filtración de las potencias del ideal de aumento, de modo que basta aplicar el corolario previo. □

Lema 3.3.5. Sea G un p-grupo finito y K un cuerpo de característica p. Supongamos que S es un subespacio multiplicativamente cerrado de $\mathrm{Aug}_K(G)$. Entonces $1+S$ es un subgrupo de $V(K[G])$.

Demostración. Por el Corolario 3.1.10 es claro que $1+S \subseteq V(K[G])$. Además $1+S$ es multiplicativamente cerrado por serlo S; en efecto, si $s,t \in S$, entonces

$$(1+s)(1+t) = 1+(t+s+st) \in 1+S.$$

Finalmente, probamos que es cerrado para inversos. Por el Lema 3.1.6 el ideal de aumento es nilpotente, de modo que existe un $n \geq 1$ tal que, para cada $s \in S$, $s^n = 0$. Tomemos una potencia de p mayor que n, digamos p^m. Entonces

$$(s+1)(s+1)^{p^m-1} = (s+1)^{p^m} = s^{p^m}+1 = 1,$$

pues es claro que los coeficientes que aparecen en el desarrollo del binomio son divisibles por p.

□

Si en el lema anterior S es además un ideal, es claro que el subgrupo $1+S$ será normal en $V(K[G])$. Además:

Lema 3.3.6. Sean G un grupo finito, K un cuerpo, e $I \subseteq \mathrm{Aug}_K(G)$ un ideal de $K[G]$. Entonces hay un isomorfismo de grupos:

$$\frac{V(K[G])}{1+I} \cong V\left(K[G]/I\right).$$

Demostración. Consideremos el homomorfismo de álgebras canónico $\pi : K[G] \to K[G]/I$. Es claro que este epimorfismo, si restringido a $V(K[G])$, determina un epimorfismo

$$\theta : V(K[G]) \longrightarrow V\left(K[G]/I\right).$$

Además, dado $1+\alpha \in V(K[G]) = 1+\mathrm{Aug}_K(G)$, es claro que $1+\alpha \in \mathrm{Ker}(\theta)$ si y sólo si $\theta(1+\alpha)=1$, i.e., si y sólo si $\pi(\alpha)=0$, o equivalentemente, si $\alpha \in \ker(\pi) = I$. □

En particular:

Corolario 3.3.7. *Sea G un p-finito, N un subgrupo de G, y K un cuerpo de característica p. Entonces*

$$\frac{V(K[G])}{1+\mathrm{Aug}_K(G,N)} \cong V(K[G/N]).$$

Demostración. Inmediato a partir del lema anterior, teniendo en cuenta que

$$K[G/N] \cong K[G]/\,\mathrm{Aug}_K(H,N).$$

□

Grupo de unidades normalizadas de un álgebra de grupo modular conmutativa

De un subconjunto B de un grupo abeliano A, decimos que B es una *base* de A si es una base de A como $\mathbb{Z}$-módulo. Si G un p-grupo abeliano, es claro que el álgebra $\mathbb{F}_p[G]$ es conmutativa, por lo que es abeliano el grupo $V(\mathbb{F}_p[G])$. Completamos la sección enunciando el siguiente teorema de R. Sandling, que da una base de este grupo:

Teorema 3.3.8. *Sea G un p-grupo abeliano, y $\{x_1, x_2, \ldots, x_d\}$ una base de G. Consideremos el conjunto*

$$D_0(G) = \{(a_1,\ldots,a_d) \in \mathbb{N}^n \ : \ 0 \le a_i < o(x_i) \text{ para cada } i, \text{ y } p \nmid a_i \text{ para algún } i\}.$$

Si escribimos $\eta(a_1,\ldots,a_d) = \prod_{i=1}^{d}(x_i-1)^{a_i}$, entonces el conjunto

$$\{1+\eta(a_1,\ldots,a_d) \ : \ (a_1,\ldots,a_d) \in D_0(G)\}$$

es una base de $V(\mathbb{F}_p[G])$.

Referencia de la demostración. Ver Teorema 2.5 de [36]. □

3.4. Álgebras de grupo modulares e ideales de Zassenhaus

Completamos el capítulo con el estudio de la estructura de las álgebras de grupo modulares, para lo cual introducimos las *potencias de Lie del ideal aumento*; partir de éstas, definimos los llamados *ideales de Zassenhaus* y encontramos para ellos algunas caracterizaciones más cómodas. Estos últimos cobrarán protagonismo en el Capítulo 4, donde serán esenciales para determinar ciertos invariantes. Además, justificados por la similitud de las técnicas utilizadas en las pruebas, incluimos algunos resultados técnicos sobre potencias de los ideales de aumento, que también desempeñarán su papel en el capítulo próximo.

Potencias de Lie del ideal de aumento

Algunas propiedades de las mencionadas potencias de Lie del ideal aumento siguen siendo válidas en el caso en que K es un cuerpo arbitrario, o al menos un cuerpo de característica p; a ellas dedicamos esta primera subsección.

Definición 3.4.1. Sean G un grupo y K un cuerpo. Se definen las *potencias de Lie del ideal de aumento* como los ideales biláteros $\Lambda_{K,i}(G)$ definidos recursivamente mediante:

(I) $\Lambda_{K,1}(G) = \mathrm{Aug}_K(G)$,

(II) $\Lambda_{K,i+1}(G) = [\mathrm{Aug}_K(G), \Lambda_{K,i}(G)]K[G]$.

Notemos que una inducción sencilla da que $\Lambda_{K,n}(G) \subseteq \mathrm{Aug}_k(G)^n$ para cada n.

Observación 3.4.2. Sean G un grupo, K un cuerpo, y $n \geq 1$ un entero. Se tiene que

$$[\mathrm{Aug}_K(G), \Lambda_{K,n}(G)] + \mathrm{Aug}_K(G)^{n+1} = \Lambda_{K,n+1}(G) + \mathrm{Aug}_K(G)^{n+1}.$$

En efecto, es inmediato que el miembro de la derecha es el menor ideal que contiene al de la izquierda. Por tanto, es suficiente probar que el miembro de la izquierda de la igualdad es un ideal de $K[G]$. Además, como dicho conjunto es la suma de un K-subespacio vectorial y un ideal de $K[G]$, basta probar que es cerrado para el producto por elementos de G. Y en efecto, si $[x, y] \in [\mathrm{Aug}_K(G), \Lambda_{K,n}(G)]$, con $x \in \mathrm{Aug}_K(G)$ e $y \in \Lambda_{K,n}(G)$, entonces, usando que $y \in \mathrm{Aug}_K(G)^n$,

$$\begin{aligned}[x, y]g &= [x, y](g - 1) + [x, y] = (xy - yx)(g - 1) + [x, y] \\ &= \underbrace{(xy - 1)(g - 1) - (yx - 1)(g - 1)}_{\in \mathrm{Aug}_K(G)^{n+1}} + \underbrace{[x, y]}_{\in [\mathrm{Aug}_K(G), \Lambda_{K,n}(G)]}.\end{aligned}$$

Lema 3.4.3. Sean G un grupo, K un cuerpo de característica p, y $n \geq 1$ un entero. Entonces

$$\Lambda_{K,n}(G) + \mathrm{Aug}_K(G)^{n+1} = \mathrm{Aug}_K\left(G, \gamma_n(G)\right) + \mathrm{Aug}_K(G)^{n+1}.$$

Demostración. Procedemos por inducción sobre n. Para $n = 1$ el resultado es trivial, pues ambos lados de la igualdad son $\mathrm{Aug}_K(G)$. Supongamos la igualdad cierta para n.

Para ver la inclusión hacia la derecha, por la Observación 3.4.2 basta probar que todos los elementos de la forma $[x, y]$, con $x \in \mathrm{Aug}_K(G)$ e $y \in \Lambda_{K,n}(G)$, están en $\mathrm{Aug}_K(\gamma_{n+1}(G)) + \mathrm{Aug}_K(G)^{n+2}$. Sea $[x, y]$ un elemento tal. Entonces por la hipótesis de inducción $y = y_1 + y_2$, con $y_1 \in \mathrm{Aug}_K\left(\gamma_n(G)\right)$ e $y_2 \in \mathrm{Aug}_K(G)^{n+1}$. Por tanto, como $[x, y_2] \in \mathrm{Aug}_K(G)^{n+2}$, vale

$$[x, y] = [x, y_1 + y_2] = [x, y_1] + [x, y_2] \equiv [x, y_1] \mod \mathrm{Aug}_K(G)^{n+2}$$

(escribiendo $y_1 = \sum_{g \in \gamma_n(G)} a_g(g - 1)$, con los $a_g \in K$)

$$\equiv \sum_{g \in \gamma_i(G)} a_g[x, g - 1] \mod \mathrm{Aug}_K(G)^{n+2}$$

(escribiendo ahora $x = \sum_{h \in G} b_h(h - 1)$, con los $b_h \in K$)

$$\begin{aligned}&\equiv \sum_{\substack{g \in \gamma_n(G) \\ h \in G}} a_g b_h[h - 1, g - 1] \mod \mathrm{Aug}_K(G)^{n+2} \\ &\equiv \sum_{\substack{g \in \gamma_n(G) \\ h \in G}} a_g b_h((h - 1)(g - 1) - (g - 1)(h - 1)) \mod \mathrm{Aug}_K(G)^{n+2} \\ &\equiv \sum_{\substack{g \in \gamma_n(G) \\ h \in G}} a_g b_h hg(1 - g^{-1}h^{-1}gh) \mod \mathrm{Aug}_K(G)^{n+2}.\end{aligned}$$

Esto, junto con el hecho de que $1 - g^{-1}h^{-1}gh \in \mathrm{Aug}_K(G, \gamma_{n+1}(G))$ (pues $g^{-1}h^{-1}gh = (g,h) \in (\gamma_n(G), G) \subseteq \gamma_{n+1}(G)$), prueba la inclusión

$$\Lambda_{K,n+1}(G) + \mathrm{Aug}_K(G)^{n+2} \subseteq \mathrm{Aug}_K(G, \gamma_{n+1}(G)) + \mathrm{Aug}_K(G)^{n+2}.$$

Para ver la inclusión opuesta recordemos que por el Lema 2.2.5 $\mathrm{Aug}_K(F, \gamma_{n+1}(G))$ está generado como ideal por la derecha de $K[G]$ por los elementos de la forma $g-1$, con $g = (g_1, z)$, para $g_1 \in \gamma_n(G)$ y $z \in G$; por tanto, basta comprobar que estos elementos pertenecen a $\Lambda_{K,n}(G) + \mathrm{Aug}_K(G)^{n+1}$. En efecto, para un elemento $g-1$ tal tenemos que

$$\begin{aligned} g - 1 &= zg_1z^{-1}g_1^{-1} - 1 = (zg_1 - g_1z)z^{-1}g_1^{-1} \\ &= (zg_1 - g_1z)(z^{-1}g_1^{-1} - 1) + (zg_1 - g_1z) \end{aligned}$$

(teniendo en cuenta que $(zg_1 - g_1z) = ((g_1^{-1}, z^{-1})^{-1} - 1)g_1z$ y, dado que $\gamma_{n+1}(G) \subseteq \mathcal{M}_{p,n+1}(G)$, este elemento esta en $\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$)

$$\equiv zg_1 - g_1z \mod \mathrm{Aug}_K(G)^{n+2}$$

(usando la identidad $zg_1 - 1 = (z-1) + (g_1 - 1) + (g_1 - 1)(z-1)$, y la análoga para $g_1z - 1$)

$$\equiv [z-1, g_1 - 1] \mod \mathrm{Aug}_K(G)^{n+2}$$

(como $g_1 \in \gamma_n(G)$, se tiene que $g_1 - 1 \in \mathrm{Aug}_K(G, \gamma_n(G))$, y por la hipótesis de inducción se puede expresar como $g_1 - 1 = \alpha_1 + \alpha_2$, con $\alpha_1 \in \Lambda_{K,i}(G)$ y $\alpha_2 \in \mathrm{Aug}_K(G)^{n+1}$)

$$\equiv [z-1, \alpha_1 + \alpha_2] \mod \mathrm{Aug}_K(G)^{m+2}$$

(por ser $[z-1, \alpha_2] = (z-1)\alpha_2 - \alpha_2(z-1) \in \mathrm{Aug}_K(G)^{n+2}$)

$$\equiv [z-1, \alpha_1] \mod \mathrm{Aug}_K(G)^{n+2}.$$

Notando ahora que $[z-1, \alpha_1] \in \Lambda_{K,n+1}(G)$, queda probada la inclusión

$$\mathrm{Aug}_K(G, \gamma_{n+1}(G)) + \mathrm{Aug}_K(G)^{n+2} \subseteq \Lambda_{K,n+1}(G) + \mathrm{Aug}_K(G)^{n+2},$$

y por ende también el lema. □

Podemos afinar un poco más esta última caracterización de las potencias de Lie del ideal de aumento; para ello, es suficiente notar que:

Observación 3.4.4. Sean G un grupo, K un cuerpo de característica p, y $n \geq 1$ un entero. Sea también N un subgrupo normal de G tal que $N \subseteq \mathcal{M}_{p,n}(G)$. Entonces

$$\mathrm{Aug}_K(N) + \mathrm{Aug}_K(G)^{n+1} = \mathrm{Aug}_K(G, N) + \mathrm{Aug}_K(G)^{n+1}.$$

Para verlo usamos un razonamiento análogo al de la última observación, es decir, basta probar que el miembro de la izquierda es un ideal de $K[G]$. Para ver esto, por K linealidad basta ver que si $h \in N$ y $g \in G$, entonces $(h-1)g \in \mathrm{Aug}_K(N) + \mathrm{Aug}_K(G)^{n+1}$. Y esto es cierto, pues

$$(h-1)g = (h-1)(g-1) + h - 1 \in \mathrm{Aug}_K(G)^{n+1} + \mathrm{Aug}_K(N),$$

pues como $h \in N \subseteq \mathcal{M}_{n,p}(G)$, se tiene que $h - 1 \in \mathrm{Aug}_K(G)^n$.

Concatenando esta observación (para $N = \gamma_n(G)$) con el último lema, se obtiene la siguiente caracterización:

Corolario 3.4.5. *Sea G un grupo, K un cuerpo de característica p, y $n \geq 1$ un entero. Entonces*

$$\Lambda_{K,n}(G) + \mathrm{Aug}_K(G)^{n+1} = \mathrm{Aug}_K(G, \gamma_n(G)) + \mathrm{Aug}_K(G)^{n+1} = \mathrm{Aug}_K(\gamma_n(G)) + \mathrm{Aug}_K(G)^{n+1}.$$

Este resultado es cierto para álgebras de grupo sobre cuerpos arbitrarios (e incluso para anillos conmutativos con unidad), pero para probarlo sería necesario obtener caracterizaciones de los subgrupos de dimensión en casos más generales, cuestión que se escapa a nuestros objetivos (un estudio detallado del tema se puede encontrar en el Capítulo 3 de [39]).

De hecho, en este trabajo sólo nos ocuparemos de estas potencias de Lie del ideal de aumento cuando son considerados en un álgebra de grupo modular $\mathbb{F}_p[G]$ (donde, recordamos, $\mathbb{F}_p$ denota al cuerpo de p elementos), y en esta situación nos sirven para definir los ideales de Zassenhaus, que, como decíamos, serán fundamentales a la hora de probar que ciertos cocientes de los términos de la $\mathcal{M}$-serie de Brauer-Jennings-Zassenhaus están determinados por $\mathbb{F}_p[G]$.

Potencias de los ideales de aumento y sus cocientes

Antes de entrar en el estudio de estos ideales de Zassenhaus será útil, de cara al Capítulo 4, manejar ciertas caracterizaciones de algunos ideales de $\mathbb{F}_p[G]$ obtenidos a partir del ideal de aumento, que basamos en resultados de [39]. Sobre el siguiente lema aritmético se apoyarán gran parte de los resultados en lo que resta de capítulo:

Lema 3.4.6. Sean G un grupo y $n \geq 1$ un entero. Sean también N un subgrupo normal de G, y $\sum_{h\in N} a_h(h-1) \in \mathrm{Aug}_{\mathbb{F}_p}(N)$, con $a_h \in \mathbb{F}_p$. Identificando $\mathbb{F}_p$ con $\mathbb{Z}/p\mathbb{Z}$, denotamos por n_h al entero $0 \leq n_h < p$ que representa a a_h, para cada h. Entonces:

(I) Se tiene la equivalencia

$$\sum_{h\in N} a_h(h-1) \equiv \left(\prod_{h\in N} h^{n_h}\right) - 1 \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(N)^2.$$

(II) Si además $N \subseteq \mathcal{M}_{p,n}(G)$, se tiene que

$$\sum_{h\in N} a_h(h-1) \equiv \left(\prod_{h\in N} h^{n_h}\right) - 1 \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^{2n}.$$

(III) En particular, si $N \subseteq \mathcal{M}_{p,n}(G)$, vale

$$\sum_{h\in N} a_h(h-1) \equiv \left(\prod_{h\in N} h^{n_h}\right) - 1 \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}.$$

En consecuencia, para cada grupo normal N vale

$$\mathrm{Aug}_{\mathbb{F}_p}(N) + \mathrm{Aug}_{\mathbb{F}_p}(N)^2 \;=\; N - 1 + \mathrm{Aug}_{\mathbb{F}_p}(N)^2,$$

y si además $N \subseteq \mathcal{M}_{p,n}(G)$, se verifican las igualdades:

$$\begin{aligned} \mathrm{Aug}_{\mathbb{F}_p}(N) + \mathrm{Aug}_{\mathbb{F}_p}(G)^{2n} &= N - 1 + \mathrm{Aug}_{\mathbb{F}_p}(G)^{2n}, \\ \mathrm{Aug}_{\mathbb{F}_p}(N) + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1} &= N - 1 + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}. \end{aligned}$$

Demostración.

(I) Lo probamos por inducción sobre el número $m = \sum_{g\in G} n_g$ (que siempre será finito, pues los n_g son finitos, y sólo una cantidad finita de ellos es distinta de 0; así, el producto de arriba también es finito). Si $m = 1$, el resultado es inmediato, y si $m = 2$, se sigue directamente de la identidad

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

pues como $g, h \in N$ vale $(g-1), (h-1) \in \mathrm{Aug}_{\mathbb{F}_p}(N)$, y por tanto $(g-1)(h-1) \in \mathrm{Aug}_{\mathbb{F}_p}(N)^2$

Sea ahora $m \geq 3$, y asumamos la afirmación cierta para cualquier suma menor que $m-1$; fijemos un $h \in G$ con $n_h \neq 0$. Entonces escribiendo $n'_h = n_h - 1$, y $n'_g = n_g$ para cada $g \neq h$ se tiene que

$$\sum_{g \in N} n_g(g-1) = (h-1) + \sum_{g \in N} n'_g(g-1);$$

pero entonces la suma $\sum_{g \in N} n'_g = m-1$, de modo que por la hipótesis de inducción

$$\sum_{g \in N} n_g(g-1) \equiv (h-1) + \left(\prod_{g \in N} g^{n'_g} \right) - 1 \mod \operatorname{Aug}_{\mathbb{F}_p}(N)^2;$$

usando ahora caso $m = 2$, la expresión anterior continúa con:

$$\equiv \left(\prod_{g \in G} g^{n'_g} \right) h - 1 \mod \operatorname{Aug}_{\mathbb{F}_p}(G)^{2n} = \left(\prod_{g \in G} g^{n_g} \right) - 1 \mod \operatorname{Aug}_{\mathbb{F}_p}(G)^2,$$

lo que completa el paso inductivo.

(II) Basta repetir *mutatis mutandis* el argumento anterior, observando que en el caso $m = 2$,

$$g, h \in N \subseteq \mathcal{M}_{p,n}(G) \quad \Rightarrow \quad (g-1)(h-1) \in \operatorname{Aug}_{\mathbb{F}_p}(G)^{2n}.$$

(III) Se obtiene directamente del punto previo notando que $\operatorname{Aug}_{\mathbb{F}_p}(G)^{2n} \subseteq \operatorname{Aug}_{\mathbb{F}_p}(G)^{n+1}$.

Cada punto prueba la inclusión hacia la derecha de una de las igualdades, siendo las recíprocas triviales. □

Más adelante necesitaremos de los dos resultados siguientes, referentes ciertas propiedades de los ideales de aumento del álgebra de grupo modular $\mathbb{F}_p[G]$.

Proposición 3.4.7. Sea G un grupo, y N un subgrupo normal de G. Entonces:

(I) $\operatorname{Aug}_{\mathbb{F}_p}(G,N) + \operatorname{Aug}_{\mathbb{F}_p}(G) \operatorname{Aug}_{\mathbb{F}_p}(G,N) = N - 1 + \operatorname{Aug}_{\mathbb{F}_p}(G) \operatorname{Aug}_{\mathbb{F}_p}(G,N)$;
$\operatorname{Aug}_{\mathbb{F}_p}(G,N) + \operatorname{Aug}_{\mathbb{F}_p}(G,N) \operatorname{Aug}_{\mathbb{F}_p}(G) = N - 1 + \operatorname{Aug}_{\mathbb{F}_p}(G,N) \operatorname{Aug}_{\mathbb{F}_p}(N)$.

(II) $1 + \operatorname{Aug}_{\mathbb{F}_p}(G,N) = N(1 + \operatorname{Aug}_{\mathbb{F}_p}(G) \operatorname{Aug}_{\mathbb{F}_p}(N))$.

(III) $1 + \operatorname{Aug}_{\mathbb{F}_p}(G) \operatorname{Aug}_{\mathbb{F}_p}(N) + \operatorname{Aug}_{\mathbb{F}_p}(N) \operatorname{Aug}_{\mathbb{F}_p}(G) = (N,G)N^{(p)}(1 + \operatorname{Aug}_{\mathbb{F}_p}(G) \operatorname{Aug}_{\mathbb{F}_p}(N))$.

(IV) Además,

$$N \cap (1 + \operatorname{Aug}_{\mathbb{F}_p}(G) \operatorname{Aug}_{\mathbb{F}_p}(N)) = \mathcal{M}_{p,2}(N).$$
$$G \cap (1 + \operatorname{Aug}_{\mathbb{F}_p}(G) \operatorname{Aug}_{\mathbb{F}_p}(N)) = \mathcal{M}_{p,2}(N).$$
$$G \cap (1 + \operatorname{Aug}_{\mathbb{F}_p}(G) \operatorname{Aug}_{\mathbb{F}_p}(N) + \operatorname{Aug}_{\mathbb{F}_p}(N) \operatorname{Aug}_{\mathbb{F}_p}(G)) = (N,G)N^{(p)}.$$

Demostración.

(I) La inclusión hacia la izquierda es trivial en ambas igualdades, pues $N - 1 \subseteq \operatorname{Aug}_{\mathbb{F}_p}(G,N)$. Para ver la opuesta en el primer caso, tomemos un elemento cualquiera $\sum_{h \in N} \alpha_h(h-1) \in \operatorname{Aug}_{\mathbb{F}_p}(G,N)$, con $\alpha_h \in K[G]$. Dados $h \in N$ y $g \in G$, por la igualdad $g(h-1) = (h-1) + (g-1)(h-1)$ tenemos que

$$g(h-1) \equiv h - 1 \mod \operatorname{Aug}_{\mathbb{F}_p}(G) \operatorname{Aug}_{\mathbb{F}_p}(G,N);$$

y de esto se sigue directamente que

$$\sum_{h \in N} \alpha_h(h-1) \equiv \sum_{h \in N} \varepsilon(\alpha_h)(h-1) \mod \operatorname{Aug}_{\mathbb{F}_p}(G) \operatorname{Aug}_{\mathbb{F}_p}(G,N).$$

Utilizando el Lema 3.4.6, e identificando como en aquel $\varepsilon(\alpha_h)$ con su correspondiente entero n_h, obtenemos que

$$\sum_{h\in N}\varepsilon(\alpha_h)(h-1)\equiv\left(\prod_{h\in N}h^{n_h}\right)-1 \quad \text{mód } \operatorname{Aug}_{\mathbb{F}_p}(N)^2$$

Finalmente, notando que $\operatorname{Aug}_{\mathbb{F}_p}(N)^2\subseteq\operatorname{Aug}_{\mathbb{F}_p}(G)\operatorname{Aug}_{\mathbb{F}_p}(G,N)$ y que $\prod_{h\in N}h^{n_h}-1\in N-1$, el resultado se sigue. La inclusión restante de la segunda igualdad se prueba análogamente.

(II) La inclusión hacia la derecha se sigue del apartado anterior teniendo en cuenta la igualdad trivial $\operatorname{Aug}_{\mathbb{F}_p}(G)\operatorname{Aug}_{\mathbb{F}_p}(G,N)=\operatorname{Aug}_{\mathbb{F}_p}(G)\operatorname{Aug}_{\mathbb{F}_p}(N)$. En efecto, por dicho apartado se tiene que cada elemento de $\operatorname{Aug}_{\mathbb{F}_p}(G,N)$ es de la forma $n-1+\alpha$, con $\alpha\in\operatorname{Aug}_{\mathbb{F}_p}(G)\operatorname{Aug}_{\mathbb{F}_p}(N)$. Y entonces

$$1+n-1+\alpha=n+\alpha=n(1+n^{-1}\alpha)\in N(1+\operatorname{Aug}_{\mathbb{F}_p}(G)\operatorname{Aug}_{\mathbb{F}_p}(N)).$$

Recíprocamente, dado un elemento de la forma $n(1+\alpha)$, con $\alpha\in\operatorname{Aug}_{\mathbb{F}_p}(G,N)$ basta notar que

$$n(1+\alpha)=1+\underbrace{\alpha+(n-1)(1+\alpha)}_{\in\operatorname{Aug}_{\mathbb{F}_p}(G,N)}.$$

(III) Veamos primero la inclusión directa. Tomemos un elemento genérico

$$1+\sum_i(g_i-1)(n_i-1)+\sum_j(n_j-1)(g_j-1)\in 1+\operatorname{Aug}_{\mathbb{F}_p}(G)\operatorname{Aug}_{\mathbb{F}_p}(N)+\operatorname{Aug}_{\mathbb{F}_p}(N)\operatorname{Aug}_{\mathbb{F}_p}(G),$$

con los $n_i,n_j\in N$, $g_i,g_j\in G$. Es directo que este elemento se puede reescribir como:

$$1+\underbrace{\sum_i(g_i-1)(n_i-1)+\sum_j(g_j-1)(n_j-1)+\sum_j(g_jn_j-1)((n_j,g_j)-1)}_{\in\operatorname{Aug}_{\mathbb{F}_p}(G)\operatorname{Aug}_{\mathbb{F}_p}(N)}+\sum_j((n_j,g_j)-1)$$

(usando que $(n_j,g_j)\in N$, por el primer punto del Lema 3.4.6, para algún $\beta\in\operatorname{Aug}_{\mathbb{F}_p}(N)^2$)

$$=1+\underbrace{\sum_i(g_i-1)(n_i-1)+\sum_j(g_j-1)(n_j-1)+\sum_j(g_jn_j-1)((n_j,g_j)-1)+\beta}_{\in\operatorname{Aug}_{\mathbb{F}_p}(G)\operatorname{Aug}_{\mathbb{F}_p}(N)}+\prod_j(n_j,g_j)-1$$

$$=\prod_j(n_j,g_j)+\underbrace{\sum_i(g_i-1)(n_i-1)+\sum_j(g_j-1)(n_j-1)+\sum_j(g_jn_j-1)((n_j,g_j)-1)+\beta}_{\in\operatorname{Aug}_{\mathbb{F}_p}(G)\operatorname{Aug}_{\mathbb{F}_p}(N)},$$

y la inclusión se sigue. La recíproca se demuestra de forma similar: tomamos un elemento genérico

$$\prod_j(g_j,n_j)\prod_k n_k^p+\sum_i(g_i-1)(n_i-1)\in(N,G)N^{(p)}(1+\operatorname{Aug}_{\mathbb{F}_p}(G)\operatorname{Aug}_{\mathbb{F}_p}(N)).$$

Como cada $(g_j,n_j)\in N$, podemos usar el primer punto del Lema 3.4.6 para deducir la existencia de un $\beta\in\operatorname{Aug}_{\mathbb{F}_p}(N)^2$ tal que el elemento considerado coincide con

$$1+\sum_j((g_j,n_j)-1)+\sum_k(n_k^p-1)+\beta+\sum_i(g_i-1)(n_i-1),$$

que se puede reescribir como:

$$1+\sum_j((g_j,n_j)-1)+\sum_j(g_j-1)(n_j-1)+\sum_j(g_jn_j-1)((n_j,g_j)-1)+$$
$$\beta+\sum_k(n_k-1)^p+\sum_i(g_i-1)(n_i-1)-\sum_j(g_j-1)(n_j-1)-\sum_j(g_jn_j-1)((n_j,g_j)-1).$$

El resultado se obtiene notando que la primera fila es precisamente $1+\sum_j(n_j-1)(g_j-1)$, y que la segunda pertenece a $\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N)$. Notemos que la misma prueba sigue siendo válida sin el factor $N^{(p)}$.

