USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Extensiones de grupos y cohomología

Raúl Alvite Pazo

2020/2021

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Extensiones de grupos y cohomología

Raúl Alvite Pazo

Xullo, 2021

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Coñecemento: Álxebra
Título: Extensións de grupos e cohomoloxía
Breve descrición do contido
Os grupos de cohomoloxía xorden en moitas áreas das matemáticas. A noción formal de grupos de cohomoloxía apareceu a mediados do século XX impulsada pola topoloxía alxébrica. A cohomoloxía en dimensións baixas dun grupo xa se estudaba clasicamente con outros métodos, moito antes da formulación da cohomoloxía de grupos. O obxectivo do traballo é estudar a relación que hai entre a cohomoloxía de grupos en dimensións baixas e as extensións de grupos.
Bibliografía
J. J. Rotman, *Advanced modern algebra. Part 2.* Third edition. Graduate Studies in Mathematics, 180. AMS, Providence, RI, 2017.
Recomendacións

Índice general

Resumen

El principal problema asociado a las extensiones de grupos es clasificar, dados dos grupos, todas sus extensiones posibles salvo equivalencia. Este es un problema difícil pero, bajo ciertas condiciones para los grupos que determinan la extensión, se vuelve más manejable, y su resolución se alcanza mediante la cohomología de grupos.

En este trabajo se estudiará dicho problema. Primero, se darán nociones básicas de sucesiones exactas, Q-módulos y productos semidirectos, así como propiedades de los mismos. Después, se estudiarán las extensiones generales y su tipo más simple, las extensiones escindidas, y su relación con el producto semidirecto.

Posteriormente, bajo las hipótesis de que la extensión tenga núcleo abeliano, se presentará una construcción general de grupos de cohomología y la teoría clásica de extensiones para dimensión baja, con la que Schreier dio solución al problema. Finalmente, se probará el Teorema de Schur-Zassenhaus utilizando los resultados anteriores y se dará una construcción de los grupos de cohomología más eficiente usando resoluciones libres.

Abstract

Given two groups, the main problem that arises when studying group extensions is classifying every possible extension of these groups up to equivalence. This is a complicated problem; however, it becomes easier to handle when certain conditions related to the groups defining the extension are satisfied, and its solution can be found using group cohomology.

We will study this problem in this paper. First, we shall present basic notions of exact sequences, Q-modules and semidirect products, and some of their properties. After that, we will study general group extensions, focusing next on the simplest of extensions, the ones that split, and their relation to the semidirect product.

Next, we will suppose the extension's kernel is abelian and present a general construction of cohomology groups and the classic group extension theory in low dimension, which leads to Schreier's solution. Lastly, we will prove the Schur-Zassenhaus theorem using these results and give a more efficient construction for cohomology groups using free resolutions.

Introducción

Sean K y Q dos grupos. Una extensión de K por Q es una sucesión exacta corta $1 \to K \to G \to Q \to 1$ (aunque algunos matemáticos llaman a esto una extensión de Q por K). El principal problema en el estudio de las extensiones de grupos es clasificar las extensiones de K por Q, salvo equivalencia. A grandes rasgos, se trata de construir de todas las formas posibles un grupo G con K como subgrupo normal y Q como grupo cociente. Este problema implica a los funtores de cohomología $H^i(Q, -)$ para $i = 1, 2, 3$.

La teoría clásica de las extensiones de grupos fue desarrollada por O. Hölder (1893), O. Schreier (1926) y R. Baer (1934), mientras que las implicaciones homológicas de la teoría fueron expuestas por S. Eilenberg y S. MacLane (1947).

Hölder y Schreier dieron una respuesta al problema de la extensión, pero tiene algunos inconvenientes considerables. Dados K y Q, puede haber muchas soluciones G que satisfagan $K \lhd G$ y $Q \cong G/K$, y la teoría de Hölder-Schreier proporciona una caracterización de todas las posibles soluciones G. Pero en general no es posible determinar si estos grupos de solución G son isomorfos entre sí o no.