(IV) Para la primera igualdad, se ve que la inclusión hacia la izquierda es clara, pues si $g\in\mathcal{M}_{p,2}(N)$, entonces $g-1\in\mathrm{Aug}_{\mathbb{F}_p}(N)^2\subseteq\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(G,N)$. Para probar la inclusión recíproca, sea X un transversal de N en G que contenga a 1. Definamos una aplicación $\phi:G\to N$ dada por, para cada $g\in G$, $\eta(g)=h$, siempre y cuando $g=xh$, con $x\in X$, $h\in N$. Esta aplicación puede extenderse a una aplicación lineal $\phi:\mathbb{F}_p[G]\to\mathbb{F}_p[N]$.

Entonces, si $g\in N$ con $g-1\in\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(G,N)$, es inmediato que $g-1$ admite una expresión de la forma

$$g-1=\sum_i a_i(g_i-1)(h_i-1),\quad a_i\in K,\ g_i\in G,\ h_i\in N,$$

de modo que, escribiendo $g_i=x_iy_i$, con $x_i\in X$, $y_i\in N$, y aplicando ϕ:

$$\begin{aligned}g-1=\phi(g-1)&=\phi\left(\sum_i a_i(x_iy_i-1)(h_i-1)\right)\\&=\phi\left(\sum_i a_i(x_iy_ih_i-x_iy_i-h_i+1)\right)\\&=\sum_i a_i(y_ih_i-y_i-h_i+1)\\&=\sum_i a_i(y_i-1)(h_i-1)\in\mathrm{Aug}_{\mathbb{F}_p}(N)^2.\end{aligned}$$

Esto prueba que $g\in\mathcal{M}_{p,2}(N)$, y por tanto también primera igualdad. La segunda se sigue directamente de lo anterior y del hecho de que

$$G\cap(1+\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N))\subseteq G\cap(1+\mathrm{Aug}_{\mathbb{F}_p}(G,N))=N.$$

Pasemos ahora a la tercera. Por el punto (III), la inclusión hacia la izquierda es trivial. Recíprocamente, si $g=h(1+\alpha)$ es un elemento de la intersección, con $h\in(N,G)N^{(p)}$ y $\alpha\in\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N)+\mathrm{Aug}_{\mathbb{F}_p}(N)\,\mathrm{Aug}_{\mathbb{F}_p}(G)$, entonces

$$h^{-1}g-1=\alpha\in\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N)+\mathrm{Aug}_{\mathbb{F}_p}(N)\,\mathrm{Aug}_{\mathbb{F}_p}(G)\subseteq\mathrm{Aug}_{\mathbb{F}_p}(G,N),$$

por lo que $h^{-1}g\in N$, es decir, $g=hn$ para cierto $n\in N$. Y entonces

$$n-1=\alpha\in\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N)+\mathrm{Aug}_{\mathbb{F}_p}(N)\,\mathrm{Aug}_{\mathbb{F}_p}(G);$$

aplicando ahora el mismo argumento de arriba (involucrando la aplicación lineal ϕ) se deduce que $n-1\in\mathrm{Aug}_{\mathbb{F}_p}(N)^2$, i.e., $n\in\mathcal{M}_{p,2}(N)=N'N^{(p)}\subseteq(N,G)N^{(p)}$, y por tanto que $g=hn\in(N,G)N^{(p)}$.

□

Proposición 3.4.8. Sea G un grupo, y N un subgrupo normal de G. Entonces se tienen los isomorfismos de grupos abelianos (entendiendo que los grupos en los cocientes de la izquierda están equipados con la suma):

(I) $$\frac{\mathrm{Aug}_{\mathbb{F}_p}(N)}{\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N)} = \frac{\mathrm{Aug}_{\mathbb{F}_p}(G,N)}{\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(G,N)} \cong \frac{N}{\mathcal{M}_{p,2}(N)},$$

(II) $$\frac{\mathrm{Aug}_{\mathbb{F}_p}(G)}{\mathrm{Aug}_{\mathbb{F}_p}(G)^2} \cong \frac{G}{\mathcal{M}_{p,2}(G)},$$

(III) $$\frac{\mathrm{Aug}_{\mathbb{F}_p}(G,N)}{\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N) + \mathrm{Aug}_{\mathbb{F}_p}(N)\,\mathrm{Aug}_{\mathbb{F}_p}(G)} \cong \frac{N}{(N,G)N^{(p)}}.$$

Además, estos isomorfismos son entre grupos abelianos elementales, y por tanto son también isomorfismos de $\mathbb{F}_p$-espacios vectoriales.

(IV) Además, se tiene el siguiente isomorfismo

$$\frac{1+\mathrm{Aug}_{\mathbb{F}_p}(G,N)}{1+\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N)} \cong \frac{N}{\mathcal{M}_{p,2}(N)},$$

siendo esta vez el grupo de la izquierda el cociente de los respectivos grupos multiplicativos.

Demostración. (I) La igualdad se ve directamente teniendo en cuenta que los denominadores son iguales, y que los numeradores también lo son módulo el denominador (véase la Proposición 3.4.7). Consideremos el homomorfismo $\lambda : N \to \mathrm{Aug}(G,N)/(\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(G,N))$ dado por $n \mapsto n-1+(\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(G,N))$. Que efectivamente es homomorfismo de grupos se sigue de la primera parte del Lema 3.4.6 para dos elementos. Que es suprayectivo es consecuencia directa del apartado (I) de la Proposición 3.4.7, y que es inyectiva de la primera igualdad del apartado (IV) de la misma proposición.

Se concluye notando por ser el grupo $N/\mathcal{M}_{p,2}(N)$ abeliano elemental es también un $\mathbb{F}_p$-espacio vectorial, de modo que el isomorfismo de grupos considerado ciertamente es $\mathbb{F}_p$-lineal.

(II) Es un caso particular del primer punto, poniendo $N = G$.

(III) Consideremos la aplicación natural

$$N \to \frac{\mathrm{Aug}_{\mathbb{F}_p}(G,N)}{\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N) + \mathrm{Aug}_{\mathbb{F}_p}(N)\,\mathrm{Aug}_{\mathbb{F}_p}(G)}$$

dada por $g \mapsto \overline{g-1}$. Que es homomorfismo de grupos se sigue también del Lema 3.4.6. Notando que del punto (I) de la Proposición 3.4.7 se sigue fácilmente que el codominio de este homomorfismo es

$$\frac{N-1+\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N) + \mathrm{Aug}_{\mathbb{F}_p}(N)\,\mathrm{Aug}_{\mathbb{F}_p}(G)}{\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N) + \mathrm{Aug}_{\mathbb{F}_p}(N)\,\mathrm{Aug}_{\mathbb{F}_p}(G)},$$

se hace claro que es un epimorfismo. Además su núcleo es

$$G \cap (1+\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N) + \mathrm{Aug}_{\mathbb{F}_p}(N)\,\mathrm{Aug}_{\mathbb{F}_p}(G)) = (N,G)N^{(p)},$$

donde la igualdad vale por el apartado (IV) de la Proposición 3.4.7. Por tanto, este homomorfismo induce el isomorfismo buscado.

(IV) Análogamente, como por el apartado (II) de la mencionada proposición se tiene la igualdad

$$\frac{1+\mathrm{Aug}_{\mathbb{F}_p}(G,N)}{1+\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N)}=\frac{N(1+\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N))}{1+\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N)},$$

es obvio que la aplicación

$$N\to\frac{N(1+\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N))}{1+\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N)},\qquad n\mapsto n(1+\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N))$$

es un epimorfismo de grupos multiplicativos cuyo núcleo es

$$N\cap(1+\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(N))=\mathcal{M}_{p,2}(N),$$

valiendo la igualdad por el apartado (IV) de la Proposición 3.4.7.

□

Otra aplicación de la Proposición 3.4.7 es el siguiente:

Lema 3.4.9. Sea G un p-grupo finito. Entonces, para cada entero $k\geq 1$ se verifica la igualdad:

$$\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(\gamma_k(G))+\mathrm{Aug}_{\mathbb{F}_p}(\gamma_k(G))\,\mathrm{Aug}_{\mathbb{F}_p}(G)=\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(\gamma_k(G))+\mathrm{Aug}_{\mathbb{F}_p}(G,\gamma_{k+1}(G)).$$

Demostración. Por el apartado (IV) de la Proposición 3.4.7 sabemos que

$$G\cap(1+\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(\gamma_k(G))+\mathrm{Aug}_{\mathbb{F}_p}(\gamma_k(G))\,\mathrm{Aug}_{\mathbb{F}_p}(G))=\gamma_{k+1}(G)\gamma_k(G)^{(p)},$$

en particular

$$\gamma_{k+1}(G)-1\subseteq\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(\gamma_k(G))+\mathrm{Aug}_{\mathbb{F}_p}(\gamma_k(G))\,\mathrm{Aug}_{\mathbb{F}_p}(G)$$

y por tanto

$$\mathrm{Aug}_{\mathbb{F}_p}(\gamma_{k+1}(G))\subseteq\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(\gamma_k(G))+\mathrm{Aug}_{\mathbb{F}_p}(\gamma_k(G))\,\mathrm{Aug}_{\mathbb{F}_p}(G),$$

de donde la inclusión hacia la izquierda se sigue directamente.

Para probar la recíproca basta notar que si $\alpha\in\mathrm{Aug}_{\mathbb{F}_p}(\gamma_k(G))$, $\beta\in\mathrm{Aug}_{\mathbb{F}_p}(G)$, se tiene que

$$\alpha\beta\in\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(\gamma_k(G))+\Big[\mathrm{Aug}_{\mathbb{F}_p}(\gamma_k(G)),\mathrm{Aug}_{\mathbb{F}_p}(G)\Big]$$

(por el Lema 2.2.14)

$$\subseteq\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(\gamma_k(G))+\mathrm{Aug}_{\mathbb{F}_p}(G,\gamma_{k+1}(G)).$$

□

Ideales de Zassenhaus

Introducimos por fin los anunciados ideales de Zassenhaus, y damos siguiendo a [20] unas caracterizaciones de los mismos mucho más manejables que la definición teórica, aunque esta última cuenta con la ventaja de que en su construcción sólo interviene la estructura de $\mathbb{F}_p$-álgebra de $\mathbb{F}_p[G]$, y no el grupo G, de modo que en cierto sentido dichos ideales quedan *determinados* por $\mathbb{F}_p$; esta propiedad será central en el siguiente capítulo, en el que especificaremos con más rigor cuál es este sentido al que nos referimos.

Definición 3.4.10. Sea G un grupo, $\mathbb{F}_p$ el cuerpo de p elementos, y $n \geq 1$ un entero. Se define el n-ésimo *ideal de Zassenhaus* $I_{\mathbb{F}_p,n}(G)$ como

$$I_{\mathbb{F}_p,n}(G) = \sum_{ip^j \geq n} \Lambda_{\mathbb{F}_p,i}(G)^{(p^j)} + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1},$$

donde $\Lambda_{\mathbb{F}_p,i}(G)^{(p^j)}$ es el subgrupo aditivo de $\mathbb{F}_p[G]$ generado por todos los elementos de la forma a^{p^j}, con $a \in \Lambda_{\mathbb{F}_p,i}(G)$.

En primer lugar, notemos que la suma que aparece en la definición es en la práctica una suma finita, pues como el ideal de aumento es nilpotente por la Proposición 3.1.6, si ip^j es lo suficientemente grande, se tiene que $\Lambda_{\mathbb{F}_p,i}(G)^{(p^j)} = \{0\}$. Además, se observa que, como para cada i se tiene que $\Lambda_{\mathbb{F}_p,i}(G) \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^i$, necesariamente $\Lambda_{\mathbb{F}_p,i}(G)^{(p_j)} \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^{ip^j} \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^n$ para $ip^j \geq n$. En consecuencia, para cada $n \geq 1$ tenemos que

$$I_{\mathbb{F}_p,n}(G) \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^n.$$

En segundo lugar, se hace necesario comprobar que esta construcción es efectivamente un ideal: como es inmediato que es un $\mathbb{F}_p$-módulo, basta ver que es cerrado bajo el producto de elementos de G. Sea $\alpha \in I_{\mathbb{F}_p,n}(G)$ y $g \in G$. Por lo anterior $\alpha \in \mathrm{Aug}_{\mathbb{F}_p}(G)^n$, y por tanto es claro que

$$\alpha g = \alpha(g-1) + \alpha \in \mathrm{Aug}_K(G)^{n+1} + I_{\mathbb{F}_p,n}(G) \subseteq I_{\mathbb{F}_p,n}(G).$$

Como una demostración enteramente análoga daría que es también un ideal por la derecha, podemos afirmar que $I_{\mathbb{F}_p,n}(G)$ es un ideal bilátero.

Proposición 3.4.11. Sea G un grupo, $\mathbb{F}_p$ un cuerpo de característica p y $n \geq 1$ un entero. Entonces se tiene que:

$$I_{\mathbb{F}_p,n}(G) = \mathrm{Aug}_{\mathbb{F}_p}(G, \mathcal{M}_{p,n}(G)) + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}.$$

Demostración. Como por definición $\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1} \subseteq I_{\mathbb{F}_p,n}(G)$, para ver la inclusión hacia la izquierda es suficiente comprobar que $I_{\mathbb{F}_p,n}(G) \supseteq \mathrm{Aug}_{\mathbb{F}_p}(G, \mathcal{M}_{p,n}(G))$, y para ello es suficiente ver que los generadores de $\mathrm{Aug}_{\mathbb{F}_p}(G, \mathcal{M}_{p,n}(G))$ como ideal, i.e., que los elementos de la forma $x-1$ con $x \in \mathcal{M}_{p,n}(G)$, están en $I_{\mathbb{F}_p,n}(G)$.

Para probar esto, notemos que un elemento cualquiera $x \in \mathcal{L}_{p,n}(G) = \mathcal{M}_{p,n}(G)$ es de la forma $x = g_{i_1}^{p^{j_1}} g_{i_2}^{p^{j_2}} \dots g_{i_m}^{p^{j_m}}$, siendo $g_{i_k} \in \gamma_{i_k}(G)$ e $i_k p^{j_k} \geq n$. Probaremos que $x - 1 \in I_{\mathbb{F}_p,n}(G)$ por inducción sobre m. Si $m = 1$, del Lema 3.4.3 se sigue fácilmente que

$$g_{i_1} - 1 \equiv \alpha \mod \mathrm{Aug}_{\mathbb{F}_p}(G)^{i_1+1}, \qquad \text{para algún } \alpha \in \Lambda_{\mathbb{F}_p,i_1}(G),$$

por lo que, elevando a p^{j_1} y recordando que $\mathrm{Aug}_{\mathbb{F}_p}(G)^{i_1 p^{j_1} + p^{j_1}} \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$, vale

$$g^{p^{j_1}} - 1 \equiv \alpha^{p^{j_1}} \mod \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1},$$

de modo que $g^{p^j} - 1 \in \Lambda_{\mathbb{F}_p,i}(G)^{(p^j)} + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1} \subseteq I_{\mathbb{F}_p,n}(G)$. Sea ahora $m > 1$; por la hipótesis de inducción sabemos que $g_{i_1}^{p^{j_1}} g_{i_2}^{p^{j_2}} \dots g_{i_{m-1}}^{p^{j_{m-1}}} - 1 \in I_{\mathbb{F}_p,n}(G)$, y por el caso base, $g_{i_m}^{p^{j_m}} - 1 \in I_{\mathbb{F}_p,n}(G)$. Así, y dado que

$$I_{\mathbb{F}_p,n}(G) \ni (g_{i_1}^{p^{j_1}} g_{i_2}^{p^{j_2}} \dots g_{i_{m-1}}^{p^{j_{m-1}}} - 1)(g_{i_m}^{p^{j_m}} - 1) =$$

$$x - 1 - (g_{i_1}^{p^{j_1}} g_{i_2}^{p^{j_2}} \dots g_{i_{m-1}}^{p^{j_{m-1}}} - 1) - (g_{i_m}^{p^{j_m}} - 1),$$

se deduce que $x - 1 \in I_{\mathbb{F}_p,n}(G)$, lo que completa el paso inductivo.

Para ver la inclusión recíproca basta probar que para cada $\alpha \in \Lambda_{\mathbb{F}_p,i}(G)$ con $ip^j \geq n$ se tiene que $\alpha^{p^j} \in \mathrm{Aug}_{\mathbb{F}_p}(G, \mathcal{M}_{p,n}(G)) + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$. En efecto, dado α en estas condiciones, usando de nuevo el Lema 3.4.3 se obtiene que

$$\alpha \in \mathrm{Aug}_{\mathbb{F}_p}(\gamma_i(G)) + \mathrm{Aug}_{\mathbb{F}_p}(G)^{i+1} = \gamma_i(G) - 1 + \mathrm{Aug}_{\mathbb{F}_p}(G)^{i+1},$$

donde la igualdad se tiene en virtud del Lema 3.4.6 (pues $\gamma_i(G) \subseteq \mathcal{M}_{p,i}(G)$). Entonces se tiene que

$$\alpha \equiv (h-1) + z', \qquad \text{con } h \in \gamma_i(G), \text{ y } z' \in \mathrm{Aug}_{\mathbb{F}_p}(G)^{i+1},$$

de modo que elevando a p^j, y recordando de nuevo que $\mathrm{Aug}_{\mathbb{F}_p}(G)^{i_1 p^{j_1} + p^{j_1}} \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$, se tiene que

$$\alpha^{p^j} \equiv (h^{p^j} - 1) \mod \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}.$$

Ahora bien, de $\gamma_i(G) \subseteq \mathcal{M}_{p,i}(G)$ se sigue que

$$\gamma_i(G)^{p^j} \subseteq \mathcal{M}_{p,i}(G)^{p^j} \subseteq \mathcal{M}_{p,ip^j}(G) \subseteq \mathcal{M}_{p,n}(G)$$

(las inclusiones segunda y tercera se tienen por ser la serie p-restringida y descendente, respectivamente) y de esto se deduce que $h^{p^j} \in \mathcal{M}_{p,n}(G)$, y por ende que $h^{p^j} - 1 \in \mathrm{Aug}_{\mathbb{F}_p}(\mathcal{M}_{p,n}(G)) \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G, \mathcal{M}_{p,n}(G))$. En definitiva, esto prueba que $\alpha^{p^j} \in \mathrm{Aug}_{\mathbb{F}_p}(G, \mathcal{M}_{p,n}(G)) + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$.

□

Podemos así reescribir la proposición anterior para obtener la caracterización:

Corolario 3.4.12. *Sea G un grupo, y $n \geq 1$ un entero. Entonces se tiene que:*

$$I_{\mathbb{F}_p,n}(G) = \mathcal{M}_{p,n}(G) - 1 + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}.$$

Demostración. En efecto,

$$I_{\mathbb{F}_p,n}(G) = \mathrm{Aug}_{\mathbb{F}_p}(G, \mathcal{M}_{p,n}(G)) + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1} =$$

$$\mathrm{Aug}_{\mathbb{F}_p}(\mathcal{M}_{p,n}(G)) + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1} = \mathcal{M}_{p,n}(G) - 1 + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1},$$

donde la primera igualdad se tiene por la Proposición 3.4.11, la segunda por la Observación 3.4.4, y la restante por el Lema 3.4.6.

□

Capítulo 4

Invariantes determinados por el álgebra de grupo

En este capítulo generalizamos la noción de *grupo determinado por su álgebra de grupo* que introducíamos en el Capítulo 2 a otros objetos. Posteriormente, dado un p-grupo G, presentaremos algunos invariantes de G que están determinados por el álgebra de grupo $K[G]$ (primero siendo K un cuerpo de característica p cualquiera, más adelante, siendo $K = \mathbb{F}_p$, el cuerpo de p elementos).

Este estudio se realiza con la esperanza de que, en algún momento, se conozcan tantos invariantes del grupo G determinados por su álgebra de grupo que a partir de éstos a su vez uno sea capaz de reconocer la clase de isomorfía de G, lo que daría solución positiva a **(MIP)**. Esta aproximación ha probado su utilidad, habiéndose alcanzado este objetivo cuando se restringe la cuestión a ciertas clases más limitadas de p-grupos finitos, como la de los p-grupos central-elemental-por-abeliano, o la de los p-grupos metacíclicos.

4.1. Objetos determinados por un álgebra de grupo

En esta sección K y G denotarán, respectivamente, un cuerpo y un grupo arbitrarios, que consideraremos fijados.

Definición 4.1.1. Sean K un cuerpo y G un grupo. Para $i = 1, 2$, sea $O_{K,i}$ una regla que a cada grupo H le asigna un objeto $O_{K,i}(H)$ (que será un número, el valor de verdad de una afirmación sobre K y G, una clase de isomorfía, o un subconjunto de $K[G]$[1]). Decimos que el objeto $O_{K,1}(G)$ está *determinado* por el objeto $O_{K,2}(G)$ si para cada grupo H se tiene la implicación:

$$O_{K,2}(G) \equiv O_{K,2}(H) \qquad \Rightarrow \qquad O_{K,1}(G) \equiv O_{K,1}(H),$$

donde:

- Si $O_{K,i}(G)$ es un número, un valor de verdad o una clase de isomorfía, '$\equiv$' denota la igualdad.
- Si $O_{K,i}(G)$ es un subconjunto del álgebra de grupo $K[G]$, '$\equiv$' denota la relación de equivalencia:

$$O_{K,i}(G) \equiv O_{K,i}(H) \qquad \Leftrightarrow \qquad \begin{array}{c} K[G] \cong K[H] \text{ y para cada isomorfismo normalizado} \\ \theta : K[G] \to K[H] \text{ se tiene que } \theta(O_{K,i}(G)) = O_{K,i}(H). \end{array}$$

Es claro que esta definición puede extenderse a familias de objetos de la forma obvia: si $\{O_{K,i}\}_{i\in I}$, $\{\bar{O}_{K,j}\}_{j\in J}$ son familias de reglas de asignación como en la definición anterior, decimos

[1] Entendemos que una misma regla no asigna objetos de distintos tipos, i.e., si $O_{K,i}(G)$ es un número, entonces $O_{K,i}(H)$ es un número para cada grupo H; lo mismo se aplica si $O_{K,i}(G)$ es un valor de verdad, la clase de isomorfía de un grupo, de un álgebra, etc.

que la familia de objetos $\{O_{K,i}(G)\}_{i\in I}$ está determinada por la familia de objetos $\{\bar{O}_{K,j}(G)\}_{j\in J}$ si para cada grupo H se verifica la implicación

$$\bar{O}_{K,j}(G) \equiv \bar{O}_{K,j}(H)\ \forall j \in J \qquad \Rightarrow \qquad O_{K,i}(G) \equiv O_{K,i}(H)\ \forall i \in I.$$

Observación 4.1.2. También es fácil ver que esta noción es transitiva, es decir, si el objeto $O_{K,1}(G)$ está determinada por $O_{K,2}(G)$ y a su vez $O_{K,2}(G)$ está determinada por $O_{K,3}(G)$, entonces $O_{K,1}(G)$ está determinada por $O_{K,3}(G)$.

En la literatura sobre la materia, se suele referir al hecho de que un subconjunto $O_K(G) \subseteq K[G]$ esté determinado por $K[G]$ como que $O_K(G)$ está *determinado canónicamente*, o simplemente que es *canónico* (en el sentido que da Passman en [32]). Normalmente, el objeto $O_{K,2}(G)$ será la clase de isomorfía del álgebra de grupo $K[G]$; si además ponemos la clase de isomorfía del grupo G en el lugar de $O_{K,1}(G)$, la Definición 4.1.1 se convierte en la Definición 2.3.1, lo que justifica la terminología. En ocasiones, si no hay riesgo de confusión, cuando la clase de isomorfía de una estructura algebraica está determinada por cierto objeto fijado simplemente diremos que la estructura en cuestión está determinada.

Ejemplo 4.1.3. Quedan trivialmente determinado por la clase de isomorfía de $K[G]$ (o, equivalentemente, por $K[G]$ como subconjunto de sí mismo) los subconjuntos siguientes: el centro $\mathcal{Z}(K[G])$, el subespacio $[K[G], K[G]]$, y el ideal de Jacobson $JK[G]$.

Observación 4.1.4. También queda determinado por el álgebra de grupo $K[G]$ el grupo de unidades $\mathcal{U}(K[G])$, así como el grupo de unidades normalizadas $V(K[G])$ (entendidos ambos como subconjuntos de $K[G]$). En particular, también las clases de isomorfismo de estos grupos están determinadas. En efecto, cualquier isomorfismo normalizado de $K[G]$ en $K[H]$, si restringido a $\mathcal{U}(K[G])$ (resp. $V(K[G])$), da un isomorfismo de grupos cuya imagen es claramente $\mathcal{U}(K[H])$ (resp. $V(K[H])$).

Además, utilizaremos casi siempre sin indicación el siguiente observación elemental:

Observación 4.1.5. Sean $K[G]$ una K-álgebra de grupo, I, J ideales de $K[G]$ y S, T subespacios vectoriales de $K[G]$, determinados todos por algún objeto $O_K(G)$. Entonces están determinados por $O_K(G)$:

(I) El ideal de $K[G]$ generado por S

(II) La clase de isomorfía del álgebra $K[G]/I$.

(III) Las potencias I^n de I.

(IV) Los ideales suma $I + J$ y producto IJ.

(V) Los subespacios $S + T$ y $S \cap T$.

(VI) El subespacio conmutador $[S, T]$.

A veces convendrá considerar una versión más débil de esta noción de determinación.

Definición 4.1.6. Sea K un cuerpo arbitrario, y $\mathfrak{C}$ cierta clase de grupos. Sea G un grupo en la clase $\mathfrak{C}$, y $O_{K,i}$ una regla que a cada grupo H en $\mathfrak{C}$ le asigna un objeto $O_{K,i}(H)$, para $i = 1, 2$. Entendemos que un objeto $O_{K,1}(G)$ está *determinado en la clase* $\mathfrak{C}$ por otro objeto $O_{K,2}(G)$ si para cualquier otro grupo H en $\mathfrak{C}$, se tiene la implicación:

$$O_{K,2}(G) \equiv O_{K,2}(H) \qquad \Rightarrow \qquad O_{K,1}(G) \equiv O_{K,1}(H),$$

donde '$\equiv$' es la relación dada en la Definición 4.1.1.

Cuando $\mathfrak{C}$ es la clase de todos los grupos, esta noción se restringe a la Definición 4.1.1. Además, es obvio que todas las propiedades anteriores también se aplican a esta nueva definición.

Observación 4.1.7. También conviene notar que si (a): $O_{K,1}(G)$ está determinado por $O_{K,2}(G)$ en la clase $\mathfrak{C}$, y (b): el valor de la afirmación "G está en la clase $\mathfrak{C}$" está determinado por $O_{K,2}(G)$, entonces $O_{K,1}(G)$ está determinado por $O_{K,2}(G)$. En efecto, si H es otro grupo tal que $O_{K,2}(G) \equiv O_{K,2}(H)$, entonces por (b) H es ha de estar en la clase $\mathfrak{C}$, de modo que por (a) $O_{K,1}(G) \equiv O_{K,1}(H)$.

4.2. Invariantes determinados por $K[G]$

A lo largo de esta sección, salvo indicación expresa K denotará a un cuerpo de característica p arbitrario, y G a un p-grupo finito. Podemos en este caso extender la lista de objetos determinados por el álgebra de grupo $K[G]$:

Observación 4.2.1. El ideal de aumento $\mathrm{Aug}_K(G)$ está determinado por $K[G]$. En efecto, por el Lema 3.1.7 sabemos que $\mathrm{Aug}_K(G) = JK[G]$, y este último está obviamente determinado por $K[G]$.

Observación 4.2.2. Es fácil comprobar que las potencias de Lie del ideal de aumento también están determinadas por $K[G]$. En efecto, $\mathrm{Aug}_K(G)$ lo está, y razonando por inducción, si $\Lambda_{K,i}(G)$ está determinado, es inmediato que también lo está $[\mathrm{Aug}_K(G), \Lambda_{K,i}(G)]$, de modo que también $\Lambda_{K,i+1}(G)$ queda determinado por $K[G]$.