La idea de "factor sets" apareció por primera vez en el trabajo de Hölder, y posteriormente Schreier hizo el primer tratamiento sistemático de los "factor sets". En 1934, R. Baer dio el primer tratamiento invariante de las extensiones (es decir sin utilizar "factor sets"). Observó que cuando K era abeliano, los "factor sets" de Schreier podían añadirse por términos, de modo que las extensiones formaban un grupo abeliano (véase [9]).

Cuando el grupo K es abeliano, el problema de la extensiones de grupo es más tratable. Eilenberg y MacLane (1947) mostraron que el segundo grupo de cohomología, $H^2(Q, K)$, del grupo Q con coeficientes en el Q-módulo K, se puede utilizar para formalizar la teoría de extensión de grupos debida a Schreier y Baer.

Más detalladamente, $H^2(Q, K)$ es isomorfo al grupo de "factor sets" módulo los "principal factor sets". Los nombres "factor sets" y "principal factor sets" son terminología antigua. Hoy en día, los "factor sets" se llaman 2-cociclos y los "principal factor sets" se llaman 2-cofronteras. También está en biyección con el conjunto de las clases de equivalencia de extensiones de K por Q en las que la acción conjugada de Q sobre K es la dada a priori.

El conjunto de las clases de equivalencia de extensiones es un grupo abeliano con la suma de Baer, y por lo tanto, la biyección es un isomorfismo.

También dieron una interpretación de $H^3(Q, K)$ en términos de extensiones de grupo con núcleo no abeliano, en el que K desempeña el papel del centro del núcleo; en concreto, en términos de obstrucciones de extensiones de un núcleo no abeliano N por Q, donde el centro de N es K.

Además, $H^1(Q, K)$ está en biyección con el conjunto de las clases de Q-conjugación de productos semidirectos de K por Q.

Uno de los resultados más importantes en teoría de grupos finitos es el Teorema de Schur-Zassenhaus, que se demostró por primera vez en 1937, que establece que si K es un subgrupo normal de un grupo finito G y $(|K|, |G/K|) = 1$, entonces G es isomorfo a un producto semidirecto de K por un grupo Q isomorfo a G/K; es decir, G puede ser tratado como un tipo de extensión particularmente simple, una extensión "escindida", de K por Q.

A continuación se procede a describir la estructura de este trabajo. Este consta de cuatro capítulos, cuya estructura y contenidos se detalla a continuación.

En el Capítulo 1 se proporciona el marco teórico necesario para el desarrollo del trabajo posterior. Concretamente, se establecerán conceptos como Q-módulo y producto semidirecto, y resultados importantes para ellos, mostrando algunos ejemplos.

Después, en el Capítulo 2, se estudiarán las extensiones de grupos, presentándolas de manera general en la Sección 2.1 y estudiando el tipo más simple de extensiones, las extensiones que escinden por la derecha, en la Sección 2.2, relacionando estas con el producto semidirecto de K por Q. Además, en este capítulo se presenta el problema de la extensión y se establecen condiciones bajo las cuales su resolución se facilita: K será un Q-módulo y la extensión determinará la misma acción de Q sobre K que su estructura de Q-módulo.

El Capítulo 3 comienza introduciendo la noción de grupos de cohomología de Q con coeficientes en un Q-módulo K de cualquier dimensión utilizando fuerza bruta en la Sección 3.1. Posteriormente, se trabaja con extensiones de Q sobre K que definen la misma acción que la original de Q sobre K para interpretar el significado de los grupos de cohomología de dimensión baja. Concretamente, se presenta la solución de Schreier al problema de la extensión por medio de $H^2(Q, K)$ en la Sección 3.2, mientras que en la Sección 3.3 y la Sección 3.4 se interpretarán los grupos de dimensiones 1 y 0, respectivamente.