Además, podemos seguir extendiendo esta lista teniendo en cuenta las caracterizaciones de los ideales del álgebra de grupo $K[G]$ obtenidas en el siguiente lema:

Lema 4.2.3. Sea G un p-grupo finito, y K un cuerpo de característica p. Se tiene que:

(I) El ideal de $K[G]$ generado por el subespacio $[K[G], K[G]]$ es $\mathrm{Aug}_K(G, G')$.

(II) El ideal de $K[G]$ generado por el subespacio $[K[G], K[G]]$ y por $\mathcal{Z}(K[G]) \cap \mathrm{Aug}_K(G)$ es $\mathrm{Aug}_K(G, \mathcal{Z}(G)G')$.

En consecuencia, los ideales $\mathrm{Aug}_K(G, G')$ y $\mathrm{Aug}_K(G, \mathcal{Z}(G)G')$ están determinadas por $K[G]$.

Demostración.

(I) Por el Lema 2.2.5 $\mathrm{Aug}_K(G, G')$ es el ideal generado por todos los elementos de la forma

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

con $g, h \in G$. Como gh es una unidad, $\mathrm{Aug}_K(G, G')$ es el ideal generado por todos los productos de Lie de elementos de G, o equivalentemente, por el subespacio $[K[G], K[G]]$.

(II) Sea I el ideal de $K[G]$ generado por $[K[G], K[G]]$ y $\mathrm{Aug}_K(G) \cap \mathcal{Z}(K[G])$. Del hecho de que $\mathcal{Z}(G) - 1 \subseteq \mathrm{Aug}_K(G) \cap \mathcal{Z}(K[G])$ y del punto anterior se siguen, respectivamente, las inclusiones

$$\mathrm{Aug}_K(G, \mathcal{Z}(G)) \subseteq I, \qquad \mathrm{Aug}_K(G, G') \subseteq I.$$

Por tanto, para cada elemento de la forma $gh - 1$, con $g \in \mathcal{Z}(G)$ y $h \in G'$ se tiene que

$$gh - 1 = (g - 1)h + (h - 1) \in I,$$

de modo que vale la inclusión

$$\mathrm{Aug}_K(G, \mathcal{Z}(G)G') \subseteq I.$$

Probar la recíproca se reduce a ver que los generadores de I están en $\mathrm{Aug}_k(G, \mathcal{Z}(G)G')$. Para los conmutadores de Lie, se tiene directamente que

$$[K[G], K[G]] \subseteq \mathrm{Aug}_k(G, G') \subseteq \mathrm{Aug}_K(G, \mathcal{Z}(G)G').$$

Sea ahora $\alpha \in \mathrm{Aug}_K(G) \cap \mathcal{Z}(K[G])$; por el Corolario 2.1.9 los coeficientes α son constantes en las clases de conjugación, es decir, α es de la forma

$$\alpha = \sum_{C \in \mathrm{Cl}(G)} a_C \left(\sum_{g \in C} g \right) = \sum_{C \in \mathrm{Cl}(G):\ |C| > 1} a_C \left(\sum_{g \in C} g \right) + \sum_{g \in \mathcal{Z}(G)} a_{\{g\}} g.$$

Fija una clase de conjugación C con $|C| > 1$, escribamos $C = \{g_1, \ldots, g_{|C|}\}$. Es claro que p divide a $|C|$, por lo que $|C| = 0$ en $K[G]$. Escribiendo $g_i = x_i^{-1} g_1 x_i$, con $x_1 = 1$ y $x_i \in G$, se verifica que

$$\sum_{g \in C} g = \sum_{i=1}^{|C|} g_i = \sum_{i=1}^{|C|} x_i^{-1} g_1 x_i = g_1 \sum_{i=1}^{|C|} (g_1, x_i) = g_1 \sum_{i=1}^{|C|} (g_1, x_i) - |C| =$$

$$g_1 \sum_{i=1}^{|C|} ((g_1, x_i) - 1) \in \mathrm{Aug}_K(G, G') \subseteq \mathrm{Aug}_K(G, \mathcal{Z}(G)G').$$

Entonces para probar que $\alpha \in \mathrm{Aug}_K(G, \mathcal{Z}(G)G')$ podemos limitarnos a probar que

$$\sum_{g \in \mathcal{Z}(G)} a_{\{g\}} g \in \mathrm{Aug}_K(G, \mathcal{Z}(G)G').$$

Como lo anterior, en particular, prueba que

$$\sum_{C \in \mathrm{Cl}(G):\ |C|>1} a_C \left(\sum_{g \in C} g \right) \in \mathrm{Aug}_K(G),$$

tendremos que

$$\sum_{g \in \mathcal{Z}(G)} a_{\{g\}} g \in \mathrm{Aug}_K(G) \cap K[\mathcal{Z}(G)] \subseteq \mathrm{Aug}_K(\mathcal{Z}(G)) \subseteq \mathrm{Aug}_K(G, \mathcal{Z}(G)G'),$$

y la inclusión queda probada.

Con esto, la última afirmación se sigue directamente de la Observación 4.1.5.

□

Pasamos en las siguientes subsecciones, como anunciábamos, a utilizar todo el aparato teórico del capítulo anterior para identificar invariantes de G que están determinados por el álgebra de grupo $K[G]$.

El exponente de G

En lo que sigue, dada un álgebra A sobre un cuerpo K, y un entero $n \geq 0$, denotaremos

$$T_n(A) = \{\alpha \in A \ :\ \alpha^{p^n} \in [A, A]\}.$$

Observemos como en [27] que en álgebras de grupo el conjunto anterior admite la siguiente caracterización:

Lema 4.2.4. Sea G un grupo finito, K un cuerpo de característica p, y $n \geq 0$ un entero. Entonces $T_n(K[G])$ es un subespacio vectorial de $K[G]$. Además, se verifica la igualdad:

$$T_n(K[G]) = \left\{ \sum_{g \in G} a_g g \in K[G] \ :\ \sum_{g \in G:\ g^{p^n} \in C} a_g = 0 \text{ para cada } C \in \mathrm{Cl}(G) \right\}.$$

Demostración. Ver que $T_n(K[G])$ es un subespacio vectorial es sencillo, pues lo es $[K[G], K[G]]$. En efecto, dados $\alpha, \beta \in T_n(K[G])$, $a \in K$, se tiene que

$$(a\alpha)^{p^n} = a^{p^n} \alpha^{p^n} \in [K[G], K[G]],$$

y por el Lema 2.1.11 existe un $r \in [K[G], K[G]]$ tal que

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} + r,$$

y claramente la última suma está en $[K[G], K[G]]$.

Probamos ahora la igualdad: por definición un elemento $\alpha = \sum_{g \in G} a_g g \in K[G]$ está en $T_n(K[G])$ si y sólo si $\alpha^{p^n} \in [K[G], K[G]]$. Por el Lema 2.1.11 existe un $\beta \in [K[G], K[G]]$ tal que

$$\alpha^{p^n} = \sum_{g \in G} a_g^{p^n} g^{p^n} + \beta,$$

de modo que podemos continuar la equivalencia anterior con: $\alpha^{p^n} \in [K[G], K[G]]$ si y sólo si $\sum_{g \in G} a_g^{p^n} g^{p^n} \in [K[G], K[G]]$. Y por el segundo apartado del Lema 2.1.12 esto ocurre si y sólo si para cada clase de conjugación C de G se tiene que

$$0 = \sum_{g \in G:\ g^{p^n} \in C} a_g^{p^n} = \left(\sum_{g \in G:\ g^{p^n} \in C} a_g \right)^{p^n}$$

(la segunda igualdad es cierta porque cada $a_g \in K$), y esto es equivalente a que

$$\sum_{g \in G:\ g^{p^n} \in C} a_g = 0.$$

□

Notamos que la primera afirmación del lema anterior es válida para K-álgebras arbitrarias.

Lema 4.2.5. Sea G un grupo finito, K un cuerpo de característica p, y $n \geq 0$ un entero. Entonces el número $\mathfrak{c}_n$ de clases de conjugación de G que contienen un elemento de la forma g^{p^n}, con $g \in G$, está determinado por $K[G]$.

Demostración. Afirmamos que

$$\dim_K(T_n(K[G]) + \mathfrak{c}_n = |G|.$$

Para verlo, sean $C_1, \ldots, C_{\mathfrak{c}_n}$ las clases de conjugación de G que contienen un elemento de la forma g^{p^n}; y consideremos representantes $g_i \in G$ tales que $g_i^{p^n} \in C_i$ para $i = 1, \ldots, \mathfrak{c}_n$. Sea L el subespacio vectorial generado por $g_1, g_2, \ldots, g_{\mathfrak{c}_n}$; es claro que estos elementos son linealmente independientes, por lo que $\dim_K(L) = \mathfrak{c}_n$. Por tanto, para probar nuestra afirmación es suficiente probar que

$$T_n(K[G]) \oplus L = K[G].$$

Si $\sum_{i=1}^{\mathfrak{c}_n} a_i g_i \in L \cap T_n(K[G])$, se sigue directamente de la caracterización dada en el lema anterior que $a_i = 0$ para cada i, y por tanto $L \cap T_n(K[G]) = \{0\}$. Para ver que la suma es efectivamente $K[G]$ será suficiente comprobar que cada $g \in G$ se puede expresar como la suma de un elemento de L y otro de $T_n(K[G])$. Distinguimos tres casos. Si $g = g_i$ para algún i, $g \in L$ y habríamos terminado; si para algún índice $g^{p^n} \in C_i$ pero $g \neq g_i$, entonces es directo (por el lema anterior) que $g - g_i \in T_n(K[G])$ y claramente $g_i \in L$, de modo que $g = g_i + g - g_i$. Finalmente, si $g^{p^n} \notin C_i$ para cada i, entonces es inmediato a partir de la mencionada caracterización que $g \in T_n(K[G])$. Queda por tanto probada nuestra afirmación.

Finalmente, como por definición es claro que $T_n(K[G])$ está determinado por $K[G]$, por estarlo $[K[G], K[G]]$, también lo estará su dimensión, y por ende $\mathfrak{c}_n = |G| - \dim_K(T_n(K[G])$ también está determinado. □

Teorema 4.2.6. *Sea G un p-grupo finito y K un cuerpo de característica p. Entonces el exponente de G está determinado por el álgebra de grupo $K[G]$.*

Demostración. Por el lema anterior, para cada $n \geq 0$ el número $\mathfrak{c}_n$ de clases de conjugación que contienen una potencia p^n-ésima está determinado por $K[G]$, y es inmediato que

$$\exp(G) = p^{\min\{n \,:\, \mathfrak{c}_n = 1\}},$$

con lo que el resultado se sigue. □

Cocientes de la serie de Brauer-Jennings-Zassenhaus

Siguiendo un argumento de D.S. Passman (en [33]), precisamos de la siguiente consideración técnica:

Observación 4.2.7. Sean ζ una indeterminada, y $\Phi_p(\zeta) \in \mathbb{Z}[\zeta]$ el p-ésimo polinomio ciclotómico. Sean $f_0, f_1, \ldots, f_m$ enteros tales que se verifica la igualdad:

$$F(\zeta) = \sum_{t=0}^{m} f_t \zeta^t = \prod_{j=1}^{d} \Phi_p(\zeta^j)^{e_j},$$

para ciertos enteros no negativos $e_1, \ldots, e_n$. Entonces la familia $\{e_i\}_{i=1}^{d}$ está determinada por la familia $\{f_t\}_{t=1}^{m}$.

En efecto, nuestra afirmación se sigue de forma sencilla 'por inducción finita hacia atrás'. Sea ξ_i una raíz ip-ésima compleja primitiva de la unidad $(i = 1, \ldots, d)$. Entonces es inmediato que e_d es la multiplicidad de ξ_d como raíz del polinomio $F(\zeta)$, y por tanto e_d está determinada por $\{f_t\}_{t=1}^{m}$. Supongamos ahora que $e_{j+1}, \ldots, e_d$ están de terminados por $\{f_t\}_{t=1}^{m}$. Entonces e_j es la multiplicidad de ξ_j como raíz del polinomio

$$\Phi_p(\zeta^{j+1})^{-e_j+1} \ldots \Phi_p(\zeta^d)^{-e_d} F(\zeta),$$

que también está determinado por $\{f_t\}_{t=1}^{m}$. La demostración se completa continuando hasta $j = 1$.

Teorema 4.2.8. *Sean G un p-grupo finito, K un cuerpo de característica p, y $n \geq 1$ un entero. Entonces los grupos cociente $\mathcal{M}_{p,n}(G)/\mathcal{M}_{p,n+1}(G)$ están determinados por el álgebra de grupo $K[G]$.*

Demostración. Por el Lema 3.1.7 sabemos que $\mathrm{Aug}_K(G) = JK[G]$ está determinado por $K[G]$. Por tanto, también lo están todas las potencias del ideal de aumento, y en particular los números:

$$f_t = \dim_K \left(\frac{\mathrm{Aug}_K(G)^t}{\mathrm{Aug}_K(G)^{t+1}} \right).$$

Además, como $\mathrm{Aug}_K(G)$ es nilpotente, habrá algún entero m tal que $f_t = 0$ para cada $t > m$. Notemos también que $\mathcal{M}_{p,i}(G)/\mathcal{M}_{p,i+1}(G)$ es abeliano elemental, digamos que de orden p^{e_i}; por tanto, es suficiente probar que los e_i están determinados por los números f_i.

Por el Teorema 3.2.14 sabemos que $D_{\mathbb{F}_p,n}(G) = \mathcal{M}_{p,n}(G)$; y como por el Teorema 3.2.10 la filtración del ideal de aumento asociada a esta N_p-serie es precisamente $\{\mathrm{Aug}_K(G)^t\}_{t\geq 1}$, el apartado (II) del Teorema 3.2.6 implica la ecuación

$$F(\zeta) = \sum_{t=0}^{m} f_t \zeta^t = \prod_{j=1}^{d} \Phi_p(\zeta)^{e_j}$$

en el anillo de polinomios $\mathbb{Z}[\zeta]$, siendo d un entero tal que $\mathcal{M}_{p,s}(G) = \langle 1 \rangle$ para cada $s > d$. Usando ahora la Observación 4.2.7, se deduce que los e_i están determinados por los f_t, y el resultado se sigue.

□

Corolario 4.2.9. *Sean G un p-grupo finito y K un cuerpo de característica p. Entonces longitud ℓ de la serie de Brauer-Jennings-Zassenhaus $\{\mathcal{M}_{p,n}(G)\}_{n\geq 1}$ está determinada por el álgebra de grupo $K[G]$.*

Demostración. Los cocientes $\mathcal{M}_{p,n}(G)/\mathcal{M}_{p,n+1}(G)$ están determinados por $K[G]$ por el teorema anterior, y ℓ no es más que el menor entero ≥ 1 tal que $\mathcal{M}_{p,n+1}(G)/\mathcal{M}_{p,n+2}(G) = \{1\}$ para cada $n \geq \ell$. □

Corolario 4.2.10. *Sean G un p-grupo finito y K un cuerpo de característica p. Entonces para cada $n \geq 1$ el orden $|\mathcal{M}_{p,n}(G)|$ de cada elemento de la serie de Brauer-Jennings-Zassenhaus está determinada por el álgebra de grupo $K[G]$.*

Demostración. Basta notar que

$$|\mathcal{M}_{p,n}(G)| = \prod_{i=n}^{\ell} \left| \frac{\mathcal{M}_{p,n}(G)}{\mathcal{M}_{p,n+1}(G)} \right|,$$

y que tanto ℓ como los factores están determinados por $K[G]$ a la luz de los dos resultados previos. □

El siguiente resultado se corresponde con un lema de C. Bagińsky en [2]:

Teorema 4.2.11. *Sean G un p-grupo finito, K un cuerpo de característica p, y $n \geq 1$ un entero. Entonces la clase de isomorfía del grupo cociente $\mathcal{M}_n(G')/\mathcal{M}_{n+1}(G')$ está determinada por el álgebra de grupo $K[G]$.*

Demostración. Por la primera parte del Lema 4.2.3 sabemos que el ideal $\mathrm{Aug}_K(G, G')$ está determinado por $K[G]$. Por tanto también lo están todas sus potencias, y en particular los números

$$f'_t = \dim_K \left(\frac{\mathrm{Aug}_K(G, G')^t}{\mathrm{Aug}_K(G, G')^{t+1}} \right).$$

Además, por la Proposición 2.2.11 se tiene que $\mathrm{Aug}_K(G, G')^t = \mathrm{Aug}_K(G')^t \cdot K[G]$ para cada t, de modo que

$$f'_t = \dim_K \left(\frac{\mathrm{Aug}_K(G')^t \cdot K[G]}{\mathrm{Aug}_K(G')^{t+1} \cdot K[G]} \right) = (G : G') \cdot \dim_K \left(\frac{\mathrm{Aug}_K(G')^t}{\mathrm{Aug}_K(G')^{t+1}} \right),$$

donde la segunda igualdad se sigue directamente del Corolario 2.2.13. Por tanto, los números

$$f_t = \frac{f'_t}{(G : G')} = \dim_K \left(\frac{\mathrm{Aug}_K(G')^t}{\mathrm{Aug}_K(G')^{t+1}} \right)$$

están determinados por $K[G]$, y el resultado se obtiene exactamente igual que en el teorema previo.

En efecto, $f_t = 0$ si t es lo suficientemente grande por ser $\mathrm{Aug}_K(G')$ nilpotente; $\mathcal{M}_{p,i}(G')/\mathcal{M}_{p,i+1}(G')$ es abeliano elemental, digamos que de orden p^{e_i}, por lo que es suficiente probar que los e_i están determinados por $K[G]$. Como por los Teoremas 3.2.14 y 3.2.10 sabemos que la filtración del ideal de aumento asociada a la N_p serie $D_{\mathbb{F}_p,n}(G') = \mathcal{M}_{p,n}(G')$ es precisamente $\{\mathrm{Aug}_K(G')^t\}_{t\geq 1}$, el apartado (II) del Teorema 3.2.6 implica la ecuación

$$F(\zeta) = \sum_{t=0} f_t \zeta^t = \prod_{j=1}^{d} \Phi_j(\zeta)^{e_j}$$

en el anillo de polinomios $\mathbb{Z}[\zeta]$, siendo d un entero tal que $\mathcal{M}_{p,s}(G') = \langle 1 \rangle$ para cada $s \geq d$. Utilizando entonces la Observación 4.2.7, se obtiene que los e_i están determinados por los f_t, y por tanto por $K[G]$. □

El centro y el abelianizado

Probamos ahora que tanto el centro de G como su abelianizado están determinados por $K[G]$, tomando como antes los argumentos de [33].

Lema 4.2.12. Sea G un p-grupo finito y K un cuerpo de característica p. Entonces el valor de la afirmación "G es abeliano" está determinado por $K[G]$.

Demostración. Basta notar que G es abeliano si y sólo si el álgebra $K[G]$ es conmutativa. □

El siguiente teorema resuelve el problema del isomorfismo modular amplio **(WMIP)** para p-grupos abelianos, y es clave para probar los dos principales teoremas de la subsección:

Teorema 4.2.13 (Deskins)**.** *Sea G un p-grupo abeliano finito y K un cuerpo de característica p. Entonces la clase de isomorfía de G está determinada por el álgebra de grupo $K[G]$.*

Demostración. Es claro que $\mathcal{M}_{p,n}(G) = G^{(p^{n-1})}$, de modo que

$$\left|\frac{\mathcal{M}_{p,i+1}(G)}{\mathcal{M}_{p,i}(G)}\right| = \frac{|G^{(p^i)}|}{|G^{(p^{i-1})}|},$$

y como el primer miembro de la igualdad está determinado por $K[G]$ por el Teorema 4.2.8, y además es $|G^{(p^i)}| = 1$ si i es lo suficientemente grande, se deduce que que los órdenes $|G^{(p^i)}|$ están también determinados por $K[G]$, para cada i. Esto, junto con la Proposición 1.1.20, prueba que G está determinado por $K[G]$ en la clase de los grupos abelianos; y como debido al Lema 4.2.12 sabemos que el hecho de pertenecer a esta clase está determinada por $K[G]$, el resultado se sigue. □

Teorema 4.2.14 (Deskins)**.** *Sea G un p-grupo finito. Entonces la clase de isomorfía de G/G' está determinada por el álgebra de grupo $K[G]$.*

Demostración. Comenzamos notando que por el Lema 4.2.3 el ideal $I = \mathrm{Aug}_K(G, G')$ está determinado por $K[G]$. Como por el Corolario 2.2.9 hay un isomorfismo $K[G/G'] \cong K[G]/I$, se deduce que $K[G/G']$ está determinado por $K[G]$; pero G/G' es abeliano, de manera que por el Teorema 4.2.13 la clase de isomorfía de G/G' está determinada por $K[G/G']$, y el resultado se sigue. □

Teorema 4.2.15 (Ward)**.** *Sea G un p-grupo finito. Entonces la clase de isomorfía de $\mathcal{Z}(G)$ está determinada por el álgebra de grupo $K[G]$.*

Demostración. En primer lugar notemos que $I = \mathcal{Z}(K[G]) \cap [K[G], K[G]]$ es un ideal de $\mathcal{Z}(K[G])$; en efecto, es evidentemente un subespacio vectorial, y además, dados $x \in \mathcal{Z}(K[G])$ y $a \in I$, podemos escribir $a = \sum_i [\alpha_i, \beta_i]$, con $\alpha_i, \beta_i \in K[G]$, de modo que

$$ax = xa = \sum_i [x\alpha_i, \beta_i] \in \mathcal{Z}(K[G]) \cap [K[G], K[G]] = I.$$

Consideremos ahora la aplicación natural $\lambda : K[\mathcal{Z}(G)] \to \mathcal{Z}(K[G])/I$; es claro que es un homomorfismo de álgebras, pues no es más que la composición de la inclusión $K[\mathcal{Z}(G)] \subseteq \mathcal{Z}(K[G])$ con el homomorfismo canónico en el álgebra cociente.

Por el Teorema 2.1.8 sabemos que un elemento cualquiera de $\mathcal{Z}(K[G])/I$ es de la forma

$$\sum_{C \in \mathrm{Cl}(G)} a_C \left(\sum_{g \in C} g \right) + I;$$

ahora, notando que para cada clase de conjugación C con más de un elemento p es un divisor de $|C|$, podemos usar el Lema 2.1.12 para deducir que $\sum_{g \in C} g$ también pertenece a $[K[G], K[G]]$.

Así, como obviamente también es central, se deduce que $\sum_{g\in G} g \in I$, y el elemento considerado se reescribe, poniendo $a_g = a_C$ si $C = \{g\}$, como

$$\sum_{g\in\mathcal{Z}(G)} a_g g + I,$$

que no es más que la imagen por λ de $\sum_{g\in\mathcal{Z}(G)} a_g g \in K[\mathcal{Z}(G)]$. Esto prueba que λ es un epimorfismo. Para ver que es un monomorfismo basta notar que de nuevo por el Lema 2.1.12 se tiene que

$$\mathcal{Z}(G) \cap \mathrm{Sop}(\alpha) = \emptyset \qquad \text{para cada } \alpha \in [K[G], K[G]],$$

de modo que que si $\sum_{g\in\mathcal{Z}(G)} a_g g \in I$, necesariamete $a_g = 0$ para cada $g \in \mathcal{Z}(G)$.

En definitiva, hemos encontrado un isomorfismo $K[\mathcal{Z}(G)] \cong \mathcal{Z}(K[G])/I$. Dado que la clase de isomorfía de la segunda álgebra está claramente determinada por la de $K[G]$, también lo está la de $K[\mathcal{Z}(G)]$; ahora bien, como $\mathcal{Z}(G)$ es abeliano, esta última determina, por el Teorema 4.2.13, la clase de isomorfía de $\mathcal{Z}(G)$, con lo que el resultado se sigue.

□

El subgrupo conmutador G', en la clase de los grupos metabelianos

Con un razonamiento análogo al de la Proposición 4.2.13 obtenemos que:

Proposición 4.2.16. Sea G un p-grupo metabeliano finito y K un cuerpo de característica p. Entonces la clase de isomorfía del subgrupo conmutador G' está determinada por el álgebra de grupo $K[G]$ en la clase de los grupos metabelianos finitos.

Demostración. Asumiendo que G' es abeliano, es inmediato que $\mathcal{M}_{p,n}(G') = (G')^{(p^{n-1})}$, de modo que

$$\left|\frac{\mathcal{M}_{p,i+1}(G')}{\mathcal{M}_{p,i}(G')}\right| = \frac{|(G')^{(p^i)}|}{|(G')^{(p^{i-1})}|},$$

y como el primer miembro de la igualdad está determinado por $K[G]$ por el Teorema 4.2.11, y además es $|(G')^{(p^i)}| = 1$ si i es lo suficientemente grande, se deduce que los órdenes $|(G')^{(p^i)}|$ están también determinados por $K[G]$, para cada i. Así, el resultado se sigue de la Proposición 1.1.20. □

El mínimo número de generadores

Recordemos que, dado un grupo H, denotábamos por $d(H)$ al mínimo número natural n tal que existe un conjunto de generadores de H de tamaño n.

Teorema 4.2.17. *Sea G un p-grupo finito, y K un cuerpo de característica p. Entonces los parámetros $d(G)$ y $d(G')$ están determinados por el álgebra de grupo $K[G]$.*

Demostración. Sea $H = G$ ó G'. Por los Teoremas 4.2.8 y 4.2.11 sabemos que la clase de isomorfía del grupo abeliano elemental

$$\frac{\mathcal{M}_{p,1}(H)}{\mathcal{M}_{p,2}(H)} = \frac{H}{\mathcal{M}_{p,2}(H)} = \frac{H}{\Phi(H)}$$

está determinada por $K[G]$, por lo que también lo está su dimensión como $\mathbb{F}_p$-espacio vectorial. Ahora bien, es claro que las bases de este espacio son precisamente los conjuntos de generadores de tamaño mínimo, por lo que

$$\dim_{\mathbb{F}_p}\left(\frac{H}{\Phi(H)}\right) = d\left(\frac{H}{\Phi(H)}\right) = d(H),$$

donde la última igualdad se tiene por la Proposición 1.1.38, y el teorema se sigue. □

La clase de nilpotencia, en ciertas condiciones

Aunque en general no se sabe si la clase de nilpotencia de un grupo G está determinada por su álgebra de grupo $K[G]$, los resultados de esta subsección, que tomamos de [7], dan una respuesta positiva a esta cuestión si imponemos alguna condición adicional sobre G. Antes de verlo conviene recordar la siguiente propiedad general:

Observación 4.2.18. Sean N, H dos subgrupos de un grupo G, con $N \trianglelefteq G$. Es bien conocida (ver [9], pág. 80 para una prueba) la igualdad:

$$|NH| = \frac{|N| \cdot |H|}{|N \cap H|}.$$

Lema 4.2.19. Sea G un p-grupo finito y K un cuerpo de característica p. Entonces los órdenes $|G'|$, $|\mathcal{Z}(G)G'|$ y $|\mathcal{Z}(G) \cap G'|$ están determinados por $K[G]$.

Demostración. En primer lugar, $|G'|$ está claramente determinado por $K[G]$, pues, por ejemplo, por el Teorema 4.2.14 lo está $|G/G'| = |G|/|G'|$, y obviamente $K[G]$ determina su dimensión $|G| = \dim_K(K[G])$.

Por otro lado, sabemos por el apartado (II) del Lema 4.2.3 que el ideal $\mathrm{Aug}_K(G, \mathcal{Z}(G)G')$ está determinado por $K[G]$, de modo que también lo está la K-álgebra

$$\frac{K[G]}{\mathrm{Aug}_K(G, \mathcal{Z}(G)G')} \cong K\left[\frac{G}{G'\mathcal{Z}(G)}\right]$$

y su K-dimensión $|G/\mathcal{Z}(G)G'| = |G|/|\mathcal{Z}(G)G'|$. Así, $|\mathcal{Z}(G)G'|$ está determinado por $K[G]$. Finalmente, como $|\mathcal{Z}(G)|$ por el Teorema 4.2.15 también está determinado por $K[G]$, se deduce que

$$|\mathcal{Z}(G) \cap G'| = \frac{|\mathcal{Z}(G)||G'|}{|\mathcal{Z}(G)G'|}$$

está determinado por $K[G]$, y el lema queda probado. □

Proposición 4.2.20. Sea G un p-grupo finito y K un cuerpo de característica p. Entonces el valor de verdad de la afirmación "$c(G) = 2$" está determinado por $K[G]$.

Demostración. Se tiene que $c(G) = 2$ si y sólo si $\langle 1\rangle = \gamma_3(G) = (\gamma_2(G), G) = (G', G)$, y esto es equivalente a que $G' \subseteq \mathcal{Z}(G)$, es decir, $G' = \mathcal{Z}(G) \cap G'$.Como $G' \supseteq \mathcal{Z}(G) \cap G'$ en cualquier caso, se deduce que $c(G) = 2$ si y sólo si $|G'| = |\mathcal{Z}(G) \cap G'|$. Como por el Lema 4.2.19 estos dos números están determinados por $K[G]$, el resultado se sigue. □

Teorema 4.2.21. *Sea G un p-grupo. Entonces $c(G)$, la clase de nilpotencia de G, viene determinada por $K[G]$ si se da alguna de las siguientes condiciones:*

(I) $\exp(G) = p$;

(II) G' *es cíclico .*

Demostración. Como tanto el exponente de G como el valor de la afirmación "G' es cíclico" están determinados por $K[G]$, basta probar que $c(G)$ está determinado por $K[G]$ en las clases de grupos de exponente p y de grupos con subgrupo conmutador cíclico, respectivamente.

(I) Si $\exp G = p$, se sigue fácilmente por inducción que $\mathcal{M}_{p,n}(G) = \gamma_n(G)$ para cada n; en efecto, $\mathcal{M}_{p,1}(G) = G = \gamma_1(G)$, y si se verifica la igualdad para $n-1$ entonces

$$\mathcal{M}_{p,n}(G) = (\mathcal{M}_{p,n-1}(G), G) \cdot \mathcal{M}_{p,i}(G)^{(p)} = (\gamma_{n-1}(G), G) \cdot \langle 1\rangle = \gamma_n(G).$$

Entonces, por el Teorema 4.2.8, el cociente

$$\gamma_n(G)/\gamma_{n+1}(G) = \mathcal{M}_{p,i}(G)/\mathcal{M}_{p,i+1}(G)$$

está determinado por $K[G]$, y por tanto también lo está $c(G)$ en la clase de grupos de exponente p, pues es el mínimo entero $n > 0$ tal que $\gamma_n(G)/\gamma_{n+1}(G) = \langle 1\rangle$.

(II) Recordemos que por el Teorema 4.2.14 la clase de isomorfía de G/G' está determinada por $K[G]$. Sea G un p-grupo con G' cíclico, digamos de orden p^m. Podemos entonces escribir $G' = \langle g \rangle$, con $o(g) = p^m$. Probaremos el resultado por inducción sobre la clase de nilpotencia de G. Si $c(G) = 1$, G es abeliano, por lo que la Proposición 4.2.13) da que G está determinado por $K[G]$, de modo que también lo está $c(G) = 1$.

Supongamos la propiedad probada para todos los grupos con clase de nilpotencia menor que c. Como por el Lema 4.2.19 sabemos que $|\mathcal{Z}(G) \cap G'|$ está determinado por $K[G]$, podemos escribir $\mathcal{Z}(G) \cap G' = \langle g^{p^k} \rangle$ para cierto entero k determinado por $K[G]$.

Consideremos el ideal $\mathrm{Aug}_K(G, G') = (g-1)K[G]$, que por el Lema 4.2.3 está determinado por $K[G]$. Entonces también lo está

$$\mathrm{Aug}_K(G, G')^{p^k} = \mathrm{Aug}_K(G')^{p^k} K[G] =$$

$$(g-1)^{p^k} K[G] = (g^{p^k} - 1)K[G] = \mathrm{Aug}_K(G, \langle g^{p^k} \rangle),$$

y en consecuencia el cociente

$$\frac{K[G]}{\mathrm{Aug}_K(G, G')^{p^k}} = \frac{K[G]}{\mathrm{Aug}_K(G, \langle g^{p^k} \rangle)} \cong K\left[\frac{G}{\langle g^{p^k} \rangle}\right]$$

también está determinado por $K[G]$.

Ahora notamos que

$$c\left(\frac{G}{\langle g^{p^k} \rangle}\right) = c\left(\frac{G}{\mathcal{Z}(G) \cap G'}\right) = c(G) - 1,$$

debiéndose la última igualdad al Lema 1.1.13; en efecto, $\gamma_c(G) \subseteq \mathcal{Z}(G) \cap G'$, por lo que

$$\gamma_c\left(\frac{G}{\mathcal{Z}(G) \cap G'}\right) = \frac{\gamma_c(G) \cdot \mathcal{Z}(G) \cap G'}{\mathcal{Z}(G) \cap G'} = \{1\},$$

y el término anterior de la serie no es trivial por no ser $\gamma_{c-1}(G)$ central. Ahora bien, por la hipótesis de inducción este número está determinado por $K\left[G/\langle g^{p^k} \rangle\right]$; así, se sigue directamente que $c(G)$ está determinado por este álgebra de grupo, y por tanto por $K[G]$ (en la clase de grupos con subgrupo conmutador cíclico).

□

4.3. Invariantes determinados por $\mathbb{F}_p[G]$

Todos los resultados de la sección anterior se pueden aplicar a $\mathbb{F}_p[G]$, siendo $\mathbb{F}_p$ el cuerpo de p elementos; en particular ya tenemos probado el siguiente resultado:

Corolario 4.3.1. *Sea G un p-grupo finito. Entonces los siguientes invariantes de G están determinados por el álgebra de grupo $\mathbb{F}_p[G]$:*

(I) El exponente de G.

(II) La clase de isomorfía de los grupos cociente $\mathcal{M}_{p,n}(G)/\mathcal{M}_{p,n+1}(G)$, para $n \geq 1$.

(III) La clase de isomorfía de los grupos cociente $\mathcal{M}_{p,n}(G')/\mathcal{M}_{p,n+1}(G')$, para $n \geq 1$.

(IV) La clase de isomorfía de G/G'.

(V) La clase de isomorfía de $\mathcal{Z}(G)$.

(VI) La clase de isomorfía de G', en la clase de los grupos metabelianos.

(VII) *Los números mínimos de generadores $d(G)$ y $d(G')$.*

(VIII) *La clase de nilpotencia de G, supuesta alguna de las siguientes condiciones:*

a) $\exp G = p$;

b) *G' es cíclico;*

c) *la clase de nilpotencia de G es a lo sumo 2.*

Además, será fundamental en la mayoría de las demostraciones tener en cuenta la siguiente consideración:

Observación 4.3.2. Los ideales de Zassenhaus $I_{\mathbb{F}_p,n}(G)$ están determinados por $\mathbb{F}_p[G]$ como consecuencia directa de la Observación 4.2.2 y la definición de $I_{\mathbb{F}_p,n}(G)$.

Más cocientes de la serie de Brauer-Jennings-Zassenhaus

A pesar de la simplicidad y generalidad de la demostración que dimos al Teorema 4.2.8, tomada de [33], conviene considerar también la demostración original limitada al caso modular, debida a Passi y Sehgal (ver [31]), y que tomamos de [39]; ésta hace uso de los ideales de Zassenhaus, que serán fundamentales a la hora de ver otros resultados más generales sobre los cocientes de la serie de Brauer-Jennings-Zassenhaus.

Otra demostración del Teorema 4.2.8 para $K = \mathbb{F}_p$. Recordemos que por el Corolario 3.4.12 se tiene la igualdad:

$$I_{\mathbb{F}_p,n}(G) = \mathcal{M}_{p,n}(G) - 1 + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1};$$

podemos entonces definir una aplicación $\lambda : \mathcal{M}_{p,n}(G) \to I_{\mathbb{F}_p,n}(G)/\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$ mediante $\lambda(m) = m - 1 + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$ para cada $m \in \mathcal{M}_{p,n}(G)$.

Esta aplicación es claramente un homomorfismo de grupos (siendo el primero multiplicativo, y el segundo aditivo), pues dados $m_1, m_2 \in \mathcal{M}_{p,n}(G) = D_{\mathbb{F}_p,n}(G)$, se tiene que $m_1 - 1, m_2 - 1 \in \mathrm{Aug}_{\mathbb{F}_p}(G)^n$, y así:

$$\lambda(m_1 m_2) = m_1 m_2 - 1 + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1} =$$

$$\underbrace{(m_1 - 1)(m_2 - 1)}_{\in \mathrm{Aug}_{\mathbb{F}_p}(G)^{2n}} + (m_1 - 1) + (m_2 - 1) + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1} =$$

$$= (m_1 - 1) + (m_2 - 1) + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1} = \lambda(m_1) + \lambda(m_2).$$

Además es evidente que es un epimorfismo. Finalmente, notamos que el núcleo de λ es precisamente $\mathcal{M}_{p,n}(G)$, pues dado $m \in \mathcal{M}_{p,n}(G)$ se tiene que $\lambda(m) = 0$ si y sólo si $m - 1 \in \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$, y esto es equivalente a que $m \in D_{\mathbb{F}_p,n+1}(G) = \mathcal{M}_{p,n+1}(G)$. Por tanto, λ induce un isomorfismo

$$\frac{\mathcal{M}_{p,n}(G)}{\mathcal{M}_{p,n+1}(G)} \cong \frac{I_{\mathbb{F}_p,n}(G)}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}},$$

y la clase de isomorfía del último grupo cociente está determinada por $\mathbb{F}_p[G]$ los ideales $I_{\mathbb{F}_p,n}(G)$ y $\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$, y por tanto la clase de isomorfismo del cociente como grupos abeliano). □

Notemos que el uso de los ideales de Zassenhaus (y, sobre todo, de su caracterización en el Corolario 3.4.12) nos impide llevar a cabo esta prueba, y la de todos los resultados subsiguientes relativos a la $\mathcal{M}$-serie, en otro cuerpo de característica p que no sea el de p elementos.

Teorema 4.3.3 (Passi-Sehgal)**.** *Sea G un p-grupo finito, y $n \geq 1$ un entero. Entonces la clase de isomorfía de $\mathcal{M}_{p,n}(G)/\mathcal{M}_{p,n+2}(G)$ está determinada por el álgebra de grupo $\mathbb{F}_p[G]$.*

Demostración. Dado que $\mathrm{Aug}_{\mathbb{F}_p}(\mathcal{M}_{p,n}(G)) \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^n$ se tiene que

$$\frac{\mathrm{Aug}_{\mathbb{F}_p}(\mathcal{M}_{p,n}(G)) + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}} = \frac{I_{\mathbb{F}_p,n}(G)}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}}$$

es un subespacio del $\mathbb{F}_p$-espacio vectorial de $\mathrm{Aug}_{\mathbb{F}_p}(G)^n / \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$, y por tanto podemos considerar la descomposición

$$\frac{\mathrm{Aug}_{\mathbb{F}_p}(G)^n}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}} = \frac{I_{\mathbb{F}_p,n}(G)}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}} \oplus \frac{L_n(G)}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}}, \tag{4.1}$$

para cierto subespacio vectorial $L_n(G)$ de $\mathbb{F}_p[G]$ con $\mathrm{Aug}^{n+1}_{\mathbb{F}_p}(G) \subseteq L_n(G) \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^n$. Por tanto, para cada $g \in G$ y $\alpha \in L_n(G)$ se tiene que

$$g\alpha = (g-1)\alpha + \alpha \in L_n(G),$$

pues $(g-1)\alpha \in \mathrm{Aug}^{n+1}_{\mathbb{F}_p}(G)$. Se sigue entonces que $L_n(G)$ es un ideal de $\mathbb{F}_p[G]$. Precisaremos de la afirmación siguiente:

- Se verifica:
$$\frac{\mathcal{M}_{p,n}(G)}{\mathcal{M}_{p,n+2}(G)} \cong \frac{\mathcal{M}_{p,n}(G) + L_{n+1}(G)}{L_{n+1}(G)}, \tag{4.2}$$
siendo el isomorfismo de grupos multiplicativos (es directo que el segundo grupo con la operación dada por el producto efectivamente lo es). Consideremos la aplicación natural
$$\lambda : \mathcal{M}_{p,n}(G) \to \frac{\mathcal{M}_{p,n}(G) + L_{n+1}(G)}{L_{n+1}(G)},$$
es decir, la dada por $\lambda(m) = \overline{m}$ para cada $m \in \mathcal{M}_{p,n}(G)$. Es entonces claro que λ es un epimorfismo de grupos que contiene a $\mathcal{M}_{p,n+2}(G) \subseteq L_{n+1}(G)$ en su núcleo.
Supongamos que $m \in \mathrm{Ker}(\lambda)$, i.e., $\lambda(m) = \overline{1}$; entonces $m - 1 \in L_{n+1}(G) \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$, y por tanto $m \in \mathcal{M}_{p,n+1}(G)$. En consecuencia,
$$m - 1 \in \mathrm{Aug}_{\mathbb{F}_p}\left(\mathcal{M}_{p,n+1}(G)\right) \cap L_{n+1}(G) = \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+2}$$
donde la igualdad se tiene por ser la suma directa en la ecuación (4.1); por tanto, se deduce que $m \in \mathcal{M}_{p,n+2}(G)$; esto termina de probar la igualdad $\mathrm{Ker}(\lambda) = \mathcal{M}_{p,n+2}(G)$. Se sigue entonces directamente que λ induce un isomorfismo como en (4.2), y hemos terminado.

Sea ahora H otro p-grupo finito tal que $\mathbb{F}_p[G] \cong \mathbb{F}_p[H]$, y sea $\theta : \mathbb{F}_p[H] \to \mathbb{F}_p[H]$ un isomorfismo normalizado. Claramente todo lo anterior sigue siendo válido para H. Además, aplicando θ a la ecuación (4.1) y usando que el ideal de Zassenhaus $I_{\mathbb{F}_p,n}(G)$ está determinado por $\mathbb{F}_p[G]$, se obtiene que:

$$\frac{\mathrm{Aug}_{\mathbb{F}_p}(H)^n}{\mathrm{Aug}_{\mathbb{F}_p}(H)^{n+1}} = \theta\left(\frac{\mathrm{Aug}_{\mathbb{F}_p}(G)^n}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}}\right) = \frac{I_{\mathbb{F}_p,n}(H)}{\mathrm{Aug}_{\mathbb{F}_p}(H)^{n+1}} \oplus \frac{\theta(L_n(G))}{\mathrm{Aug}_{\mathbb{F}_p}(H)^{n+1}}. \tag{4.3}$$

Repitiendo el mismo razonamiento que nos permitió deducir (4.2) de (4.1, podemos inferir de la ecuación anterior que

$$\frac{\mathcal{M}_{p,n}(H)}{\mathcal{M}_{p,n+2}(H)} = \frac{\mathcal{M}_n(H) + \theta(L_{n+1}(G))}{\theta(\mathbb{F}_{p_{n+1}}(G))}. \tag{4.4}$$

Ahora afirmamos que:

- Se tiene que
$$\theta\left(\mathcal{M}_{p,n}(G) + L_{n+1}(G)\right) = \mathcal{M}_{p,n}(H) + \theta\left(L_{n+1}(G)\right). \tag{4.5}$$
Para ver la inclusión hacia la derecha, sea $m \in \mathcal{M}_{p,n}(G)$. Entonces $m-1 \in I_{\mathbb{F}_p,n}(G)$ por el Corolario 3.4.12. Por tanto, como los ideales de Zassenhaus están determinados por el álgebra de grupo, se tendrá que $\theta(m-1) \in I_{\mathbb{F}_p,n}(H)$. Así, de nuevo por el Corolario 3.4.12 podemos escribir
$$\theta(m-1) = h - 1 + \gamma, \qquad \text{con } h \in \mathcal{M}_{p,n}(H),\ \gamma \in \mathrm{Aug}_{\mathbb{F}_p}(H)^{n+1},$$
y por tanto $\theta(m) = h + \gamma$. Además, usando ahora la ecuación 4.3 y el mencionado corolario se deduce que γ admite una expresión de la forma
$$\gamma = u - 1 + v, \qquad \text{con } u \in \mathcal{M}_{n+1}(H),\ v \in \theta(L_{n+1}(G)).$$
Por tanto, se tiene que
$$\begin{aligned}\theta(m) &= h + u - 1 + v \\ &= \underbrace{hu}_{\in \mathcal{M}_{p,n}(H)} - \underbrace{(h-1)(u-1)+v}_{\in \theta(L_{n+1})},\end{aligned}$$
pues que el primer sumando esté en $\mathcal{M}_{p,n}(H)$ es evidente, mientras que como $u \in \mathcal{M}_{p,n](H)}$, u está en la n-ésima potencia del ideal de aumento, y por tanto $(h-1)(u-1) \in \mathrm{Aug}_{\mathbb{F}_p}(H)^{n+1} = \theta(\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}) \subseteq \theta(L_{n+1}(G))$.
Para la inclusión recíproca, teniendo en cuenta que en la ecuación (4.3) el subespacio $\theta(L_{n+1}(G))$ representa el papel de $L_{n+1}(H)$ en la ecuación (4.1), intercambiando G y H y sustituyendo θ por θ^{-1}, el razonamiento que probaba la inclusión anterior también prueba que
$$\theta^{-1}(\mathcal{M}_{p,n}(H) + \theta(L_{n+1}(G))) \subseteq \mathcal{M}_{p,n}(G) + L_{n+1}(G),$$
de modo que aplicando θ a ambos lados se termina de demostrar (4.5).

Queda con esto la demostración completa: en efecto, ya hemos mostrado que
$$\frac{\mathcal{M}_n(G)}{\mathcal{M}_{n+2}(G)} \cong \frac{\mathcal{M}_{p,n}(G) + L_{n+1}(G)}{L_{n+1}(G)} \cong \frac{\mathcal{M}_n(H) + \theta(L_{n+1}(G))}{\theta(L_{n+1}(G))} \cong \frac{\mathcal{M}_{p,n}(H)}{\mathcal{M}_{p,n+2}(H)},$$
donde el primer isomorfismo es el de (4.2), el segundo es el inducido por θ (pues en la ecuación (4.5) el miembro de la derecha es la imagen por θ del de la izquierda) y el último es el de (4.4). □

El siguiente teorema de Ritter y Sehgal (que tomamos de [34]) es el resultado más general conocido en relación a los cocientes de la serie de Brauer-Jennings-Zassenhaus determinados por el álgebra de grupo $\mathbb{F}_p[G]$.

Teorema 4.3.4 (Ritter-Sehgal)**.** *Sea G un p-grupo finito, y $n \geq 1$ un entero. Entonces la clase de isomorfía de $\mathcal{M}_{p,n}(G)/\mathcal{M}_{p,2n+1}(G)$ está determinada por el álgebra de grupo $\mathbb{F}_p[G]$.*

Demostración. Fijemos $n \geq 1$. Razonando como en la demostración del teorema anterior, sabemos que existe una descomposición como suma directa de espacios vectoriales
$$\frac{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+2}} = \frac{I_{\mathbb{F}_p,n+1}(G)}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+2}} \oplus \frac{L_1}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+2}}, \tag{4.6}$$
donde L_1 es un subespacio de $\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$ que contiene a $\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+2}$.

Observando ahora que $L_1 \supseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+2} \supseteq \mathrm{Aug}_{\mathbb{F}_p}(\mathcal{M}_{p,n+2}) + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+3}$, se deduce razonando análogamente la existencia de un subespacio L_2 de L_1 que contiene a $\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+3}$ tal que
$$\frac{L_1(G)}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+3}} = \frac{I_{\mathbb{F}_p,n+2}(G)}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+3}} \oplus \frac{L_2}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+3}}.$$

Procediendo de esta manera, obtenemos subespacios L_j tales que

$$\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1} = L_0 \supseteq L_1 \supseteq L_2 \supseteq \cdots \supseteq L_j \supseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+j+1}$$

y descomposiciones

$$\frac{L_j}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+j+2}} = \frac{I_{\mathbb{F}_p,n+j+1}(G)}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+j+2}} \oplus \frac{L_{j+1}}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+j+2}}. \tag{4.7}$$

Además, siempre que $j \leq n$, se tiene que $\mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1} \subseteq L_j \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$, por lo que cada uno de estos L_j es un ideal de $\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$.

- Afirmamos que
$$\mathcal{M}_{p,n}(G) + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1} = \mathcal{M}_{p,n}(G) + L_n. \tag{4.8}$$
En efecto, como $L_n \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$, la inclusión hacia la izquierda es trivial. Si probamos que, para $i = 0, 1, \ldots, n$, se tiene que para cada $m_n \in \mathcal{M}_{p,n}(G)$ y cada $l_0 \in L_0 = \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$ existen ciertos $g_n \in \mathcal{M}_{p,n}(G)$ y $l_i \in L_i$ tales que
$$m_n + l_0 = g_n + l_i,$$
el contenido restante obtiene directamente del caso $i = n$.

  Lo haremos por inducción sobre i. El caso $i = 0$ es trivial. Supongamos que tenemos la expresión $m_n + l_0 = g_n + l_i$ para $i < n$. Usando la ecuación (4.7) con $j = i$ y teniendo presente el Corolario 3.4.12 y la inclusión $\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+i+1} \subseteq L_i$, podemos escribir
$$l_i = m_{n+1} - 1 + l_{i+1}, \qquad \text{con } m_{n+1} \in \mathcal{M}_{p,n+1}(G), \text{ y } l_{i+1} \in L_{i+1}.$$
  Entonces se tiene que
$$m_n + l_0 = g_n + l_i = g_n + m_{n+1} - 1 + l_{i+1} =$$
$$\underbrace{m_n m_{n+1}}_{g'_n \in \mathcal{M}_{p,n}(G)} + \underbrace{l_{i+1} - (g_n - 1)(m_{n+1} - 1)}_{l'_{i+1} \in L_{i+1}} = g'_n + l'_{i+1} \in \mathcal{M}_{p,n}(G) + L_1$$
  ya que $(m_n - 1)(m_{n+1} - 1) \in \mathrm{Aug}_K(G)^{2n+1} \subseteq L_{i+1}$, y lo que completa el paso inductivo.

- Ahora afirmamos que
$$\frac{\mathcal{M}_{p,n}(G)}{\mathcal{M}_{p,2n+1}(G)} \cong \frac{\left(\frac{\mathcal{M}_{p,n}(G)+\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1}}\right)}{\left(\frac{(1+L_n)}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1}}\right)} \tag{4.9}$$
  Entendemos que $(\mathcal{M}_{p,n}(G) + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1})/\mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1}$ es un grupo multiplicativo contenido en $\mathbb{F}_p[G]/\mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1}$. Para probar la afirmación, comenzamos notando que la ecuación (4.8) los elementos de este grupo son de la forma $m + l + \mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1}$, donde $m \in \mathcal{M}_{p,n}(G)$ y $l \in L_n$. Podemos entonces definir la aplicación
$$\lambda : \frac{\mathcal{M}_{p,n}(G) + \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1}} \to \frac{\mathcal{M}_{p,n}(G)}{\mathcal{M}_{p,2n+1}(G)}; \qquad \lambda(m+l+\mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1}) = m\mathcal{M}_{p,2n+1}(G).$$
  Veamos primero que está bien definida. Supongamos que $m + l = m' + l' + \alpha$, con $\alpha \in \mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1}$, $m, m' \in \mathcal{M}_{p,n}(G)$ y $l, l' \in L_n$. Entonces
$$m^{-1}m' - 1 = m^{-1}l - m^{-1}l' - m^{-1}\alpha =$$

$$(m^{-1}-1)l + l - (m^{-1}-1)l' - l' - m^{-1}\alpha \in L_n,$$

por ser $\mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1} \subseteq L_n$, y este último subespacio cerrado para productos por elementos de $\mathrm{Aug}_{\mathbb{F}_p}(G)^n$. Entonces

$$m^{-1}m' - 1 \in L_n \subseteq L_1 \qquad \Rightarrow \qquad m^{-1}m' - 1 \in L_1 \cap \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1} = \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+2}$$

(siendo la igualdad cierta por (4.6)). Esto a su vez implica que $m^{-1}m'-1 \in L_2 \cap \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+2} = \mathrm{Aug}_{\mathbb{F}_p}(G)^{n+3}$, y repitiendo el proceso n veces obtenemos que $m^{-1}m'-1 \in \mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1}$, por lo que $m^{-1}m' \in \mathcal{M}_{p,2n+1}(G)$, con lo que se sigue inmediatamente que λ está bien definida.

Además, como cada L_j es cerrado para productos por elementos de $\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}$, se tiene que, dados $m_1, m_2 \in \mathcal{M}_{p,n}(G)$, $l_1, l_2 \in L_n$, vale

$$(m_1+l_1)(m_2+l_2) = m_1m_2 + \underbrace{(m_1-1)l_2 + l_1(m_2-1) + l_1 + l_2 + l_1l_2}_{l'} = m_1m_2 + l',$$

donde claramente $l' \in L_n$; esto prueba que λ es un homomorfismo. Además es evidente que λ es suprayectivo. Por otro lado, se tiene que

$$\mathrm{Ker}(\lambda) = \left\{ m + l_n + \mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1} \in \frac{\mathcal{M}_{p,n}(G) + L_n}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1}} \ : \ m \in \mathcal{M}_{p,2n+1}(G) \right\}$$

$$= \frac{\mathcal{M}_{p,2n+1}(G) + L_n}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1}} = \frac{\mathcal{M}_{p,2n+1}(G) - 1 + 1 + L_n}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1}} = \frac{1 + L_n}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1}},$$

donde, en la última igualdad la inclusión hacia la derecha se tiene por ser $\mathcal{M}_{p,2n+1}(G) - 1 \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1} \subseteq L_n$.

En definitiva, todo esto demuestra que λ induce un isomorfismo como en (4.9).

Con todo esto, ya podemos probar el teorema. Sea H otro grupo tal que $\mathbb{F}_p[G] \cong \mathbb{F}_p[H]$, digamos que mediante un isomorfismo θ que podemos suponer normalizado. Ahora, si aplicamos θ a la ecuación (4.7) obtenemos que

$$\frac{\theta(L_j)}{\mathrm{Aug}_{\mathbb{F}_p}(H)^{n+j+2}} = \frac{I_{\mathbb{F}_p,n+j+1}(H)}{\mathrm{Aug}_{\mathbb{F}_p}(H)^{n+j+2}} \oplus \frac{\theta(L_{j+1})}{\mathrm{Aug}_{\mathbb{F}_p}(H)^{n+j+2}},$$

que no es más que la versión de dicha ecuación para H; así, de los razonamientos hechos hasta ahora (i.e., los de las dos afirmaciones) se deduce que

$$\frac{\mathcal{M}_{p,n}(H)}{\mathcal{M}_{p,2n+1}(H)} \cong \frac{\left(\frac{\mathcal{M}_{p,n}(H)+\mathrm{Aug}_{\mathbb{F}_p}(H)^{n+1}}{\mathrm{Aug}_{\mathbb{F}_p}(H)^{2n+1}}\right)}{\left(\frac{(1+\theta(L_n))}{\mathrm{Aug}_{\mathbb{F}_p}(H)^{2n+1}}\right)},$$

donde el último cociente no es más que la imagen isomórfica por θ (se ve inmediatamente notando que el 'numerador del numerador' no es más que $I_{\mathbb{F}_p,n}(H)+1$, y por tanto está determinado por el álgebra de grupo) de

$$\frac{\left(\frac{\mathcal{M}_{p,n}(G)+\mathrm{Aug}_{\mathbb{F}_p}(G)^{n+1}}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1}}\right)}{\left(\frac{(1+L_n)}{\mathrm{Aug}_{\mathbb{F}_p}(G)^{2n+1}}\right)} \cong \frac{\mathcal{M}_{p,n}(G)}{\mathcal{M}_{p,2n+1}(G)},$$

y el teorema se sigue.

□

Corolario 4.3.5. *Sea G un p-grupo finito cuya $\mathcal{M}$-serie tiene longitud $\ell \leq 2$. Entonces la clase de isomorfía de G está determinada por su álgebra de grupo modular $\mathbb{F}_p[G]$.*

Demostración. Basta notar que si $\mathcal{M}_{p,3}(G) = \{1\}$, por cualquiera de los dos teoremas anteriores la clase de isomorfía del cociente $G/\mathcal{M}_{p,3}(G) \cong G$ está determinada por $\mathbb{F}_p[G]$. □

En particular, el corolario anterior da solución positiva a **(MIP)** para la siguiente clase de p-grupos:

Corolario 4.3.6. *Sea G un p-grupo finito con clase de nilpotencia 2 y exponente p. Entonces la clase de isomorfía de G está determinada por su álgebra de grupo modular $\mathbb{F}_p[G]$.*

Demostración. Sea G un grupo en las condiciones del enunciado. Entonces, recordando la Observación 1.3.5 el tercer término de la $\mathcal{M}$-serie de G viene dado por

$$\begin{aligned} \mathcal{M}_{2,3}(G) &= G^{(4)}\gamma_2(G)^{(2)}\gamma_3(G); \\ \mathcal{M}_{p,3}(G) &= G^{(p)}\gamma_3(G), \qquad \text{para } p > 2. \end{aligned}$$

Es obvio que en las condiciones del enunciando estos subgrupos son triviales, con los que el resultado se sigue del Corolario 4.3.5. □

Otro cociente de la serie de Brauer-Jennings-Zassenhaus

Terminamos el estudio sobre la determinación de los cocientes de la serie de Brauer-Jennings-Zassenhaus por $\mathbb{F}_p[G]$ con el siguiente teorema de Hertweck (vid. [19]) que, a diferencia de los anteriores, involucra al grupo de las unidades normalizadas de $\mathbb{F}_p[G]$ y hace uso de bases de Jennings. Será útil tener en mente las identidades módulo $\mathrm{Aug}_{\mathbb{F}_p}(G)^4$ que listamos en el próximo lema:

Lema 4.3.7. Sea G un p-grupo finito, $g, h \in G$ y $x, y, x_1, \ldots, x_m \in \mathcal{M}_{p,2}(G)$. Valen:

(I) $x_1 \ldots x_n - 1 \equiv (x_1 - 1) + \cdots + (x_m - 1) \mod \mathrm{Aug}_{\mathbb{F}_p}(G)^4$;

(II) $(g,h) - 1 \equiv 1 - (h,g) \mod \mathrm{Aug}_{\mathbb{F}_p}(G)^4$;

(III) $(x,h) - 1 \equiv (x-1)(h-1) - (h-1)(x-1) \mod \mathrm{Aug}_{\mathbb{F}_p}(G)^4$;

(IV) $(xy,h) - 1 \equiv (x,h) - 1 + (y,h) - 1 \mod \mathrm{Aug}_{\mathbb{F}_p}(G)^4$.

Demostración. En primer lugar, recordemos las identidades

$$gh - 1 = (g-1) + (h-1) + (g-1)(h-1) \tag{4.10}$$

$$hg((g,h) - 1) = (g-1)(h-1) - (h-1)(g-1). \tag{4.11}$$

(I) No es más que una versión débil de la primera afirmación del Lema 3.4.6 con $N = \mathcal{M}_{p,2}(G)$.

(II) Basta notar que como $(g,h) \in \mathcal{M}_{p,2}(G)$, por (4.10) vale

$$(g,h) - 1 + (h,g) - 1 = -((g,h) - 1)((h,g) - 1) \in \mathrm{Aug}_{\mathbb{F}_p}(G)^4.$$

(III) Por (4.11) obtenemos que

$$(x-1)(h-1) - (h-1)(x-1) = hx((x,h) - 1) = (hx - 1)((x,h) - 1) + (x,h) - 1,$$

donde $(hx-1)((x,h)-1) \in \mathrm{Aug}_{\mathbb{F}_p}(G)^4$, dado que $(x,h) \in \mathcal{M}_{p,3}(G)$.

(IV) Por (III) se tiene que

$$(xy,h)-1 \equiv (xy-1)(h-1)-(h-1)(xy-1) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4$$

(por (4.11))

$$\equiv (x-1)(h-1)+(y-1)(h-1)-(h-1)(x-1)-(h-1)(y-1) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4$$

(de nuevo por (III))

$$\equiv (x,h)-1+(y,h)-1 \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4.$$

□

Lema 4.3.8. Sea G un p-grupo finito, $\mathbb{F}_p[G]$ su álgebra de grupo modular, y $x_1,\dots,x_m \in G$. Escribamos $c_{ij} = (x_j,x_i)$. Escribamos también, por abreviar, $X_i = (x_i-1)$ y $C_{ij} = (c_{ij}-1)$. Entonces, para cada terna de índices i,j,k:

(I) Vale

$$C_{ij}^{x_k} \equiv C_{ij} - ((c_{ki},x_j)-1) + ((c_{kj},x_i)-1) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4.$$

(II) Se tiene que

$$(X_iX_j)^{x_k} \equiv X_iX_j + X_iC_{kj} + X_jC_{ki} + ((c_{ki},x_j)-1) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4.$$

(III) En particular,

$$(X_i^2)^{x_k} \equiv X_i^2 + 2X_iC_{ki} + ((c_{ki},x_i)-1) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4.$$

(IV) Supongamos ahora que p es impar. Vale la identidad:

$$\left(X_iX_j+\frac{1}{2}C_{ij}\right)^{x_k} \equiv \left(X_iX_j+\frac{1}{2}C_{ij}\right) + X_iC_{kj} + X_jC_{ki} + \frac{1}{2}((c_{kj},x_i)-1) + \frac{1}{2}((c_{ki},x_j)-1) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4,$$

(V) Asumimos de nuevo que p es impar, y supongamos que para ciertos índices i,j,k fijados se verifica que $c_{kj} = b_1^{a_1}\dots b_m^{a_m}$, con $b_s \in \mathcal{M}_{p,2}(G)$ y $0 \le a_s < p$ para cada s. Escribamos $B_s = (b_s-1)$. Entonces

$$X_iC_{kj} \equiv a_1X_iB_1 + a_2X_iB_2 + \dots + a_mX_iB_m \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4,$$

y

$$\frac{1}{2}((c_{kj},x_i)-1) \equiv \sum_{s=1}^{m} a_s\frac{1}{2}((b_s,x_i)-1) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4.$$

Demostración. En primer lugar, son de comprobación directa las igualdades

$$C_{ij}^{x_k} = (x_j^{-1}x_i^{-1}x_jx_i-1)^{x_k} = c_{kj}^{-1}x_j^{-1}c_{ki}^{-1}x_i^{-1}x_jc_{kj}x_ic_{ki}-1$$

$$= c_{kj}^{-1}(x_j,c_{ki})c_{ki}^{-1}(x_j,x_i)c_{kj}(c_{kj},x_i)c_{ki}-1$$

(notando que todos los factores de la expresión anterior están en $\mathcal{M}_{p,2}(G)$, y aplicando el primer apartado del lema anterior)

$$\equiv (c_{kj}^{-1}-1)+((x_j,c_{ki})-1)+(c_{ki}^{-1}-1)+(c_{ij}-1)+(c_{kj}-1)+((c_{kj},x_i)-1)+(c_{ki}-1) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4$$

(aplicando el mismo apartado, ahora en sentido inverso, a las parejas de sumandos primero y quinto, y tercero y último)

$$\equiv ((x_j, c_{ki}) - 1) + (c_{ij} - 1) + ((c_{kj}, x_i) - 1) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4.$$

En resumen, y aplicando el apartado (IV) del lema anterior al primer sumando, hemos probado el primer apartado:

$$C_{ij}^{x_k} \equiv C_{ij} - ((c_{ki}, x_j) - 1) + ((c_{kj}, x_i) - 1) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4.$$

Ahora, usando la identidad (4.10) vale

$$(X_iX_j)^{x_k} = (x_ic_{ki} - 1)(x_jc_{kj} - 1) = (X_i + C_{ki} + X_iC_{ki})(X_j + C_{kj} + X_jC_{kj})$$
$$\equiv (X_i + C_{ki})(X_j + C_{kj}) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4$$

y por el apartado (III) del lema anterior

$$C_{ki}X_j \equiv X_jC_{ki} + ((c_{ki}, x_j) - 1) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4;$$

uniendo ambas expresiones, se deduce que

$$(X_iX_j)^{x_k} \equiv X_iX_j + X_iC_{kj} + X_jC_{ki} + ((c_{li}, x_j) - 1) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4,$$

y el segundo apartado queda probado. Poniendo en esta expresión $i = j$, también obtenemos el tercero. Supongamos ahora que p es impar. Entonces

$$\left(X_iX_j + \frac{1}{2}C_{ij}\right)^{x_k} = (X_iX_j)^{x_k} + \frac{1}{2}C_{ij}^{x_k},$$

y aplicando los dos primeros apartados se desprende el cuarto.

Finalmente, asumamos las hipótesis del quinto apartado. La primera identidad se sigue directamente de (I) del Lema 4.3.7, y la segunda de aplicar m veces (IV) del mismo lema.

□

Ya estamos casi en condiciones de dar el teorema, a falta del siguiente:

Lema 4.3.9. Sea G un p-grupo finito, S un subespacio multiplicativamente cerrado de $\mathrm{Aug}_{\mathbb{F}_p}(G)$, y $n \geq 1$ un entero. Supongamos que

$$S \cap I_{\mathbb{F}_p,i}(G) \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^{i+1} \tag{4.12}$$

para cada $i < n$. Entonces:

(I) $G \cap (1 + S) \leq \mathcal{M}_{p,n}(G)$.

(II) Si además H es otro p-grupo finito, y $\theta : \mathbb{F}_p[G] \to \mathbb{F}_p[H]$ es un isomorfismo normalizado, se tiene que

$$H \cap \theta(1 + S) \leq \mathcal{M}_{p,n}(H).$$

Demostración.

(I) Como por el Lema 3.3.5 sabemos que $G \cap (1 + S)$ es un grupo, basta probar la inclusión. Sea $g \in G \cap (1 + S)$. Entonces $g \in G \cap (1 + \mathrm{Aug}_{\mathbb{F}_p}(G)) = \mathcal{M}_{p,1}(G)$.

Notemos que si en estas condiciones $g \in \mathcal{M}_{p,i}(G)$, e $i < n$, con la ayuda del Corolario 3.4.12 se deduce que

$$g - 1 \in S \cap I_{\mathbb{F}_p,i}(G) \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^{i+1},$$

es decir, que $g \in \mathcal{M}_{p,i+1}(G)$. Aplicando a g este argumento n veces se deduce que $g \in \mathcal{M}_{p,n}(G)$, y hemos terminado.

(II) Aplicando θ a la ecuación (4.12), y teniendo en cuenta que tanto las potencias del ideal de aumento como los ideales de Zassenhaus están determinados por $\mathbb{F}_p[G]$, se tiene que

$$\theta(S) \cap I_{\mathbb{F}_{p,i}}(H) \subseteq \mathrm{Aug}_{\mathbb{F}_p}(H)^{i+1},$$

para cada $i < n$, y el resultado se sigue del apartado anterior.

□

Teorema 4.3.10 (Hertweck)**.** *Sean p un primo impar y G un p-grupo finito. Existe un subgrupo normal N de $V(\mathbb{F}_p[G])$ tal que*

$$\frac{V(\mathbb{F}_p[H])}{\theta(N)} \cong \frac{G}{\mathcal{M}_{p,4}(G)}$$

para cada grupo H tal que $K[G] \cong K[H]$, y cada isomorfismo normalizado $\theta : K[G] \to K[H]$. En particular, la clase de isomorfía del cociente $G/\mathcal{M}_{p,4}(G)$ está determinada por el álgebra de grupo modular $\mathbb{F}_p[G]$.

Demostración. Sea

$$x_1, \ldots, x_r, y_1, \ldots, y_s, z_1, \ldots, z_t, w_1, \ldots, w_u \tag{4.13}$$

un sistema de generadores de G elegidos como en el Lema 3.2.3 a partir de un refinamiento a serie de composición de la $\mathcal{M}$-serie de Brauer-Jennings-Zassenhaus (ver Sección 3.2); es claro que podemos renombrarlos de forma que:

$$\begin{array}{rcc} \{x_1, \ldots, x_r\} & \subseteq & G \setminus \mathcal{M}_{p,2}(G), \\ \{y_1, \ldots, y_s\} & \subseteq & \mathcal{M}_{p,2}(G) \setminus \mathcal{M}_{p,3}(G), \\ \{z_1, \ldots, z_t\} & \subseteq & \mathcal{M}_{p,3}(G) \setminus \mathcal{M}_{p,4}(G), \\ \{w_1, \ldots, w_u\} & \subseteq & \mathcal{M}_{p,4}(G). \end{array}$$

Notemos que es posible que la serie se "estanque". Si, por ejemplo, $\mathcal{M}_{p,3}(G) = \mathcal{M}_{p,4}(G)$, ponemos $t = 0$ y $\{z_1, \ldots, z_t\} = \emptyset$. Por definición, los generadores dados dan lugar a una base Jennings $\mathscr{B}$ de $\mathbb{F}_p[G]$. Escribamos

$$\mathcal{X}_* = \{(x_1 - 1), \ldots, (x_r - 1)\}, \qquad \mathcal{Y}_* = \{(y_1 - 1), \ldots, (y_s - 1)\},$$

$$\mathcal{Z}_* = \{(z_1 - 1), \ldots, (z_t - 1)\}, \qquad \mathcal{X}_*^2 = \{(x_1 - 1)^2, \ldots, (x_r - 1)^2\},$$

$$\mathcal{X}_{**} = \{(x_i - 1)(x_j - 1) \ : \ 1 \leq i < j \leq r\},$$

$$\mathcal{X}_*\mathcal{Y}_* = \{(x_i - 1)(y_j - 1) \ : \ 1 \leq i \leq r, \ 1 \leq j \leq s\},$$

$$\mathcal{X}_{***} = \{(x_i - 1)(x_j - 1)(x_k - 1) \ : \ 1 \leq i \leq j \leq k \leq r, \ \text{ si } p = 3, \text{ no } i = j = k\},$$

Es claro que los elementos de $\mathscr{B}$ de peso 1 son los de $\mathcal{X}_*$; los de peso 2, los de $\mathcal{Y}_* \cup \mathcal{X}_{**} \cup \mathcal{X}_*^2$; y finalmente se ve que los de peso 3 son los elementos de $\mathcal{Z}_* \cup \mathcal{X}_*\mathcal{Y}_* \cup \mathcal{X}_{***}$. Sea también $\mathcal{W}$ el conjunto de los elementos de $\mathscr{B}$ con peso mayor que 3; entonces por el Lema 3.2.5 $\mathcal{W}$ forma una base de $\mathrm{Aug}_{\mathbb{F}_p}(G)^4$. Escribamos ahora

$$(\mathcal{X}_{**})' = \left\{(x_i - 1)(x_j - 1) + \frac{1}{2}((x_j, x_i) - 1) \ : \ 1 \leq i < j \leq r\right\}$$

$$(\mathcal{X}_*\mathcal{Y}_*)' = \left\{(x_i - 1)(y_j - 1) + \frac{1}{2}((y_j, x_i) - 1) \ : \ 1 \leq i \leq r, \ 1 \leq j \leq r\right\},$$

y denotemos

$$\mathscr{B}' = \{1\} \cup \mathcal{X}_* \cup \mathcal{Y}_* \cup \mathcal{Z}_* \cup \mathcal{X}_*^2 \cup (X_{**})' \cup (X_*\mathcal{Y}_*)' \cup \mathcal{X}_{***} \cup \mathcal{W}.$$

Fijada toda esta notación, para facilitar la lectura dividimos la demostración en cuatro fases:

Fase 1: Se puede comprobar, si asignamos a los elementos de $(\mathcal{X}_{**})'$ peso 2, y a los de $(\mathcal{X}_*\mathcal{Y}_*)'$ peso 3, que $\mathscr{B}'$ es una base adaptada a la filtración de las potencias del ideal de aumento. En efecto, notando que $\mathscr{B}$ es una base de Jennings, y considerando el Lema 3.2.4:

- $\mathcal{X}_*$ claramente genera $\mathrm{Aug}_{\mathbb{F}_p}(G)$ módulo $\mathrm{Aug}_{\mathbb{F}_p}(G)^2$.
- Que $\mathcal{X}_*^2 \cup (\mathcal{X}_{**})' \cup \mathcal{Y}_*$ genera $\mathrm{Aug}_{\mathbb{F}_p}(G)^2$ módulo $\mathrm{Aug}_{\mathbb{F}_p}(G)^3$ se sigue del hecho de que ciertamente $\mathcal{X}_*^2 \cup \mathcal{X}_{**} \cup \mathcal{Y}_*$ lo hace, y de que, como $(x_j, x_i) \in \mathcal{M}_{p,2}(G)$ admite una expresión, salvo un cambio en el orden de los factores, de la forma

  $$(x_j, x_i) = y_1^{\alpha_1} \dots y_s^{\alpha_s} z_1^{\beta_1} \dots z_t^{\beta_t} w_1^{\gamma_1} \dots w_u^{\gamma_u}$$

  para cada elección válida de índices se tiene que por el apartado (I) del Lema 4.3.7 vale:

  $$(x_i - 1)(x_j - 1) + \frac{1}{2}((x_j, x_i) - 1) \equiv (x_i - 1)(x_j - 1) + \frac{1}{2}\sum_{k=1}^{s} \alpha_k (y_k - 1) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^3.$$

- El conjunto de los elementos de peso 3, $\mathcal{Z}_* \cup (\mathcal{X}_*\mathcal{Y}_*)' \cup \mathcal{X}_{***}$ genera $\mathrm{Aug}_{\mathbb{F}_p}(G)^3$ módulo $\mathrm{Aug}_{\mathbb{F}_p}(G)^4$ por hacerlo $\mathcal{Z}_* \cup \mathcal{X}_*\mathcal{Y}_* \cup \mathcal{X}_{***}$. En efecto, como $(y_j, x_i) \in \mathcal{M}_{p,3}(G)$, es (salvo un cambio en el orden de los factores) de la forma

  $$(y_j, x_i) = z_1^{\beta_1} \dots z_t^{\beta_t} w_1^{\gamma_1} \dots w_u^{\gamma_u},$$

  se tiene la identidad, de nuevo por el apartado (I) del Lema 4.3.7:

  $$(x_i - 1)(y_j - 1) + \frac{1}{2}((y_j, x_i) - 1) \equiv (x_i - 1)(y_j - 1) + \frac{1}{2}\sum_{k=1}^{t} \beta_k (z_k - 1) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4.$$

- Los elementos de peso t con $t \geq 4$ son los mismos en $\mathscr{B}$ que en $\mathscr{B}'$, y por tanto generan $\mathrm{Aug}_{\mathbb{F}_p}(G)^t$ módulo $\mathrm{Aug}_{\mathbb{F}_p}(G)^{t+1}$.

Por tanto, podemos aplicar el Corolario 3.3.3 para deducir que $1 + \mathscr{B}' \setminus \{1\}$ es un conjunto generador de $V(\mathbb{F}_p[G])$. Además, como $\mathrm{Aug}_{\mathbb{F}_p}(G)$ es nilpotente, esto también prueba que $\mathscr{B}'$ genera $K[G]$, y como $\mathscr{B}'$ tiene el mismo cardinal que $\mathscr{B}$, y este último conjunto es una base, se desprende que también $\mathscr{B}'$ es una base.

Fase 2: Sea entonces C el subespacio vectorial generado por

$$(\mathcal{X}_{**})' \cup \mathcal{X}_*^2 \cup (\mathcal{X}_*\mathcal{Y}_*)' \cup \mathcal{X}_{***} \cup \mathcal{W};$$

y D el generado por

$$\mathcal{X}_* \cup \mathcal{Y}_* \cup \mathcal{Z}_*.$$

Por la Fase 1 es inmediato que $\mathrm{Aug}_{\mathbb{F}_p}(G) = C \oplus D$; además, como

$$\mathrm{Aug}_{\mathbb{F}_p}(G)^4 \subseteq C \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^2$$

(debiéndose la primera inclusión a que $\mathcal{W} \subseteq C$, y la segunda a que todos los elementos de C' son combinación lineal de elementos de la base de Jennings con peso mayor que 1). De estas inclusiones se deduce que C es multiplicativamente cerrado (pues si los elementos de C están en $\mathrm{Aug}_{\mathbb{F}_p}(G)$, entonces el producto de cada par de ellos está en $\mathrm{Aug}_{\mathbb{F}_p}(G)^4 \subseteq C$). Entonces, el Lema 3.3.5 garantiza que $N = 1 + C$ es un subgrupo de $V(\mathbb{F}_p[G])$. Además, teniendo en cuenta que todos los elementos de $\mathscr{B}' \setminus \{1\}$, excepto algunos de la forma $g - 1$, con $g \in G$, están en C, se deduce que $N \cdot G = V(\mathbb{F}_p[G])$.

Además, para cada $1 \leq i < 4$ se tiene que

$$I_{\mathbb{F}_p,i}(G) = \mathcal{M}_{p,i}(G) - 1 + \mathrm{Aug}_{\mathbb{F}_p}(G)^{i+1} \subseteq D + \mathrm{Aug}_{\mathbb{F}_p}(G)^{i+1},$$

siendo la igualdad el Corolario 3.4.12, y justificándose la inclusión como sigue. Cada $x \in \mathcal{M}_{p,i}(G)$ es de la forma $x = g_1 g_2 \dots g_n$, donde cada $g_j \in \mathcal{M}_{p,i}(G)$ es alguno de los elementos dados en (4.13), de modo que por el Lema 3.4.6:

$$x - 1 \equiv \sum_{j=1}^{n} (g_j - 1) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^{i+1},$$

donde cada $g_j - 1$ o bien está $\mathrm{Aug}_{\mathbb{F}_p}(G)^{i+1}$, o tiene peso i, en cuyo caso está en $\mathcal{X}_* \cup \mathcal{Y}_* \cup \mathcal{Z}_* \subseteq D$.

Por tanto, vale la inclusión

$$C \cap I_{\mathbb{F}_p,i}(G) \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G)^{i+1}. \tag{4.14}$$

para cada $i < 4$. En efecto, si c está en la intersección, por el párrafo anterior se tiene que $c = d + \alpha$, con $d \in D$ y $\alpha \in \mathrm{Aug}_{\mathbb{F}_p}(G)^{i+1}$. Consideremos la expresión en la base $\mathscr{B}'$ del elemento $d = c - \alpha$. Si $i = 1$, los coeficientes de los elementos de $\mathcal{X}_*$ deben ser 0, y por tanto $d \in \mathrm{Aug}_{\mathbb{F}_p}(G)^2$. Similarmente, si $i = 2$, los coeficientes de elementos de $\mathcal{X}_* \cup \mathcal{Y}_*$ han de ser nulos, de modo que $d \in \mathrm{Aug}_{\mathbb{F}_p}(G)^3$. Y $i = 3$ el resultado es trivial, pues $\alpha \in \mathrm{Aug}_{\mathbb{F}_p}(G)^4 \subseteq C$, y por tanto $c = \alpha$.

Así, por la ecuación (4.14), el Lema 4.3.9 da que $N \cap G \leq \mathcal{M}_{p,4}(G)$, mientras que la inclusión recíproca es consecuencia directa de que $\mathcal{M}_{p,4}(G) - 1 \subseteq \mathcal{W} \subseteq C$. En definitiva, hemos probado:

$$N \cdot G = V(\mathbb{F}_p[G]), \qquad N \cap G = \mathcal{M}_{p,4}(G).$$

Fase 3: Dado que $N \cdot G = V(\mathbb{F}_p[G])$, para probar que N es un subgrupo normal de $V(\mathbb{F}_p[G])$ es suficiente probar que es invariante para conjugaciones por elementos de G, y para ver esto es suficiente comprobar que C verifica esta condición. Así que basta comprobarlo para los generadores de C. Fijemos un $x \in G$ cualquiera; para aprovechar la notación del Lema 4.3.8, escribamos $x_{r+1} = x$.

- $(\mathcal{X}_*)^x \subseteq C$. En efecto, por (III) del mencionado lema:

  $$(X_i^2)^{x_{r+1}} \equiv X_i^2 + 2X_i C_{(r+1)i} + ((c_{(r+1)i}, x_i) - 1) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4;$$

  ahora bien, por definición $c_{(r+1)i} \in \mathcal{M}_{p,2}(G)$, de modo que se puede expresar (salvo un cambio de orden de los factores) como

  $$c_{(r+1)i} = y_1^{\alpha_1} \dots y_s^{\alpha_s} z_1^{\beta_1} \dots z_t^{\beta_t} w_1^{\gamma_1} \dots w_u^{\gamma_u}.$$

  Por tanto, (V) del mismo lema permite continuar la expresión anterior con:

  $$\equiv X_i^2 + \sum_{k=1}^{s} 2\alpha_k \left(X_i Y_k + \frac{1}{2}((y_k, x_i) - 1) \right) \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4,$$

  pues los sumandos restantes están en $\mathrm{Aug}_{\mathbb{F}_p}(G)^4$. Por tanto, $(\mathcal{X}_*)^x \in C$.

- De forma completamente análoga, sustituyendo el apartado (III) por el (IV), se prueba que $((\mathcal{X}_*\mathcal{Y}_*)')^x \subseteq C$.

- Finalmente, los elementos η de $(\mathcal{X}_*\mathcal{Y}_*)'$ y de $\mathcal{X}_{***}$ están en $\mathrm{Aug}_{\mathbb{F}_p}(G)^3$, por lo que

  $$\eta^x = x^{-1}\eta x = x^{-1}\eta(x-1) + (x^{-1} - 1)\eta + \eta \equiv \eta \quad \text{mód } \mathrm{Aug}_{\mathbb{F}_p}(G)^4,$$

  de modo que $\eta^x \in C$.

Queda entonces probada la normalidad de N.

Fase 4: Finalmente, sea H otro grupo tal que $\mathbb{F}_p[G] \cong \mathbb{F}_p[H]$, digamos mediante un isomorfismo normalizado θ. Teniendo en cuenta la ecuación (4.14), la segunda parte del Lema 4.3.9 da que $H \cap \theta(N) \leq \mathcal{M}_{p,4}(H)$, mientras que la inclusión recíproca también es evidente, dado que $\mathcal{M}_{p,4}(H) \subseteq 1 + \mathrm{Aug}_{\mathbb{F}_p}(H)^4 \subseteq \theta(N)$, por ser las potencias del ideal de aumento ideales determinados por $\mathbb{F}_p[G]$. Además, es claro que $\theta(N) \cdot H \leq V(\mathbb{F}_p[H])$ y tomando órdenes:

$$|V(\mathbb{F}_p[H])| = |V(\mathbb{F}_p[G])| = |N \cdot G| = \frac{|N| \cdot |G|}{|N \cap G|} = \frac{|N| \cdot |G|}{|\mathcal{M}_{p,4}(G)|}$$

(usando que por el Corolario 4.2.10 el orden de $\mathcal{M}_{p,4}(G)$ está determinado por $\mathbb{F}_p[G]$)

$$= \frac{|\theta(N)| \cdot |H|}{|\mathcal{M}_{p,4}(H)|} = \frac{|\theta(N)| \cdot |H|}{|\theta(N) \cap H|} = |\theta(N) \cdot H|,$$

por lo que ha de verificarse la igualdad. En resumen, hemos probado que:

$$V(\mathbb{F}_p[H]) = \theta(N) \cdot H, \qquad \mathcal{M}_{p,4}(H) = \theta(N) \cap H.$$

Así, si consideramos el homomorfismo natural

$$H \to \frac{V(\mathbb{F}_p[H])}{\theta(N)}$$

i.e., la composición de la inclusión con el homomorfismo canónico en el cociente, por la descomposición anterior es claro que es un epimorfismo, y su núcleo es $H \cap \theta(N) = \mathcal{M}_{p,4}(H)$. Por tanto, induce un isomorfismo

$$\frac{H}{\mathcal{M}_{p,4}(H)} \cong \frac{V(\mathbb{F}_p[H])}{\theta(N)}.$$

Y como θ induce otro isomorfismo

$$\frac{V(\mathbb{F}_p[G])}{N} \cong \frac{V(\mathbb{F}_p[H])}{\theta(N)},$$

la primera afirmación se sigue. Si además consideramos el isomorfismo identidad $i : \mathbb{F}_p[G] \to \mathbb{F}_p[G]$, dicha afirmación da que

$$\frac{G}{\mathcal{M}_{p,4}(G)} \cong \frac{V(\mathbb{F}_p[G])}{N},$$

de modo que componiendo con los isomorfismos anteriores se obtiene también la segunda. □

Corolario 4.3.11. *Sea p un primo impar, y G un p-grupo finito cuya $\mathcal{M}$-serie tiene longitud $\ell \leq 3$. Entonces la clase de isomorfía de G está determinada por su álgebra de grupo modular $\mathbb{F}_p[G]$.*

Demostración. Como la longitud ℓ de la $\mathcal{M}$-serie está determinada por $\mathbb{F}_p[G]$, basta probar el teorema en la clase de los grupos con $\ell \leq 3$. Y si G es un p-grupo finito con $\mathcal{M}_{p,4}(G) = \{1\}$, por el teorema anterior la clase de isomorfía del cociente $G/\mathcal{M}_{p,4}(G) \cong G$ está determinada por $\mathbb{F}_p[G]$. □

La clase de nilpotencia de $G/\Phi(G')$

Sea G un p-grupo finito. En esta subsección, basada en la primera sección de [5], consideraremos la serie de ideales del álgebra grupo $\mathbb{F}_p[G]$ definida recursivamente mediante:

$$\begin{aligned} J_2 &= \mathrm{Aug}_{\mathbb{F}_p}(G, G'), \\ J_k &= J_{k-1}\,\mathrm{Aug}_{\mathbb{F}_p}(G) + \mathrm{Aug}_{\mathbb{F}_p}(G) J_{k-1}, \quad \text{para } k > 2. \end{aligned}$$

Se obtienen fácilmente las caracterizaciones siguientes:

Lema 4.3.12. Sea G un p-grupo finito, y $\{J_k\}_{k\geq 2}$ la serie J. Entonces, para cada $k \geq 2$ vale

$$J_k = \sum_{i=2}^{k} \mathrm{Aug}_{\mathbb{F}_p}(G)^{k-i} \mathrm{Aug}_{\mathbb{F}_p}(\gamma_i(G)),$$

donde $\mathrm{Aug}_{\mathbb{F}_p}(G)^0$ denota a $\mathbb{F}_p[G]$. Por tanto,

$$J_k = \mathrm{Aug}_{\mathbb{F}_p}(G) J_{k-1} + \mathrm{Aug}_{\mathbb{F}_p}(G, \gamma_k(G)).$$

Demostración. Probamos la primera identidad por inducción sobre k. Si $k = 2$ el resultado es evidente, pues $\mathbb{F}_p[G]\,\mathrm{Aug}_{\mathbb{F}_p}(G') = \mathrm{Aug}_{\mathbb{F}_p}(G, G')$. Sea entonces $k > 2$, y supongamos que

$$J_{k-1} = \sum_{i=2}^{k-1} \mathrm{Aug}_{\mathbb{F}_p}(G)^{k-1-i} \mathrm{Aug}_{\mathbb{F}_p}(\gamma_i(G)).$$

Entonces

$$\begin{aligned} J_k &= \sum_{i=2}^{k-1} \mathrm{Aug}_{\mathbb{F}_p}(G)^{k-1-i} \mathrm{Aug}_{\mathbb{F}_p}(\gamma_i(G)) \mathrm{Aug}_{\mathbb{F}_p}(G) + \sum_{i=2}^{k-1} \mathrm{Aug}_{\mathbb{F}_p}(G)^{k-i} \mathrm{Aug}_{\mathbb{F}_p}(\gamma_i(G)) \\ &= \sum_{i=2}^{k-1} \mathrm{Aug}_{\mathbb{F}_p}(G)^{k-1-i} \Big(\mathrm{Aug}_{\mathbb{F}_p}(\gamma_i(G)) \mathrm{Aug}_{\mathbb{F}_p}(G) + \mathrm{Aug}_{\mathbb{F}_p}(G) \mathrm{Aug}_{\mathbb{F}_p}(\gamma_i(G)) \Big) \end{aligned}$$

(usando el Lema 3.4.9)

$$\begin{aligned} &= \sum_{i=2}^{k-1} \mathrm{Aug}_{\mathbb{F}_p}(G)^{k-1-i} \Big(\mathrm{Aug}_{\mathbb{F}_p}(G, \gamma_{i+1}(G)) + \mathrm{Aug}_{\mathbb{F}_p}(G) \mathrm{Aug}_{\mathbb{F}_p}(\gamma_i(G)) \Big) \\ &= \sum_{i=2}^{k-1} \Big(\mathrm{Aug}_{\mathbb{F}_p}(G)^{k-(i+1)} \mathrm{Aug}_{\mathbb{F}_p}(\gamma_{i+1}(G)) + \mathrm{Aug}_{\mathbb{F}_p}(G)^{k-i} \mathrm{Aug}_{\mathbb{F}_p}(\gamma_i(G)) \Big); \end{aligned}$$

así, es claro que para el par de sumandos i-ésimo ($2 \leq i < k-1$) en la expresión anterior, el primero de ellos es precisamente el segundo del par $(i+1)$-ésimo, y por tanto es superfluo. Así, la ecuación anterior puede continuar con:

$$= \sum_{i=2}^{k-1} \mathrm{Aug}_{\mathbb{F}_p}(G)^{k-i} \mathrm{Aug}_{\mathbb{F}_p}(\gamma_k(G)) + \mathrm{Aug}_{\mathbb{F}_p}(G, \gamma_k(G)),$$

y la primera identidad se sigue. Con esto la segunda es trivial, pues:

$$\begin{aligned} J_k &= \sum_{i=2}^{k-1} \mathrm{Aug}_{\mathbb{F}_p}(G)^{k-i} \mathrm{Aug}_{\mathbb{F}_p}(\gamma_k(G)) + \mathrm{Aug}_{\mathbb{F}_p}(G, \gamma_k(G)) \\ &= \mathrm{Aug}_{\mathbb{F}_p}(G) \left(\sum_{i=2}^{k-1} \mathrm{Aug}_{\mathbb{F}_p}(G)^{k-1-i} \mathrm{Aug}_{\mathbb{F}_p}(\gamma_k(G)) \right) + \mathrm{Aug}_{\mathbb{F}_p}(G, \gamma_k(G)) \\ &= \mathrm{Aug}_{\mathbb{F}_p}(G) J_{k-1} + \mathrm{Aug}_{\mathbb{F}_p}(G, \gamma_k(G)). \end{aligned}$$

□

Lema 4.3.13. Sean G un p-grupo finito, $n \geq 2$ un entero, y $\alpha_1, \ldots, \alpha_n \in V(\mathbb{F}_p[G])$. Entonces

$$[\alpha_1, \ldots, \alpha_n] \in J_n, \quad \text{y}$$

$$(\alpha_1, \ldots, \alpha_n) - 1 \equiv [\alpha_1, \ldots, \alpha_n] \mod J_{n+1}.$$

Demostración. Escribamos $\alpha_i = 1 + \beta_i$, con $\beta_i \in \operatorname{Aug}_{\mathbb{F}_p}(G)$ (ver Corolario 3.1.10). Probamos la primera afirmación por inducción sobre n. Si $n = 2$, por el Lema 4.2.3 es claro que $[\alpha_1, \alpha_2] \in \operatorname{Aug}_{\mathbb{F}_p}(G, G') = J_2$. Y, si $n > 2$, suponiendo la propiedad cierta para $n-1$ tenemos que

$$\begin{aligned}[\alpha_1, \dots, \alpha_{n-1}, \alpha_n] &= [\alpha_1, \dots, \alpha_{n-1}]\alpha_n - \alpha_n[\alpha_1, \dots, \alpha_{n-1}] \\ &= [\alpha_1, \dots, \alpha_{n-1}]\beta_n - \beta_n[\alpha_1, \dots, \alpha_{n-1}] \in J_{k-1}\operatorname{Aug}_{\mathbb{F}_p}(G) + \operatorname{Aug}_{\mathbb{F}_p}(G)J_{k-1} = J_k.\end{aligned}$$

Probamos también la segunda afirmación por inducción. Para $n = 2$ vale

$$\begin{aligned}(\alpha_1, \alpha_2) - 1 &= \alpha_1^{-1}\alpha_2^{-1}[\alpha_1, \alpha_2] \\ &= [\alpha_1, \alpha_2] + (\alpha_1^{-1}\alpha_2^{-1} - 1)[\alpha_1, \alpha_2] \\ &\equiv [\alpha_1, \alpha_2] \mod J_3,\end{aligned}$$

donde la equivalencia se obtiene directamente de la última caracterización del Lema 4.3.12. Supongamos la propiedad cierta para $n-1$, con $n > 2$. Entonces existe un $\beta \in J_n$ tal que

$$(\alpha_1, \dots, \alpha_{n-1}) = 1 + [\alpha_1, \dots, \alpha_{n-1}] + \beta,$$

de modo que

$$\begin{aligned}(\alpha_1, \dots, \alpha_n) - 1 &= (\alpha_1, \dots, \alpha_{n-1})^{-1}\alpha_n^{-1}[(\alpha_1, \dots, \alpha_{n-1}), \alpha_n] \\ &= (\alpha_1, \dots, \alpha_{n-1})^{-1}\alpha_n^{-1}[1 + [\alpha_1, \dots, \alpha_{n-1}] + \beta, \alpha_n] \\ &= (\alpha_1, \dots, \alpha_{n-1})^{-1}\alpha_n^{-1}\left([\alpha_1, \dots, \alpha_n] + [\beta, \alpha_n]\right) \\ &= [\alpha_1, \dots, \alpha_n] + [\beta, \alpha_n] + \left((\alpha_1, \dots, \alpha_{n-1})^{-1}\alpha_n^{-1} - 1\right) \cdot \left([\alpha_1, \dots, \alpha_n] + [\beta, \alpha_n]\right) \\ &\equiv [\alpha_1, \dots, \alpha_n] \mod J_{n+1},\end{aligned}$$

teniendo en cuenta que $[\beta, \alpha_n] \in J_{n+1}$, y que $[\alpha_1, \dots, \alpha_n] \in J_n$ junto con la definición de J_{n+1}. □

Proposición 4.3.14. Sea G un p-grupo finito. Entonces los grupos

$$\frac{G}{\Phi(G')} \quad \text{y} \quad \frac{V(\mathbb{F}_p[G])}{1 + \operatorname{Aug}_{\mathbb{F}_p}(G, G')}$$

tienen la misma clase de nilpotencia.

Demostración. Sea c la clase de nilpotencia de $G/\Phi(G')$, es decir, el menor entero c para el que $\gamma_{c+1}(G) \subseteq G'$. Comenzamos notando que

$$\begin{aligned}J_{c+1} &= \sum_{i=2}^{c+1} \operatorname{Aug}_{\mathbb{F}_p}(G)^{c+1-1} \operatorname{Aug}_{\mathbb{F}_p}(\gamma_i(G)) \\ &= \sum_{i=2}^{c} \operatorname{Aug}_{\mathbb{F}_p}(G)^{c+1-1} \operatorname{Aug}_{\mathbb{F}_p}(\gamma_i(G)) + \operatorname{Aug}_{\mathbb{F}_p}(G, \gamma_{c+1}(G)) \\ &\subseteq \operatorname{Aug}_{\mathbb{F}_p}(G) \operatorname{Aug}_{\mathbb{F}_p}(G') + \operatorname{Aug}_{\mathbb{F}_p}(G, \gamma_{c+1}(G));\end{aligned}$$

ahora, observando que

$$\begin{aligned}\operatorname{Aug}_{\mathbb{F}_p}(G, \gamma_{c+1}(G)) \subseteq \operatorname{Aug}_{\mathbb{F}_p}(G, \Phi(G)) = \operatorname{Aug}_{\mathbb{F}_p}(G, \mathcal{M}_{p,2}(G')) \\ \subseteq \operatorname{Aug}_{\mathbb{F}_p}(G, G')^2 \subseteq \operatorname{Aug}_{\mathbb{F}_p}(G) \operatorname{Aug}_{\mathbb{F}_p}(G'),\end{aligned}$$

se deduce que

$$J_{c+1} \subseteq \operatorname{Aug}_{\mathbb{F}_p}(G) \operatorname{Aug}_{\mathbb{F}_p}(G').$$

Entonces, por el Lema 4.3.13. para cada $\alpha_1, \dots, \alpha_{c+1} \in V(\mathbb{F}_p[G])$ se tiene que

$$(\alpha_1, \dots, \alpha_{c+1}) \in 1 + J_{c+1} \subseteq 1 + \operatorname{Aug}_{\mathbb{F}_p}(G) \operatorname{Aug}_{\mathbb{F}_p}(G').$$

Como, por el Lema 1.2.2 los elementos de esta forma generan

$$\gamma_{c+1}\left(\frac{V(\mathbb{F}_p[G])}{1+\mathrm{Aug}_{\mathbb{F}_p}(G,G')}\right) \quad \text{módulo} \quad \gamma_{c+2}\left(\frac{V(\mathbb{F}_p[G])}{1+\mathrm{Aug}_{\mathbb{F}_p}(G,G')}\right),$$

se deduce que estos dos subgrupos han de ser iguales, y por tanto triviales; en consecuencia

$$c\left(\frac{V(\mathbb{F}_p[G])}{1+\mathrm{Aug}_{\mathbb{F}_p}(G,\Phi(G'))}\right) \leq c.$$

Para ver la desigualdad recíproca, consideremos el homomorfismo

$$\iota : G \longrightarrow \frac{V(\mathbb{F}_p[G])}{1+\mathrm{Aug}_{\mathbb{F}_p}(G,G')}$$

que se obtiene componiendo la inclusión en $V(\mathbb{F}_p[G])$ con el homomorfismo canónico en el cociente. Es claro que el núcleo de este homomorfismo es $\mathrm{Ker}(\iota) = G \cap (1+\mathrm{Aug}_{\mathbb{F}_p}(G,G'))$, que por el apartado (IV) de la Proposición 3.4.7 es precisamente $\mathcal{M}_{p,2}(G') = \Phi(G')$. Por tanto, $\mathrm{Im}(\iota)$ es un sugrupo de $\frac{V(\mathbb{F}_p[G])}{1+\mathrm{Aug}_{\mathbb{F}_p}(G,G')}$ isomorfo a $G/\Phi(G')$. Así, el Lema 1.1.13 da que:

$$c = c\left(\mathrm{Im}(\iota)\right) \leq c\left(\frac{V(\mathbb{F}_p[G])}{1+\mathrm{Aug}_{\mathbb{F}_p}(G,\Phi(G'))}\right).$$

□

Corolario 4.3.15. *Sea G un p-grupo finito. Entonces la clase de nilpotencia de $G/\Phi(G')$ está determinada por el álgebra de grupo modular $\mathbb{F}_p[G]$.*

Demostración. Basta notar que tanto el grupo $V(\mathbb{F}_p[G])$ como el ideal $\mathrm{Aug}_{\mathbb{F}_p}(G,G')$ están determinados por $\mathbb{F}_p[G]$, y el resultado se sigue de la proposición anterior. □

En particular, se obtiene que la clase de isomorfismo de un p-grupo finito G está determinado por $\mathbb{F}_p[G]$ en la clase de los p-grupos finitos con subgrupo conmutador abeliano elemental.

El cociente de Sandling

En esta de subsección, denotaremos:

$$J(G) = \mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(G') + \mathrm{Aug}_{\mathbb{F}_p}(G')\,\mathrm{Aug}_{\mathbb{F}_p}(G).$$

Es claro que este ideal se puede reescribir como

$$J(G) = \mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(G,G') + \mathrm{Aug}_{\mathbb{F}_p}(G,G')\,\mathrm{Aug}_{\mathbb{F}_p}(G),$$

y como los ideales $\mathrm{Aug}_{\mathbb{F}_p}(G)$ y $\mathrm{Aug}_{\mathbb{F}_p}(G,G')$ están determinados por $\mathbb{F}_p[G]$, también lo estará $J(G)$.

Lema 4.3.16. Sea G un p-grupo finito; y L un ideal por la izquierda de $\mathrm{Aug}_{\mathbb{F}_p}(G)$. Entonces α y β coinciden módulo L si y sólo si $1+\alpha$, $1+\beta$ están en la misma clase lateral, de entre las determinadas por el subgrupo $1+L$ en el grupo $V(\mathbb{F}_p[G])$. Formalmente:

$$\alpha + L = \beta + L \qquad \Leftrightarrow \qquad (1+\alpha)(1+L) = (1+\beta)(1+L).$$

Demostración. Si $\alpha - \beta = \lambda \in L$, entonces

$$1+\alpha = 1+\beta+\lambda = (1+\beta)(1+(1+\beta)^{-1}\lambda),$$

donde $(1+\beta)^{-1}\lambda \in L$. Recíprocamente, si $(1+\alpha) = (1+\beta)(1+\lambda)$, entonces $\alpha = \beta + (1+\beta)\lambda$. □

Lema 4.3.17. Sea G un p-grupo finito y $J(G)$ el ideal de arriba. Entonces:

(I) $J(G) = \mathrm{Aug}_{\mathbb{F}_p}(G, \gamma_3(G)) + \mathrm{Aug}_{\mathbb{F}_p}(G') \mathrm{Aug}_{\mathbb{F}_p}(G)$;

(II) $G \cap (1 + J(G)) = \gamma_2(G)^{(p)}\gamma_3(G)$.

(III) $1 + \mathrm{Aug}_{\mathbb{F}_p}(G, G') = G'(1 + J(G))$.

Demostración.

(I) No es más que el caso $k = 2$ del Lema 3.4.9. También se ve claramente notando que $J(G)$ coincide con el ideal J_3 de la sección anterior, y aplicar el Lema 4.3.12 .

(II) No es más que la primera parte del apartado (IV) de la Proposición 3.4.7 con $N = G'$.

(III) Por el apartado (II) de la misma proposición, con $N = G'$, tenemos que

$$1 + \mathrm{Aug}_{\mathbb{F}_p}(G, G') = G'(1 + \mathrm{Aug}_{\mathbb{F}_p}(G') \mathrm{Aug}_{\mathbb{F}_p}(G)) \subseteq G'(1 + J(G)),$$

donde la inclusión es trivial. Por tanto, será suficiente probar

$$G'(1 + J(G)) \subseteq 1 + \mathrm{Aug}_{\mathbb{F}_p}(G, G'),$$

y esto es directo, pues si $g(1 + \alpha) \in G'(1 + J(G))$, con $g \in G'$ y $\alpha \in J(G)$, es claro que

$$g(1 + \alpha) = 1 + (g - 1) + g\alpha \in 1 + \mathrm{Aug}_{\mathbb{F}_p}(G, G').$$

□

Lema 4.3.18. Sea G un p-grupo finito. Entonces:

(I) Es central el ideal

$$\frac{\mathrm{Aug}_{\mathbb{F}_p}(G)^2}{J(G)} \subseteq \mathcal{Z}\left(\frac{\mathbb{F}_p[G]}{J(G)}\right).$$

(II) Es central el subgrupo

$$\frac{1 + \mathrm{Aug}_{\mathbb{F}_p}(G)^2}{1 + J(G)} \subseteq \mathcal{Z}\left(\frac{V(\mathbb{F}_p[G])}{1 + J(G)}\right).$$

Como consecuencia, dados un entero $n \geq 1$ y $\alpha, \beta \in \mathrm{Aug}_{\mathbb{F}_p}(G)$, se tiene que

$$(\alpha\beta)^n \equiv \alpha^n\beta^n \mod J(G).$$

Demostración.

(I) Basta probar que los elementos de $\mathrm{Aug}_{\mathbb{F}_p}(G)^2$ conmutan con los elementos de G módulo J. Sean $x, y, g \in G$, entonces, como

$$(x(x, g) - 1) = (x - 1)((x, g) - 1) + x - 1 + (x, g) - 1 \equiv x - 1 + (x, g) - 1 \mod J(G),$$

$$(y(y, g) - 1) = (y - 1)((y, g) - 1) + y - 1 + (y, g) - 1 \equiv y - 1 + (y, g) - 1 \mod J(G),$$

se deduce se deduce inmediatamente que

$$\begin{aligned}((x - 1)(y - 1))^g &= (x^g - 1)(y^g - 1)\\ &= (x(x, g) - 1)(y(y, g) - 1)\\ &\equiv (x - 1)(y - 1) \mod J(G).\end{aligned}$$

(II) Se sigue inmediatamente del punto anterior y del Lema 4.3.16.

La última afirmación se obtiene directamente por inducción usando el primer punto: para $n = 1$ es trivial; y si $(\alpha\beta)^n = \alpha^n\beta^n + \chi$, con $\chi \in J(G)$, se tiene que

$$\begin{aligned}(\alpha\beta)^{n+1} &= \alpha\beta(\alpha\beta)^n \\ &= \alpha\beta\alpha^n\beta^n + \alpha\beta\chi \\ &= \alpha(\alpha^n\beta + [\beta, \alpha^n])\beta^n + \alpha\beta\chi \\ &= \alpha^{n+1}\beta^{n+1} + \alpha[\beta, \alpha^n]\beta^n + \alpha\beta\chi\end{aligned}$$

y el resultado se sigue notando que $[\beta, \alpha^n] \in [\mathbb{F}_p[G], \mathbb{F}_p[G]] \subseteq \mathrm{Aug}_{\mathbb{F}_p}(G, G')$, y por tanto

$$\alpha[\beta, \alpha^n]\beta^n + \alpha\beta\chi \in J(G).$$

□

Lema 4.3.19. Sea G un p-grupo abeliano con base $\{x_1, \ldots, x_d\}$. Sean $a_1, \ldots, a_d$ enteros no negativos, no todos nulos. Supongamos además que para cada j, $a_j \leq o(x_j)$. Si $a_j \neq 0$, sea definamos s_j como la mayor potencia de p menor o igual que a_j. Entonces el orden del elemento

$$1 + \eta(a_1, \ldots, a_n) = 1 + \prod_{j=1}^{d}(x_j - 1)^{a_j}$$

en el grupo de las unidades $V(\mathbb{F}_p[G])$ es $\min\{o(x_j)/s_j \ : \ a_j \neq 0\}$.

Demostración. Sea $q_j = o(x_j)$. Podemos suponer que $0 < a_j < q_j$ para cada j, de modo que será $\eta(a_1, \ldots, a_n) \neq 0$. Probaremos el resultado por inducción sobre $\exp(G)$. El lema es inmediato si G es abeliano elemental, pues si q_t/s_t es el mínimo del enunciado, sería

$$(1 + \eta(a_1, \ldots, a_d))^{q_t/s_t} = 1 + \prod_{j=1}^{d}(x_j - 1)^{a_j q_t/s_t}$$

$$= 1 + \underbrace{(x_t - 1)^{q_t}}_{0}(x_t - 1)^{(a_t - s_t)q_t/s_t} \prod_{j \neq t}(x_j - 1)^{a_j q_j/s_j} = 1;$$

como se comprueba fácilmente que para ningún exponente menor ninguno de los productos se anula, ya tenemos el caso $\exp(G) = 1$.

Supongamos ahora que $\exp(G) > 1$. Si fuese $a_t \geq q_t/p$ para algún t,

$$(1 + \eta(a_1, \ldots, a_d))^p = 1 + \eta(a_1, \ldots, a_d)^p = 1 + \prod_{j=1}^{d}(x_j - 1)^{a_j p}$$

$$= 1 + \underbrace{(x_t - 1)^{q_t}}_{0}(x_t - 1)^{a_t p - q_t} \prod_{j \neq t}(x_j - 1)^{a_j p} = 1,$$

por lo que el orden buscado es p; además, es claro que por ser $q_t/p \leq a_t < q_t$ será $s_t = q_t/p$, y por tanto el mínimo del enunciado también será $q_t/s_t = p$; esto prueba el lema en este caso.

Finalmente, supongamos que $a_j \leq q_j/p$ para cada j; escribimos

$$(1 + \eta(a_1, \ldots, a_d))^p = 1 + \tilde{\eta}(a_1, \ldots, a_d)^p$$

$$= 1 + \prod_{j=1}^{d}(x_j^p - 1)^{a_j} = 1 + \tilde{\eta}(a_1, \ldots, a_d),$$

donde $\tilde{\eta}(a_1,\ldots,a_d) = \prod_{j=1}^{d}(x_j^p-1)^{a_j}$ es el análogo a $\eta(a_1,\ldots,a_d)$ para el grupo $G^{(p)}$, con el subconjunto $\{x_1^p,\ldots,x_d^p\}$ como base. Es claro que $\exp(G^{(p)}) = \exp(G)-1$, de modo que por la hipótesis de inducción

$$o(1+\tilde{\eta}(a_1,\ldots,a_d)) = \text{mín}\{o(x_j^p)/s_j\} = \text{mín}\{q_j/s_j\}/p,$$

y por tanto

$$o(1+\eta(a_1,\ldots,a_d)) = \text{mín}\{q_j/s_j\},$$

lo que completa el paso inductivo.

□

Fijamos más notación para lo que resta de subsección. Sea G un p-grupo finito. Sea $\{x_1,\ldots,x_d\}$ un conjunto de generadores de tamaño mínimo de G. Para cada d-tupla de números enteros no negativos $a=(a_1,\ldots,a_d)$, no todos nulos, definimos:

$$\eta(a) = \prod_{j=1}^{d}(x_j-1)^{a_j}.$$

Recordamos la notación:

$$D_0(G) = \{a\in\mathbb{N}^n \ : \ 0\le a_i < o(x_i) \text{ para cada } i, \text{ y } p\nmid a_i \text{ para algún } i\},$$

y escribimos además

$$D_1(G) = \{a\in D_0(G) \ : \ \sum_{i=1}^{d} a_i > 1\}.$$

Denotamos por $W(G)$ al subgrupo de $V(\mathbb{F}_p[G])$ generado por el conjunto:

$$\{\eta(a) \ : \ a\in D_1(G)\}\cup(1+J(G)).$$

Denotemos con una barra a la proyección $\rho_{G'}$ de G a G', así como al epimorfismo inducido de $\mathbb{F}_p[G]$ a $\mathbb{F}_p[G']$. Escribimos entonces

$$\overline{\eta}(a) = \overline{\eta(a)} = \prod_{j=1}^{d}(\overline{x_j}-1)^{a_j}.$$

Observación 4.3.20. Es claro que $\{\overline{x_1},\ldots,\overline{x_d}\}$ es una base de $\overline{G}$. Así, como por definición es evidente que $\overline{1+J(G)} = \overline{1}$, se deduce que $\overline{W(G)} = W(\overline{G})$ es precisamente el subgrupo de $V(\mathbb{F}_p[\overline{G}])$ generado por los $1+\overline{\eta}(a_1,\ldots,a_d)$, con $(a_1,\ldots,a_d)\in D_1(\overline{G})$. Y como estos elementos, junto con $\{\overline{x_1},\ldots,\overline{x_d}\}$, forman una base de $V(\mathbb{F}_p[G])$ por el Teorema 3.3.8, tenemos que

$$V(\mathbb{F}_p[\overline{G}]) = W(\overline{G})\oplus\overline{G}.$$

Observación 4.3.21. También conviene notar que, como $W(G)\le 1+\text{Aug}_{\mathbb{F}_p}(G)^2$, el Lema 4.3.18 garantiza que $W(G)$ es normal en $V(\mathbb{F}_p[G])$. En efecto, si $\alpha\in W(G)$ y $x\in V(\mathbb{F}_p[G])$, por el mencionado lema x conmuta con α salvo un factor $\beta\in 1+J(G)\subseteq W(G)$, por lo que

$$\alpha^x = x^{-1}\alpha x = x^{-1}x\alpha\beta = \alpha\beta\in W(G).$$

Lema 4.3.22. Con la notación anterior, $W(G)\cap(1+\text{Aug}_{\mathbb{F}_p}(G,G')) = 1+J(G)$.

Demostración. Por el tercer apartado del Lema 4.3.17 vale $1 + \mathrm{Aug}_{\mathbb{F}_p}(G, G') = G'(1 + J(G))$, y como $1 + J(G) \subseteq W(G)$, es inmediata la inclusión

$$W(G) \cap (1 + \mathrm{Aug}_{\mathbb{F}_p}(G, G')) \supseteq 1 + J(G).$$

Y para ver la recíproca, basta comprobar que cada producto $\prod_{a \in D_1(G)}(1 + \eta(a))^{m_a}$ que esté en $1 + \mathrm{Aug}_{\mathbb{F}_p}(G, G')$ ha de estar también en $1 + J(G)$. Como la proyección $\prod_{a \in D_1(G)}(1 + \overline{\eta}(a))^{m_a}$ en $V(\mathbb{F}_p[\overline{G}])$ es necesariamente 1, se sigue del hecho de que los $1 + \bar{\eta}(a)$ formen una base que $o(1 + \overline{\eta}(a))$ divide a m_a para cada a. Así, fijo a, el Lema 4.3.19 garantiza que existe un índice i y alguna potencia q de p tales que $q = o(x_i)/s_i = o(1 + \bar{\eta}(a))$ divide a m_a, con $0 < s_i \leq a_i$. Por la última afirmación del Lema 4.3.18 se tiene que

$$\eta(a)^q \equiv \eta(qa) \quad \text{mód } J(G),$$

siendo $qa = (qa_1, qa_2, \ldots, qa_d)$; en consecuencia, por el Lema 4.3.16,

$$(1 + \eta(a))^q \equiv 1 + \eta(qa) \quad \text{mód } 1 + J(G).$$

Como $(\overline{x_i} - 1)^{qa_i} = 0$ en $\mathbb{F}_p[\overline{G}]$, se tiene que $(x_i - 1)^{qa_i} \in \mathrm{Aug}_{\mathbb{F}_p}(G, G')$. Distinguimos dos casos:

- Si existe algún $j \neq i$ tal que $a_j \neq 0$, entonces $\eta(qa)$ está o bien en $\mathrm{Aug}_{\mathbb{F}_p}(G)\,\mathrm{Aug}_{\mathbb{F}_p}(G')$ o bien en $\mathrm{Aug}_{\mathbb{F}_p}(G')\,\mathrm{Aug}_{\mathbb{F}_p}(G)$. Esto prueba que $(1 + \eta(a))^q \in 1 + J(G)$.
- Si $a_i = 0$ para cada $i \neq 0$, entonces a_i no es una potencia de p por definición de $D(\overline{G})$. Por tanto, $(x_i - 1)^{qa_i} \in \mathrm{Aug}_{\mathbb{F}_p}(G, G')^2 \subseteq 1 + J(G)$, y de nuevo $(1 + \eta(a))^q \in 1 + J(G)$.

Como $q | m_a$, se sigue que $(1 + \eta(a))^{m_a}$ está en $1 + J(G)$, y como el razonamiento es válido para cada $a \in D_1(G)$, se deduce que también lo está el producto $\prod_{a \in D_1(G)}(1 + \eta(a))^{m_a}$.

□

Teorema 4.3.23 (Sandling)**.** *Sea G un p-grupo finito. Entonces $V(\mathbb{F}_p[G]) = G \cdot W(G)$, y $G \cap W(G) = \gamma_2(G)^{(p)}\gamma_3(G)$. Además, hay un isomorfismo de grupos*

$$\frac{V(\mathbb{F}_p[G])}{1 + J(G)} \cong \frac{G}{\gamma_2(G)^{(p)}\gamma_3(G)} \oplus W\left(G/G'\right).$$

Demostración. Como siempre, denotamos la proyección en $\overline{G} = G/G'$ con una barra arriba. Por la Observación 4.3.21 sabemos que $V(\mathbb{F}_p[\overline{G}]) = \overline{G} \cdot W(\overline{G})$, de modo que

$$V(\mathbb{F}_p[G]) = G \cdot W(G) \cdot (1 + \mathrm{Aug}_{\mathbb{F}_p}(G, G')) = G \cdot W(G) \cdot G'(1 + J(G)) = G \cdot W(G),$$

(siguiéndose la primera igualdad de lo anterior y el Corolario 3.3.7, la segunda del tercer apartado del Lema 4.3.17, y la última se deduce directamente del Lema 4.3.22); así, queda probada la primera afirmación. Para la segunda, hay que notar que, como $\overline{G} \cap W(\overline{G}) = \{1\}$, se tiene que $G \cap W(G) \leq G'$, y por tanto $G \cap W(G) = G' \cap W(G)$, y como del Lema 4.3.22 se deduce directamente que

$$G' \cap W(G) \subseteq 1 + J(G) \subseteq W(G),$$

intersecando con G obtenemos que

$$G \cap W(G) = G \cap (1 + J(G)) = \gamma_3(G)\gamma_2(G)^{(p)},$$

siendo la última igualdad cierta por el segundo apartado del Lema 4.3.17.

Por la Observación 4.3.21 sabemos que $W(G)$ es central en $V(\mathbb{F}_p[G])$ módulo $1 + J(G)$, de modo que, como ya hemos probado que $V(\mathbb{F}_p[G]) = G \cdot W(G)$, es una comprobación directa que $G(1 + J(G))$ es normal en $V(\mathbb{F}_p[G])$. Además, como $1 + J(G) \subseteq W(G)$ se tiene que

$$G(1 + J(G)) \cap W(G) = (G \cap W(G)) \cdot (1 + J(G)) = 1 + J(G)$$

Se sigue entonces que

$$\frac{V(\mathbb{F}_p[G])}{1+J(G)} = \frac{G(1+J(G))}{1+J(G)} \oplus \frac{W(G)}{1+J(G)},$$

donde sabemos que

$$\frac{G(1+J(G))}{1+J(G)} \cong \frac{G}{G\cap(1+J(G))} = \frac{G}{\gamma_2(G)^{(p)}\gamma_3(G)}$$

y que

$$\frac{W(G)}{1+J(G)} = \frac{W(G)}{W(G)\cap(1+\mathrm{Aug}_{\mathbb{F}_p}(G,G'))} \cong \frac{W(G)\cdot(1+\mathrm{Aug}_{\mathbb{F}_p}(G,G'))}{1+\mathrm{Aug}_{\mathbb{F}_p}(G,G')} = W(\overline{G}),$$

el resultado buscado.

□

Teorema 4.3.24 (Sandling)**.** *Sea G un p-grupo finito. Entonces la clase de isomorfía del grupo cociente $G/(\gamma_2(G)^{(p)}\gamma_3(G))$ está determinada por $\mathbb{F}_p[G]$.*

Demostración. Como por el Teorema 4.2.14 la clase de isomorfía de G/G' está determinada por $\mathbb{F}_p[G]$, también lo está $\mathbb{F}_p[G/G']$; y como en este álgebra de grupo es válida la descomposición

$$V(\mathbb{F}_p[G/G']) = W(G/G')\oplus G/G'$$

y el grupo de unidades normalizadas también está determinado, se sigue del el Teorema fundamental de los grupos abelianos finitos (ver Teorema 1.1.1) que está determinado $W(G/G')$.

Finalmente, el Teorema 4.3.23 da que

$$\frac{V(\mathbb{F}_p[G])}{1+J(G)} \cong \frac{G}{\gamma_2(G)^{(p)}\gamma_3(G)} \oplus W\left(G/G'\right),$$

donde $V(\mathbb{F}_p[G])/(1+J(G))$ está determinado por $\mathbb{F}_p[G]$ por estarlo $J(G)$, y acabamos de probar que también lo está $W(G/G')$. Así, dado que considerando las descomposiciones en subgrupos indescomponibles el Teorema de Krull-Schmidt (Teorema 1.1.46) garantiza que la clase de isomorfía de $G/(\gamma_2(G)^{(p)}\gamma_3(G))$ está determinada por los grupos anteriores, el resultado se sigue. □

Al cociente $G/(\gamma_2(G)^{(p)}\gamma_3(G))$ del teorema anterior se lo suele denominar *cociente de Sandling*, pues todos los resultados de la subsección se deben a R. Sandling (ver [37]).

Corolario 4.3.25. *Sea G un p-grupo finito con clase de nilpotencia 2 y tal que G' es abeliano elemental. Entonces la clase de isomorfía de G está determinada por el álgebra de grupo modular $\mathbb{F}_p[G]$.*

Demostración. La afirmación "$c(G) = 2$" está determinada por $\mathbb{F}_p[G]$ por la Proposición 4.2.20; ahora, todos los grupos de clase de nilpotencia 2 tienen subgrupo conmutador abeliano, por lo que G' está determinado por $\mathbb{F}_p[G]$ (ver Proposición 4.2.16), y en particular lo está si es abeliano elemental o no.

Por tanto, podemos limitarnos a probar que G está determinado en la clase de los grupos con clase de nilpotencia 2 y subgrupo conmutador abeliano elemental. Y esto es inmediato a partir del teorema anterior, pues estas condiciones implican que $\gamma_2(G)^{(p)}\gamma_3(G) = \{1\}$. □

Obviamente, este último resultado generaliza el Corolario 4.3.6, y de hecho es, junto con el Teorema 4.3.10, el resultado más potente que probamos en este trabajo. Además, la clase de grupos para la que el Corolario 4.3.25 resuelve **(MIP)** admite la siguiente caracterización.

Definición 4.3.26. Sea G un -grupo. Decimos que G es *central-elemental-por-abeliano* si existe un subgrupo central N de G tal que N es abeliano elemental y G/N es abelinao.

Se comprueba fácilmente que la clase de los grupos abeliano-elemental-por-cíclico es precisamente la clase de los grupos con clase de nilpotencia 2 y subgrupo conmutador abeliano elemental. En efecto, si G tiene clase de nilpotencia 2 y G' es abeliano elemental, es claro que tomando $N = G'$ se verifican las condiciones de la definición anterior. Recíprocamente, si N es un subgrupo central de G como en la definición previa, es claro que $G' \subseteq N$ por ser N abeliano, y en consecuencia G' también es central y abeliano elemental. Por tanto, el Corolario 4.3.25 se puede reescribir como:

Corolario 4.3.27. *Sea G un p-grupo finito central-elemental-por-abeliano. Entonces la clase de isomorfía de G está determinada por el álgebra de grupo modular $\mathbb{F}_p[G]$.*

Observación 4.3.28. Además, teniendo en cuenta que un p-grupo G es metacíclico si y sólo si lo es el grupo cociente $G/\Phi(G)\gamma_3(G) = G/\gamma_2(G)^{(p)}\gamma_3(G)$ (para una prueba, ver el Lema 11.3 de [22]), el Teorema 4.3.24 también garantiza que el valor de la afirmación "G es metacíclico" está determinado por $\mathbb{F}_p[G]$.

Tamaño del núcleo

Presentamos un último invariante numérico. Sea de nuevo G un p-grupo finito. Puede llegar a ser muy útil considerar la siguiente construcción, propuesta inicialmente por R. Brauer (de acuerdo a [32]). Tomamos la aplicación:

$$\lambda : \frac{\mathrm{Aug}_K(G)}{\mathrm{Aug}_K(G)^2} \to \frac{\mathrm{Aug}_K(G)^p}{\mathrm{Aug}_K(G)^{p+1}}, \qquad \alpha + \mathrm{Aug}_K(G) \mapsto \alpha^p + \mathrm{Aug}_K(G)^{p+1}.$$

Claramente está bien definida, pues si $\alpha = \beta + \delta$, con $\delta \in \mathrm{Aug}_K(G)^2$, entonces

$$\alpha^p = (\beta + \delta)^p \equiv \beta^p \mod \mathrm{Aug}_K(G)^{p+1},$$

pues es evidente que todos los sumandos en el desarrollo del binomio en los que aparece δ pertenecen al menos a la $(p+1)$-ésima potencia $\mathrm{Aug}_K(G)$.

Estos ideales están obviamente determinados por $K[G]$, por lo que, si K es un cuerpo finito, también lo estará el tamaño del "núcleo de esta aplicación", i.e.,

$$|\operatorname{Ker}\lambda| = \left| \left\{ \overline{\alpha} \in \frac{\mathrm{Aug}_K(G)}{\mathrm{Aug}_K(G)^2} \ : \ \lambda(\overline{\alpha}) = \mathrm{Aug}_K(G)^{p+1} \right\} \right|.$$

A este número lo llamaremos *tamaño del núcleo*. En definitiva, particularizando al caso $K = \mathbb{F}_p$, hemos probado:

Proposición 4.3.29. Sea G un p-grupo finito, y sea λ como arriba. Entonces el tamaño del núcleo, $|\operatorname{Ker}(\lambda)|$, está determinado por $\mathbb{F}_p[G]$.

4.4. El Problema del Isomorfismo Modular

En resumen, los invariantes obtenidos en las dos secciones previas permiten dar respuesta positiva a la restricción del Problema del Isomorfismo Modular a un par de clases de grupos, que recopilamos en el siguiente teorema:

Teorema 4.4.1. *Sea G un p-grupo finito. Entonces la clase de isomorfía de G está determinada por su álgebra de grupo modular $\mathbb{F}_p[G]$ si se verifica alguna de las condiciones siguientes:*

(I) p es impar y $\mathcal{M}_{p,4}(G) = \{1\}$.

(II) G es central-elemental-por-abeliano.

Demostración. Son los Corolarios 4.3.11 y 4.3.27, respectivamente. □

En la clase de p-grupos del segundo punto se agrupan todos los p-grupos con clase de nilpotencia a lo sumo 2 y subgrupo conmutador abeliano elemental, por lo que, en particular, incluye a todos los p-grupos abelianos, y a los p-grupos tales que la $\mathcal{M}$-serie tiene longitud 2. Además, destacamos que entre los grupos considerados en el primer punto puede haber grupos con clase de nilpotencia 3. De hecho, teniendo en cuenta que

$$\mathcal{M}_{3,4}(G) = G^{(9)}\gamma_3(G)^{(3)}\gamma_3(G)^{(3)}\gamma_4(G),$$
$$\mathcal{M}_{p,4}(G) = G^{(p)}\gamma_4(G), \qquad \text{para } p > 3;$$

es claro que los grupos verificando $\mathcal{M}_{p,4}(G) = \{1\}$ con p impar son precisamente los p-grupos de exponente p y clase de nilpotencia (a lo sumo) 3, si $p > 3$; y los 3-grupos G con exponente (a lo sumo) 9 y clase de nilpotencia (a lo sumo) 3 tales que los subgrupos $\gamma_2(G)$ y $\gamma_3(G)$ tienen exponente no mayor que 3.

Otros resultados conocidos

Notemos que los invariantes descritos en las dos secciones previas se demuestran determinados por el álgebra de grupo $\mathbb{F}_p[G]$ independientemente de cual sea el p-grupo finito G, siendo las únicas excepciones la clase de nilpotencia y la clase de isomorfismo de G', que, hasta el momento, sólo se han demostrado determinadas cuando G pertenece a ciertas clases de p-grupos.

En este último sentido, se destaca que la mayor parte de los resultados parciales existentes relativos al Problema del Isomorfismo Modular no se apoyan solamente en resultados generales como los ya probados, sino que, normalmente, sus demostraciones proceden como sigue: fijada alguna clase de grupos para la que ya exista una clasificación relativamente manejable de todos sus componentes (salvo isomorfismo), se utilizan los invariantes generales ya obtenidos, junto con otros construidos *ad hoc* para esa clase de grupos (i.e., tales que no es conocido que estén determinados por $K[G]$ ó $\mathbb{F}_p[G]$ para grupos que no estén en dicha clase, o incluso que no tengan sentido para p-grupos finitos arbitrarios) para comprobar que los grupos de la clase considerada dan lugar a álgebras de grupo dos a dos no isomorfas.

Dedicamos esta última sección, con el fin de ofrecer una panorámica completa del estado actual del Problema del Isomorfismo Modular, a presentar los resultados de este tipo que nos son conocidos, dando para unos pocos de ellos esquemas de sus demostraciones, e indicando qué papel desempeñan en ellas los invariantes generales que manejamos. Recopilamos esos resultados en el siguiente teorema.

Teorema 4.4.2. *Sea G un p-grupo finito. Entonces la clase de isomorfía de G está determinada por el álgebra de grupo modular $\mathbb{F}_p[G]$ si G pertenece alguna de las siguientes clases:*

(I) *2-grupos de clase maximal;*

(II) *p-grupos con centro de índice p^2;*

(III) *p-grupos de clase maximal, orden no mayor que p^{p+1} y con un subgrupo maximal abeliano;*

(IV) *2-grupos de clase casi maximal (en la clase de los 2-grupos de clase casi maximal);*

(V) *p-grupos metacíclicos;*

(VI) *p-grupos abeliano-elemental-por-cíclico;*

(VII) *p-grupos de orden no mayor que p^5;*

(VIII) *p-grupos con un subgrupo cíclico de índice p^2;*

(IX) *2-grupos de orden no mayor que 2^6 (con demostraciones teóricas) y 2-grupos de orden no mayor que 2^9 (con demostraciones computacionales).*

Referencias de las demostraciones. Las demostraciones de (I) y (VI) se deben a C. Bagiński, y se pueden encontrar, respectivamente, en [3] y [4]. Las de (IV) y (VIII) se deben también a C. Bagiński, junto con A. Konovalov, y se pueden consultar en [6] y en [7], respectivamente. Además, en [5] C. Bagiński y A. Caranti demuestran (III). La prueba de (V) fue dada originalmente por C. Bagiński, para $p > 2$, en [2], y completada por R. Sandling en [38]. El resultado de (II) es probado por V. Drensky en [13].

El resultado de (VII) fue demostrado por D.S. Passman, para p-grupos con orden no mayor que p^4 en [32]. Para grupos de orden p^5, el caso $p = 2$ viene dado por A. Masasikis en [28]; para $p > 2$, la prueba se debe a R. Sandling y M.A.M. Salim, y se puede consultar en [35].

Finalmente, el resultado (teórico) de (IX) sobre grupos de orden 2^6 viene dado por M. Hertweck y M. Soriano en [20]. El resultado para grupos de orden 2^7 (debido F.M. Bleher, W.Kimmerle, K.W. Roggenkamp y M. Wursthorn) se presenta en [10]; para grupos de órdenes 2^8 y 3^6 (por B. Eick) aparece en [14]); y finalmente para grupos de orden 2^9, debido a B. Eick y A. Konovalov se puede consultar en [15].

□

Los resultados de este teorema están ordenados de tal forma que la demostración (original) de cada punto puede llevarse a cabo utilizando sólo los puntos precedentes. Además, las demostraciones de los dos primeros apartados siguen siendo válidas si sustituimos $\mathbb{F}_p$ por un cuerpo de característica p arbitrario, constituyendo así también respuestas afirmativas a **(WMIP)** para esas dos clases de grupos.

Seleccionamos ahora algunos de estos resultados, a modo de ejemplo, para dar esquemas de sus pruebas e ilustrar la utilidad de los invariantes presentados anteriormente.

p-grupos de orden divisor de p^4

Antes de entrar en la demostración de este resultado, es conveniente considerar la siguiente observación sobre los 2-grupos de clase maximal.

Observación 4.4.3. Un grupo de orden 2^n es de clase maximal si y sólo si $(G : G') = 4$. Además, un grupo en estas condiciones es necesariamente isomorfo[2] a uno de los siguientes:

$$\begin{aligned} D_n =& \langle a, b \ : \ a^{2^{n-1}} = b^2 = 1, \ a^b = a^{-1} \rangle \\ Q_n =& \langle a, b \ : \ a^{2^{n-1}} = 1, \ a^{2^{n-2}} = b^2, \ a^b = a^{-1} \rangle \\ S_n =& \langle a, b \ : \ a^{2^{n-1}} = b^2 = 1, \ a^b = a^{-1+2^{n-2}} \rangle \end{aligned}$$

Este es un resultado largo tiempo conocido, para el que nos remitimos al Teorema 5.4.5 de [17].

Partiendo de esta observación, de los resultados relativos a p-grupos de clase maximal[3], y de las clasificaciones que daremos a continuación, se demuestra fácilmente el resultado de D.S. Passman en [32] que da solución a **(MIP)**) para p-grupos de orden a lo sumo p^4. Como decíamos, precisaremos de la clasificación de los p-grupos no abelianos de orden a los sumo p^4 dada por W. Burnside en [11], págs. 145-146, y que reproducimos en las siguientes tablas. En primer lugar, hay dos posibles clases de isomorfía para 2-grupos no abelianos de orden 2^3:

De orden 2^3	Presentación del grupo
(a-i)	$\langle g, h \ : \ g^4 = h^2 = 1, \ g^h = g^3 \rangle$
(a-ii)	$\langle g, h \ : \ g^4 = h^4 = 1, \ g^h = g^{-1}, \ h^2 = g^2 \ \rangle$

[2]Nótese la simplicidad de esta clasificación: de hecho, la demostración del punto (I) del Teorema 4.4.2 – correspondiente a [3]– se limita a comprobar que (para cada orden) estos tres grupos dan lugar a álgebras de grupo no isomorfas.

[3]De hecho, los resultados de [5] son una generalización de los argumentos que usa D.S. Passman para tratar los p-grupos de clase maximal y orden no mayor que p^4 que surgen en [32], pero se sostienen independientemente de éstos.

mientras que de orden 2^4 hay nueve:

De orden 2^4	Presentación del grupo
(b-i)	$\langle g,h \ : \ g^8=h^2=1,\ g^h=g^5\rangle$
(b-ii)	$\langle g,h,k \ : \ g^4=h^2=k^2=1,\ h^k=hg^2\ g^h=g\rangle$
(b-iii)	$\langle g,h \ : \ g^4=h^4=1,\ g^h=g^3\rangle$
(b-iv)	$\langle g,h,k \ : \ g^4=h^2=k^2=1,\ g^k=g^3\ h^g=h,\ h^k=h\rangle$
(b-v)	$\langle g,h,k \ : \ g^4=h^2=k^2=1,\ g^k=gh\ g^h=g,\ h^k=h\rangle$
(b-vi)	$\langle g,h,k \ : \ g^4=h^4=k^2=1,\ g^h=g^{-1},\ h^2=p^2, h^k=h, g^k=g\rangle$
(b-vii)	$\langle g,h \ : \ g^8=h^2=1,\ g^h=g^{-1}\rangle$
(b-viii)	$\langle g,h \ : \ g^8=h^2=1,\ g^h=g^3\rangle$
(b-ix)	$\langle g,h \ : \ g^8=h^4=1,\ g^h=g^{-1},\ h^2=g^4\rangle$

Ahora, sea $p>2$. Hay dos clases de isomorfismo de p-grupos no abelianos de orden p^3:

De orden p^3	Presentación del grupo
(c-i)	$\langle g,h \ : \ g^{p^2}=h^p=1,\ g^h=g^{1+p}\rangle$
(c-ii)	$\langle g,h,k \ : \ g^p=h^p=k^p=1,\ h^k=hg,\ g^k=g,\ g^h=h\rangle$

Y finalmente, hay diez p-grupos no abelianos de orden p^4:

De orden p^4	Presentación del grupo
(d-i)	$\langle g,h \ : \ g^{p^3}=h^p=1,\ g^h=g^{1+p^2}\rangle$
(d-ii)	$\langle g,h,k \ : \ g^{p^2}=h^p=k^p=1,\ h^k=hg^p\ g^h=g\rangle$
(d-iii)	$\langle g,h \ : \ g^{p^2}=h^{p^2}=1,\ g^h=g^{p+1}\rangle$
(d-iv)	$\langle g,h,k \ : \ g^{p^2}=h^p=k^p=1,\ g^k=g^{p+1}\ h^g=h,\ h^k=h\rangle$
(d-v)	$\langle g,h,k \ : \ g^{p^2}=h^p=k^p=1,\ g^k=gh\ g^h=g,\ h^k=h\rangle$
(d-vi)	$\langle g,h,k \ : \ g^{p^2}=h^p=1,\ g^h=g^{1+p},\ g^k=gh,\ h^k=h,\ k^p=1\rangle$
(d-vii)	$\langle g,h,k \ : \ g^{p^2}=h^p=1,\ g^h=g^{1+p},\ g^k=gh,\ h^k=h,\ k^p=g^p\rangle$
(d-viii)	$\langle g,h,k \ : \ g^{p^2}=h^p=1,\ g^h=g^{1+p},\ g^k=gh,\ h^k=h,\ k^p=g^{\alpha p}\rangle$
(d-ix)	$\langle g,h,k,s \ : \ g^p=h^p=k^p=s^p=1,\ k^s=kg,\ h^s=s,\ g^s=g, h^k=h,\ g^h=g\rangle$
(d-x), $p>3$	$\langle g,h,k,s \ : \ g^p=h^p=k^p=s^p=1,\ k^s=kh,\ h^s=hg,\ g^s=g, h^k=h,\ g^k=g, g^h=g\rangle$
(d-x), $p=3$	$\langle g,h,k \ : \ g^9=h^3=k^3=1,\ g^h=g,\ g^k=gh,\ h^k=g^{-3}h\rangle$

(donde en (viii) α es cualquier entero que no sea un residuo cuadrático módulo p).

Teorema 4.4.4 (Passman)**.** *Sea G un p-grupo de orden a lo sumo p^4. Entonces G está determinado por su álgebra de grupo $K[G]$.*

Esquema de la demostración. En primer lugar, notemos que si G es abeliano el Teorema 4.2.13 da el resultado. Por tanto, si G tiene orden p o p^2 no hay nada que probar (pues o es cíclico, o por la Proposición 1.1.25 ha de ser abeliano). Como el orden de un grupo viene claramente determinado por su álgebra de grupo, bastará probar que grupos del mismo orden no dan lugar a álgebras de grupo isomorfas. Consideremos entonces los grupos no abelianos de orden p^3. Distinguimos dos casos:

- Caso $p=2$. Sólo hay dos dos grupos no isomorfos, los dados (a-i) y (a-ii), que de hecho son, salvo isomorfismo, respectivamente el grupo diédrico y el grupo de los cuaterniones. Es directo comprobar las $\mathcal{M}$-series de ambos coinciden, y son

$$\mathcal{M}_{2,1}(G)=G, \qquad \mathcal{M}_{2,2}(G)=\langle g\rangle, \qquad \mathcal{M}_{2,3}(G)=\{1\},$$

de modo que la longitud de sus $\mathcal{M}$-series es 2, con lo que, en virtud del Corolario 4.3.5 sus álgebras de grupo no pueden ser isomorfas.

- Caso $p > 2$. Denotemos por G_1 y G_2 a los grupos dados en (c-i) y (c-ii), respectivamente. Es un cálculo directo ver que sus $\mathcal{M}$-series son:

$$\mathcal{M}_{p,1}(G_1) = G_1, \quad \mathcal{M}_{p,2}(G_1) = \mathcal{M}_{p,3}(G_1) = \cdots = \mathcal{M}_{p,p}(G_1) = \langle g^p \rangle, \quad \mathcal{M}_{p,p+1}(G_1) = \{1\};$$
$$\mathcal{M}_{p,1}(G_2) = G_2, \qquad \mathcal{M}_{p,2}(G_2) = \langle g \rangle, \qquad \mathcal{M}_{p,3}(G_2) = \{1\};$$

así, por ser $p > 2$ se ve que las $\mathcal{M}$-series tienen longitud distinta, y por tanto estos grupos no pueden dar lugar a álgebras de grupo isomorfas (por el Corolario 4.2.9).

Analicemos ahora los grupos no abelianos de orden p^4. Como antes, distinguimos entre los casos:

- Caso $p = 2$. Para los grupos en estas condiciones se tiene la siguiente tabla, que tomamos de [32]:

G	Tipo de $\mathcal{Z}(G)$	Tipo de G/G'	Tamaño del núcleo
(b-i)	(4)	(4, 2)	
(b-ii)	(4)	(2, 2, 2)	
(b-iii)	(2, 2)	(4, 2)	1
(b-iv)	(2, 2)	(2, 2, 2)	6
(b-v)	(2, 2)	(4, 2)	2
(b-vi)	(2, 2)	(2, 2, 2)	2
(b-vii)	(2)	(2, 2)	3
(b-viii)	(2)	(2, 2)	3
(b-ix)	(2)	(2, 2)	3

Todos estos invariantes se pueden calcular directamente; además por los resultados de las secciones previas están todos determinados por las respectivas álgebras de grupo modulares. Así, de la tabla se deduce que sólo los grupos de (b-vii), (b-viii), (b-ix) podrían dar lugar a álgebras de grupo isomorfas; y este no es el caso, pues estos son los grupos de clase maximal (por la Observación 4.4.3, pues el subgrupo conmutador tiene índice 4), de modo que el resultado se seguiría del punto (I) del Teorema 4.4.2, correspondiente a [3].

- Caso $p > 2$. De nuevo se puede calcular directamente una tabla como en [32]:

G	$\mathcal{Z}(G)$	G/G'	$\mathcal{M}_{p,2}(G)/\mathcal{M}_{p,3}(G)$	$\mathcal{M}_{p,3}(G)/\mathcal{M}_{p,4}(G)$ ($p > 3$)	Tamaño del núcleo ($p = 3$)
(d-i)	(p^2)	(p^2, p)			
(d-ii)	(p^2)	(p, p, p)			
(d-iii)	(p, p)	(p^2, p)	(1)		
(d-iv)	(p, p)	(p, p, p)	(1)		
(d-v)	(p, p)	(p^2, p)	(p)		
(d-vi)	(p)	(p, p)		(1)	5
(d-vii)	(p)	(p, p)		(1)	3
(d-viii)	(p)	(p, p)		(1)	1
(d-ix)	(p, p)	(p, p, p)	(p)		
(d-x), $p > 3$	(p)	(p, p)		(p)	
(d-x), $p = 3$	(3)	(3, 3)			7

De esta tabla se sigue, teniendo en cuenta que todos los invariantes que aparecen están determinados por $\mathbb{F}_p[G]$, que sólo los grupos (d-vi), (d-vii), (d-viii), con $p > 3$, podrían dar lugar a álgebras de grupo modulares isomorfas. Y de nuevo estos grupos se pueden probar de clase maximal, de modo que no pueden tener álgebras de grupo modulares isomorfas por el punto (III) del Teorema 4.4.2, correspondiente a [5] (siendo aplicable el resultado por ser $p \geq 3$, y en consecuencia $p^{p+1} \geq p^4$).

□

p-grupos metacíclicos

Como indicábamos arriba, la demostración de que **(MIP)** tiene respuesta positiva en las clase de los p-grupos metacíclicos finitos fue dada originalmente por C. Bagiński, para $p > 2$, y completada por R. Sandling. Seguimos el argumento de este último (ver [38]), que se apoya en la clasificación de los p-grupos metacíclicos dada por B.W. King, a partir de la cual el resultado es un mero corolario de las Secciones 4.2 y 4.3, y de [3]. Sintetizamos dicha clasificación en la siguiente proposición.

Proposición 4.4.5. Sean p un natural primo, y n, h, h', k, k' enteros no negativos. Si existe un p-grupo metacíclico G de orden p^n tal que su abelianizado G/G' es de tipo (p^h, p^k), y centro $\mathcal{Z}(G)$ es de tipo $(p^{h'}, p^{k'})$, entonces hay dos posibilidades:

(I) G es el único p-grupo metacíclico (salvo isomorfismo) en estas condiciones.

(II) G/G' es un grupo abeliano de clase $(2^m, 2)$ y $\mathcal{Z}(G)$ es un grupo abeliano de clase $(2^{m-1}, 2)$, para algún entero positivo n. En este último caso, si $m > 1$ necesariamente G es isomorfo a alguno de los grupos siguientes:

$$\langle a, b \ : \ a^{2^n} = b^{2^m} = 1, a^b = a^{-1} \rangle, \quad \text{o bien} \quad \langle a, b \ : \ a^{2^n} = b^{2^m} = 1, a^b = a^{-1+2^{n-1}} \rangle;$$

y si $m = 1$, a uno de los grupos:

$$\begin{aligned} D_n =& \langle a, b \ : \ a^{2^{n-1}} = b^2 = 1, \ a^b = a^{-1} \rangle \\ Q_n =& \langle a, b \ : \ a^{2^{n-1}} = 1, \ a^{2^{n-2}} = b^2, \ a^b = a^{-1} \rangle \\ S_n =& \langle a, b \ : \ a^{2^{n-1}} = b^2 = 1, \ a^b = a^{-1+2^{n-2}} \rangle \end{aligned}$$

Referencia de la demostración. Ver el Teorema 3.3 de [25]. □

Teorema 4.4.6. *Sea G un p-grupo metacíclico finito. Entonces la clase de isomorfía de G está determinada por el álgebra de grupo modular $\mathbb{F}_p[G]$.*

Esquema de la demostración. Por la Observación 4.3.28, si G es o no metacíclico esta determinado por $\mathbb{F}_p[G]$, por lo que uno puede limitarse a probar el enunciado en la clase de los grupos metacíclicos. Sea G un grupo metacíclico de orden p^n. Por la Proposición 4.4.5 el orden y las clases de isomorfía del centro y el abelianizado de G determinan a G (salvo en la excepción del apartado (II) de dicha proposición, con $p = 2$), y como estas clases de isomorfía están determinadas por $\mathbb{F}_p[G]$, el resultado se sigue.

Sólo quedaría probar que los 2-grupos de la excepción no dan lugar a álgebras de grupo isomorfas. En el caso $m = 1$ (con la notación de la mencionada proposición), los grupos que surgen son D_n, Q_n y S_n, que son 2-grupos de clase maximal por la Observación 4.4.3. Y [3] (es decir, el punto (I) del Teorema 4.4.2) da una respuesta positiva para el Problema del Isomorfismo Modular en ese caso, i.e, sus álgebras de grupo no pueden ser isomorfas.

Finalmente, para $m > 1$ habría que probar que los grupos

$$\langle a, b \ : \ a^{2^n} = b^{2^m} = 1, \ a^b = a^{-1} \rangle \quad \text{y} \quad \langle a, b \ : \ a^{2^n} = b^{2^n} = 1, \ a^b = a^{-1+2^{n-1}} \rangle$$

no dan lugar a álgebras de grupo isomorfas; y efectivamente ese no es el caso, pues el número de clases de conjugación de cuadrados es distinto en ambos grupos (y este número está determinada por $\mathbb{F}_p[G]$ en virtud del Lema 4.2.5). En efecto, se puede comprobar que en ambos casos los subconjuntos $\{b^{4i}a^{2j}, b^{4i}a^{-2j}\}$, con i, j arbitrarios, y $\{b^{2i}\}$, con i impar, son clases de conjugación. Pero en el primer caso estas son las únicas clases de conjugación conteniendo un cuadrado, mientras que en el segundo también lo son los subconjuntos centrales $\{b^{2i}a^{2^{n-1}}\}$, con i impar. □

		Presentación del grupo
$m \geq 4$	G_1	$\langle a, b \ : \ a^{2^{m-2}} = b^4 = 1, \ a^b = a^{1+2^{m-1}} \rangle$
	G_2	$\langle a, b, c \ : \ a^{2^{m-2}} = c^2 = 1, \ b^2 = a^{2^{m-3}}, \ a^b = a^{-1}, \ a^c = a, \ b^c = b \rangle$
	G_3	$\langle a, b, c \ : \ a^{2^{m-2}} = b^2 = c^2 = 1, \ a^b = a^{-1}, \ a^c = a, \ b^c = b \rangle$
	G_4	$\langle a, b, c \ : \ a^{2^{m-2}} = b^2 = c^2 = 1, \ a^b = a, \ a^c = a, \ b^c = a^{2^{m-3}} b \rangle$
	G_5	$\langle a, b, c \ : \ a^{2^{m-2}} = b^2 = c^2 = 1, \ a^b = a, \ a^c = ab, \ b^c = b \rangle$
$m \geq 5$	G_6	$\langle a, b \ : \ a^{2^{m-2}} = b^4 = 1, \ a^b = a^{-1} \rangle$
	G_7	$\langle a, b \ : \ a^{2^{m-2}} = b^4 = 1, \ a^b = a^{-1+2^{m-3}} \rangle$
	G_8	$\langle a, b \ : \ a^{2^{m-2}} = 1, \ b^4 = a^{2^{m-3}}, \ a^b = a^{-1} \rangle$
	G_9	$\langle a, b \ : \ a^{2^{m-2}} = b^4 = 1, \ b^a = b^{-1} \rangle$
	G_{10}	$\langle a, b, c \ : \ a^{2^{m-2}} = b^2 = c^2 = 1, \ a^b = a^{1+2^{m-3}}, \ a^c = a, \ b^c = b \rangle$
	G_{11}	$\langle a, b, c \ : \ a^{2^{m-2}} = b^2 = c^2 = 1, \ a^b = a^{-1+2^{m-3}}, \ a^c = a, \ b^c = b \rangle$
	G_{12}	$\langle a, b, c \ : \ a^{2^{m-2}} = b^2 = c^2 = 1, \ a^b = a, \ a^c = a^{-1}, \ b^c = a^{2^{m-3}} b \rangle$
	G_{13}	$\langle a, b, c \ : \ a^{2^{m-2}} = b^2 = c^2 = 1, \ a^b = a, \ a^c = a^{-1}, \ b^c = a^{-1} b, \ b^c = b \rangle$
	G_{14}	$\langle a, b, c \ : \ a^{2^{m-2}} = b^2 = 1, \ c^2 = a^{2^{m-3}}, \ a^b = a, \ a^c = a^{-1}, \ b^c = a^{-1} b, \ b^c = b \rangle$
	G_{15}	$\langle a, b, c \ : \ a^{2^{m-2}} = b^2 = c^2 = 1, \ a^b = a^{1+2^{m-3}}, \ a^c = a^{-1+2^{m-3}}, \ b^c = a^{-1} b, \ b^c = b \rangle$
	G_{16}	$\langle a, b, c \ : \ a^{2^{m-2}} = b^2 = c^2 = 1, \ a^b = a^{1+2^{m-3}}, \ a^c = a^{-1+2^{m-3}}, \ b^c = a^{-1} b, \ b^c = a^{2^{m-3}} b \rangle$
	G_{17}	$\langle a, b, c \ : \ a^{2^{m-2}} = b^2 = c^2 = 1, \ a^b = a^{1+2^{m-3}}, \ a^c = ab, \ b^c = b \rangle$
	G_{18}	$\langle a, b, c \ : \ a^{2^{m-2}} = b^2 = 1, \ c^2 = b, \ a^b = a^{1+2^{m-3}}, \ a^c = a^{-1} b \rangle$
$m \geq 6$	G_{19}	$\langle a, b \ : \ a^{2^{m-2}} = b^4 = 1, \ a^b = a^{1+2^{m-4}} \rangle$
	G_{20}	$\langle a, b \ : \ a^{2^{m-2}} = b^4 = 1, \ a^b = a^{-1+2^{m-4}} \rangle$
	G_{21}	$\langle a, b \ : \ a^{2^{m-2}} = 1, \ b^4 = a^{2^{m-3}}, \ a^b = b^{-1} \rangle$
	G_{22}	$\langle a, b, c \ : \ a^{2^{m-2}} = b^2 = c^2 = 1, \ a^b = a, a^c = a^{1+2^{m-4}} b, \ b^c = a^{2^{m-3}} b \rangle$
	G_{23}	$\langle a, b, c \ : \ a^{2^{m-2}} = b^2 = c^2 = 1, \ a^b = a, a^c = a^{-1+2^{m-4}} b, \ b^c = a^{2^{m-3}} b \rangle$
	G_{24}	$\langle a, b, c \ : \ a^{2^{m-2}} = b^2 = c^2 = 1, \ a^b = a^{1+2^{m-3}}, a^c = a^{-1+2^{m-4}} b, \ b^c = b \rangle$
	G_{25}	$\langle a, b, c \ : \ a^{2^{m-2}} = b^2 = 1, \ c^2 = a^{2^{m-3}}, \ a^b = a^{1+2^{m-3}}, a^c = a^{-1+2^{m-4}} b, \ b^c = b \rangle$
$m = 5$	G_{26}	$\langle a, b, c \ : \ a^8 = b^2 = 1, \ c^2 = a^4, \ a^b = a^5, a^c = ab, \ b^c = b \rangle$

Cuadro 4.1: p-grupos finitos con un subgrupo cíclico de índice p^2

2-grupos finitos con un subgrupo cíclico de índice 4

Ahora, partiendo sólo del resultado anterior (relativo a los p-grupos metacíclicos), del resultado sobre 2-grupos de clase maximal y casi maximal, y del el Teorema 4.4.4, los invariantes obtenidos prueban fácilmente que **(MIP)** tiene respuesta para 2-grupos con un subgrupo cíclico de índice 4, es decir, prueban la versión par del resultado de C. Bagiński y A. Konovalov en [7].

En primer lugar, notemos que, en general, si un p-grupo no abeliano G de orden p^m contiene un subgrupo cíclico de orden p^{m-2}, el exponente ha de ser mayor o igual que p^{m-2}, y por ser G no abeliano, las únicas posibilidades son $\exp(G) = p^{m-1}$ y $\exp(G) = p^{m-2}$. Los p-grupos finitos no abelianos de orden p^m y exponente p^{m-2} están clasificados en [30]. Para el caso $p = 2$ vienen dados por las presentaciones del Cuadro 4.1. Y los grupos no abelianos de orden 2^m y exponente 2^{m-1} están catalogados ya largo tiempo en [11], siendo cada uno de ellos isomorfo a alguno de los siguientes:

$$\begin{aligned} D_m &= \langle a, b \ : \ a^{2^{m-1}} = b^2 = 1, \ a^b = a^{-1} \rangle, \\ Q_m &= \langle a, b \ : \ a^{2^{m-1}} = 1, \ a^{2^{m-2}} = b^2, \ a^b = a^{-1} \rangle, \\ S_m &= \langle a, b \ : \ a^{2^{m-1}} = b^2 = 1, \ a^b = a^{-1+2^{m-2}} \rangle, \\ M_m &= \langle a, b \ : \ a^{2^{m-1}} = b^2 = 1, \ a^b = a^{1+2^{m-2}} \rangle. \end{aligned}$$

Teorema 4.4.7. *Sea G un 2-grupo finito que contiene un subgrupo cíclico de índice 4. Entonces la clase de isomorfía de G está determinada por el álgebra de grupo modular $\mathbb{F}_2[G]$.*

Esquema de la demostración. Sea G un grupo de orden 2^m. El caso para $m < 5$ el resultado es cierto en general por el Teorema 4.4.4. Podemos entonces limitarnos a estudiar la cuestión para $m \geq 5$. Como $\exp(G)$ está determinado por $\mathbb{F}_p[G]$, podemos estudiar por separado los grupos de exponente 2^{m-1} y los de exponente 2^{m-2}.

Si G tiene exponente 2^{m-1}, por los comentarios previos G ha de ser isomorfo a uno de los grupos D_m, Q_m, S_m ó M_m. Los tres primeros son 2-grupos de clase maximal, de modo que no pueden tener álgebras de grupo modular isomorfas; además, como la propiedad de ser un 2-grupo de clase maximal también está determinada por $\mathbb{F}_p[G]$ (pues lo está el índice $(G : G')$), el álgebra de grupo del último ha de ser no isomorfa a las de los anteriores.

n	Tipo de $(G_n)'$	Tipo de $\mathcal{Z}(G_n)$	$c(G_n)$
1	(2)	$(2^{m-3}, 2)$	2
2	(2^{m-3})	$(2, 2)$	$m-2$
3	(2^{m-3})	$(2, 2)$	$m-2$
4	(2)	(2^{m-2})	2
5	(2)	$(2^{m-3}, 2)$	2
6	(2^{m-3})	$(2, 2)$	$m-2$
7	(2^{m-3})	$(2, 2)$	$m-2$
8	(2^{m-3})	(4)	$m-2$
9	(2)	$(2^{2^{m-3}}, 2)$	2
10	(2)	$(2^{2^{m-3}}, 2)$	2
11	(2^{m-3})	$(2, 2)$	$m-2$
12	(2^{m-3})	(4)	$m-2$
13	(2^{m-3})	$(2, 2)$	$m-2$
14	(2^{m-3})	$(2, 2)$	$m-2$
15	(2^{m-3})	(2)	$m-2$
16	(2^{m-3})	(2)	$m-2$
17	$(2, 2)$	(2^{m-4})	3
18, $m = 5$	(2^{m-3})	(4)	$m-2$
18, $m > 5$	(2^{m-3})	(2)	$m-2$
19	(4)	(2^{m-4})	2
20	(2^{m-3})	(2)	$m-2$
21	(4)	(2^{m-3})	3
22	(4)	(2^{m-3})	3
23	(2^{m-3})	(4)	$m-2$
24	(2^{m-3})	(2)	$m-2$
25	(2^{m-3})	(2)	$m-2$
26	$(2, 2)$	(2)	3

Cuadro 4.2: Invariantes de p-grupos finitos con un subgrupo cíclico de índice p^2

Supongamos ahora que $\exp(G) = 2^{m-2}$; de nuevo, como el exponente está determinado por $\mathbb{F}_p[G]$, es suficiente probar que las álgebras de grupo modulares de los grupos considerados en el Cuadro 4.1 son dos a dos no isomorfas. Nos apoyamos en el Cuadro 4.2 (tomado de [7]). En primer lugar, notamos que todos son metabelianos, de modo que la clase de isomorfía del subgrupo conmutador está determinada por $\mathbb{F}_p[G]$ (ver Teorema 4.2.16); además, en todos casos este subgrupo es o bien abeliano elemental o bien cíclico, por lo que, en virtud la proposición 4.3.15 o del Teorema 4.2.21, la clase de nilpotencia de todos ellos está determinada. Además, por el Teorema 4.2.15, también la clase de isomorfía del centro está determinada.

Ahora, los grupos con clase de nilpotencia 2 salvo G_{19}, es decir, los G_n con $n \in \{1, 4, 5, 9, 10\}$, tienen todos subgrupo conmutador abeliano elemental, de modo que el Corolario 4.3.25 garantiza que su clase de isomorfía está determinada por $\mathbb{F}_p[G]$. Como G_{19} es el único grupo restante con clase de nilpotencia 2, se deduce que no puede dar lugar a un álgebra de grupo isomorfa a la de ningún otro grupo.

Por otro lado, los 2-grupos de clase casi maximal (no isomorfos) no pueden tener álgebras de grupo isomorfas por el punto (IV) Teorema 4.4.2 (correspondiente a [6]), por lo que también podemos descartar los grupos de clase $m-2$. En particular, esto resuelve el problema[4] para $m = 5$.

Supongamos entonces que $m > 5$. Sólo queda comprobar los grupos G_n, con $n \in \{17, 21, 22\}$ dan lugar a álgebras de grupo modulares dos a dos no isomorfas. La clase de isomorfía del centro (o del subgrupo conmutador) nos permiten distinguir el álgebra de grupo de G_{17} de las de G_{21} y G_{22}. Finalmente, se puede comprobar que G_{21} es metacíclico pero G_{22} no lo es, y el resultado se sigue del Teorema 4.4.6 (o de la Observación 4.3.28).

□

Otros problemas relacionados

En el contexto del Problema del Isomorfismo Modular, formula S.D. Berman el llamado *Problema del Isomorfismo Modular para Grupos de Unidades Normalizadas*, que se pregunta sobre la validez de la siguiente afirmación:

Problema 5 (**UMIP**). *Sea G un p-grupo finito. ¿Está entonces la clase de isomorfía de G determinada por $V(\mathbb{F}_p[G])$, el grupo de unidades normalizadas del el álgebra de grupo modular $\mathbb{F}_p[G]$?*

Claramente una solución positiva a este problema implicaría una solución positiva de **(MIP)**, por lo que necesariamente los avances alcanzados en su estudio son menos amplios que los del problema estudiado en este trabajo; sin embargo sí existen algunos resultados positivos.

Por ejemplo, A. Konovalov y A. Krivokhata comprueban computacionalmente en [26] que **(UMIP)** tiene respuesta positiva para 2-grupos de orden a lo sumo 2^5. Además, R. Sandling ha dado una prueba teórica en [36] de **(UMIP)** en el caso conmutativo, i.e., cuando G es un p-grupo abeliano. Este problema también tiene respuesta positiva sobre la clase de los 2-grupos de clase maximal, como prueban Zs. Balogh y A. Bovdi en [8].

Otro problema estrechamente relacionado con el Problema del Isomorfismo Modular, y para el que, de hecho, en la aproximación a **(MIP)** que hemos seguido se ha obtenido un resultado parcial, es el llamado *Problema del Complemento Normal* para álgebras de grupo modulares (que abreviaremos por **(NCP)**):

Problema 6 (**NCP**). *Sea G un p-grupo finito. ¿El grupo de unidades normalizadas $V(\mathbb{F}_p[G])$ contiene un subgrupo normal N tal que $N \cdot G = V(\mathbb{F}_p[G])$ y $N \cap G = \{1\}$?*

En efecto, es obvio que del Teorema 4.3.10 se sigue inmediatamente una respuesta afirmativa a este problema para los p-grupos G, con p impar, tal que $\mathcal{M}_{p,4}(G) = \{1\}$. Otros resultados relativos a este problema se pueden consultar, por ejemplo, en [24].

En otra dirección, cabe extender el Problema del Isomorfismo Modular (Amplio) considerando p-grupos que no sean necesariamente finitos; muy poco es conocido en este sentido, a excepción del siguiente teorema de D. Berman y W. May, que extiende la Proposición 4.2.13 a grupos abelianos numerables:

Teorema 4.4.8. *Sea G un grupo abeliano numerable, y K un cuerpo de característica p. Entonces la clase de isomorfía de G está determinada por el álgebra de grupo $K[G]$.*

Referencia de la demostración. Ver el Teorema 14.3.6 de [33]. □

[4] De hecho, este caso se podía haber dado por conocido, teniendo en cuenta el apartado (VII) del Teorema 4.4.2

Índice alfabético

N-serie, 19
  p-restringida, 19
N_p-serie, 19
p-grupo
  finito, 5
p-parte de un entero, 20

Abelianizado
  de un grupo, 2
Altura
  de un elemento, 39
Anillo local, 37
Aplicación de aumento, 28

Base
  adaptada a una filtración, 42
  de Jennings, 43
    generalizada, 40
  de un grupo abeliano, 48

Clase de nilpotencia, 2
Cociente de Sandling, 89
Condición
  de cadena ascendente, 10
  de cadena descendente, 11
Conmutador, 1
  n-ario, 13
    canónico, 11
  de Lie, 26

Ecuación
  de clases, 5
Elemento
  nilpotente, 35
  no-generador, 9
Exponente
  de un grupo, 9

Fórmulas
  de Hall-Petresco, 15
Filtración
  de un ideal, 37
  graduada, 37
    determinada por una N_p-serie, 39

Grupo
  abeliano elemental, 9
  central-elemental-por-abeliano, 89
  de clase casi maximal, 7
  de clase maximal, 7
  indescomponible, 10
  metabeliano, 2
  metacíclico, 2
  nilpotente, 2

Ideal
  de aumento, 28
  de Jacobson, 36
  de Zassenhaus, 57
  maximal, 35
  nilpotente, 35
Isomorfismo normalizado, 32

Método de agrupación de conmutadores, 14

Peso
  de un elemento de una base de Jennings, 40
Potencias de Lie del ideal de aumento, 49
Problema
  de los Subgrupos de Dimensión, 45
  del Complemento Normal, 98
  del Isomorfismo, 33, 34
  del Isomorfismo Modular, 34
  del Isomorfismo Modular (Amplio), 34
  del Isomorfismo Modular para Grupos de Unidades Normalizadas, 98

Serie
  central inferior, 2
  central superior, 3
  de Brauer-Jennings-Zassenhaus, 21
  de Lazard, 19
Soporte de un elemento, 24
Subespacio
  conmutador, 26
Subgrupo
  conmutador, 2
  de dimensión, 43
  de Frattini, 8

derivado, 2
maximal, 8

Tamaño del núcleo, 90
Teorema
de Krull-Smith, 11
Fundamental de los Grupos Abelianos Finitos, 1
Tipo
de un grupo abeliano, 1

Bibliografía

[1] F.W. Anderson y K.R. Fuller: *Rings and Categories of Modules*. Graduate Texts in Mathematics. Springer New York, 2012.

[2] C Bagiński: *The isomorphism question for modular group algebras of metacyclic p-groups*. Proceedings of The American Mathematical Society, 104:39–39, 1988.

[3] C. Bagiński: *Modular group algebras of 2–groups of maximal class*. Communications in Algebra, 20(5):1229–1241, 1992.

[4] C. Bagiński: *On the isomorphism problem for modular group algebras of elementary abelian-by-cyclic p-groups*. Colloquium Mathematicae, 82(1):125–136, 1999.

[5] C. Bagiński y A. Caranti: *The Modular Group Algebras of p-Groups of Maximal Class*. Canadian Journal of Mathematics, 40(6):1422–1435, 1988.

[6] C. Bagiński y A. Konovalov: *On 2-groups of almost maximal class*. Publ. Math. Debrecen, 65(1-2):97–131, 2004.

[7] C. Bagiński y A. Konovalov: *The modular isomorphism problem for finite p-groups with a cyclic subgroup of index p^2*, volumen 1 de *London Mathematical Society Lecture Note Series*, página 186–193. Cambridge University Press, 2007.

[8] Zs. Balogh y A. Bovdi: *On Units of Group Algebras of 2-Groups of Maximal Class*. Communications in Algebra, 32:3227–3245, 2004.

[9] P. B. Bhattacharya, S. K. Jain y S. R. Nagpaul: *Basic Abstract Algebra*. Cambridge University Press, 1994.

[10] F. M. Bleher, W. Kimmerle, K. W. Roggenkamp y M. Wursthorn: *Computational Aspects of the Isomorphism Problem*. En *Algorithmic Algebra and Number Theory*, páginas 313–329. Springer Berlin Heidelberg, 1999.

[11] W. Burnside: *Theory of Groups of Finite Order*. Cambridge Library Collection - Mathematics. Cambridge University Press, 1911.

[12] E.C. Dade: *Deux groupes finis distincts ayant la même algèbre de groupe sur tout corps*. Mathematische Zeitschrift, 119:345–348, 1971.

[13] V. Drensky: *The isomorphism problem for modular group algebras of groups with large centres*. Contemp. Math., 93:145–153, 1989.

[14] B. Eick: *Computing automorphism groups and testing isomorphisms for modular group algebras*. Journal of Algebra, 320:3895–3910, 2008.

[15] B. Eick y A. Konovalov: *The modular isomorphism problem for the groups of order 512*, volumen 2 de *London Mathematical Society Lecture Note Series*, página 375–383. Cambridge University Press, 2011.

[16] G.A. Fernández-Alcober: *An introduction to finite p-groups: regular p-groups and groups of maximal class*. `https://www.mat.unb.br/~matcont/20_3.pdf`.

[17] D. Gorenstein: *Finite Groups*. AMS Chelsea Publishing. Chelsea Pub. Co., 1980.

[18] M. Hertweck: *A Counterexample to the Isomorphism Problem for Integral Group Rings*. Annals of Mathematics. Second Series, 154(1):115–138, 2001.

[19] M. Hertweck: *A note on the modular group algebras of odd p-groups of M-length three*. Publicationes mathematicae, 71(1-2):1–11, 2007.

[20] M. Hertweck y M. Soriano: *On the modular isomorphism problem: groups of order* 2^6. Amer. Math. Soc, 420:177–213, 2006.

[21] T. W. Hungerford: *Algebra*. Graduate Texts in Mathematics. Springer, 1980.

[22] B. Huppert: *Endliche Gruppen I*. Die Grundlehren der mathematischen Wissenschaften 134. Springer, 1967.

[23] S. A. Jennings: *The Structure of the Group Ring of a p-Group Over a Modular Field*. Transactions of the American Mathematical Society, 50(1):175–185, 1941.

[24] S. Kaur y M. Khan: *A note on normal complement problem for split metacyclic groups*. Communications in Algebra, 47(9):3842–3848, 2019.

[25] B. W. King: *Presentations of metacyclic groups*. Bulletin of the Australian Mathematical Society, 8(1):103–131, 1973.

[26] A. Konovalov y A. Krivokhata: *On the isomorphism problem for unit groups of modular group algebras*. Acta Sci. Math (Szeged), 73(1-2):53–59, 2007.

[27] B. Külshammer: *Group-theoretical descriptions of ring-theoretical invariants of group algebras*. En *Representation Theory of Finite Groups and Finite-Dimensional Algebras: Proceedings of the Conference at the University of Bielefeld from May 15–17, 1991, and 7 Survey Articles on Topics of Representation Theory*, páginas 425–442. Birkhäuser Basel, 1991.

[28] A. Makasikis: *Sur l'isomorphie d'algèbres de groupes sur un champ modulaire*. Bull. Soc. Math. Belg, 28(2):91–109, 1976.

[29] C.P. Milies y S.K. Sehgal: *An Introduction to Group Rings*. Algebra and Applications. Springer Netherlands, 2002.

[30] Y. Ninomiya: *Finite p-groups with cyclic subgroups of index* p^2. Mathematical Journal of Okayama University, 36:1–21, 1994.

[31] I.B.S. Passi: *Group Rings and Their Augmentation Ideals*. Lecture Notes in Mathematics. Springer, 1979.

[32] D. S. Passman: *The group algebras of groups of order* p^4 *over a modular field*. Michigan Math. J., 12(4):405–415, 1965.

[33] D.S. Passman: *The algebraic structure of group rings*. Pure and applied mathematics. Wiley, 1977.

[34] J. Ritter y S.K. Sehgal: *Isomorphism of group rings*. Archiv der Mathematik, 40:32–39, 1983.

[35] M. A. M. Salim y R. Sandling: *The modular group algebra problem for groups of order* p^5. Journal of the Australian Mathematical Society. Series A. Pure Mathematics and Statistics, 61(2):229–237, 1996.

[36] R. Sandling: *Units in the modular group algebra of a finite abelian p-group.* Journal of Pure and Applied Algebra, 33(3):337 – 346, 1984.

[37] R. Sandling: *The modular group algebra of a central-elementary-by-abelian p -group.* Archiv Der Mathematik, 52:22–27, 1989.

[38] R. Sandling: *The modular group algebra problem for metacyclic p-groups.* Proceedings of the American Mathematical Society, 124(5):1347–1350, 1996.

[39] S.K. Sehgal: *Topics on Group Rings.* Algebra and Applications. Dekker, New York, 1978.