En el Capítulo 4, Sección 4.1, se aplicarán los resultados obtenidos al estudiar los grupos de cohomología de dimensiones bajas para dar una prueba sencilla del Teorema de Schur-Zassenhaus en el caso de que el subgrupo K sea abeliano, así como estudiar los complementos de K. Finalmente, en la Sección 4.2, se introduce una forma de cálculo de los grupos de cohomología más eficiente por medio de la construcción de resoluciones libres.

Capítulo 1

Preliminares

Este capítulo está dedicado a presentar conceptos, resultados y ejemplos que se utilizarán a lo largo de este trabajo. Algunos de estos son importantes, pero se han incluido en este capítulo porque su uso es constante durante el trabajo y porque no requieren nociones previas de extensiones de grupos o de cohomología para ser presentados.

Definición 1.1. Una sucesión de grupos y homomorfismos de grupos

$$\cdots \to G_{n+1} \xrightarrow{f_{n+1}} G_n \xrightarrow{f_n} G_{n-1} \to \cdots$$

se dice **exacta** si $\operatorname{Im} f_{n+1} = \ker f_n$ para todo $n \in \mathbb{Z}$.

Observación 1.2. Que una sucesión sea exacta significa lo siguiente: por un lado, el contenido $\operatorname{Im} f_{n+1} \subset \ker f_n$ indica que $f_n \circ f_{n+1} = 0$ para todo $n \in \mathbb{Z}$, es decir, es el homomorfismo trivial. Pero la definición es más fuerte, pues por otro, $\ker f_n \subset \operatorname{Im} f_{n+1}$ indica que sólo elementos de la imagen de f_{n+1} van al elemento neutro por f_n.

Definición 1.3. Una **sucesión exacta corta** es una sucesión exacta de la forma

$$1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1,$$

donde no es necesario nombrar a los homomorfismos $1 \to K$ ni $Q \to 1$ porque son únicos.

Proposición 1.4. *Si* $1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ *es una sucesión exacta corta, entonces* i *es inyectivo y* p *es sobreyectivo.*

Demostración. Por exactitud de la sucesión, el resultado es inmediato: el homomorfismo $1 \to K$ tiene imagen $\{1\}$, luego $\ker i = \{1\}$ e i es inyectivo. Por otro lado, $Q \to 1$ es el homomorfismo trivial, luego $\operatorname{Im} p = Q$ y p es sobreyectivo. □

Observación 1.5. El Primer Teorema de Isomorfía da lugar a $K \cong \operatorname{Im} i$ y $G/\operatorname{Im} i \cong Q$. Esta es la razón de la notación escogida para las sucesiones exactas cortas en este trabajo: $K \cong \operatorname{Im} i = \ker p$ recuerda a kernel, y el homomorfismo i a una inclusión; Q recuerda a cociente (ya que se tiene $G/\operatorname{Im} i \cong Q$), y la elección de p como homomorfismo sobreyectivo resulta acertada, pues recuerda a la proyección cociente.

Definición 1.6. Una sucesión exacta corta $1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ ***escinde por la izquierda*** si existe un homomorfismo $f : G \longrightarrow K$ tal que $f \circ i = 1_K$. Se dice que ***escinde por la derecha*** si existe un homomorfismo $j : Q \longrightarrow G$ tal que $p \circ j = 1_Q$.

Definición 1.7. Sea G un grupo y A un anillo conmutativo. Se define el ***anillo de grupo*** AG [4, pág. 38] como el conjunto formado por todas las aplicaciones $\alpha : G \longrightarrow A$ tales que $\alpha(g) = 0\ \forall g \in G$ salvo un número finito de $g \in G$ (si para $\alpha : G \longrightarrow A$ se define el ***soporte de*** α como $\operatorname{Supp} \alpha = \{g \in G \mid \alpha(g) \neq 0\}$, AG es el conjunto las aplicaciones de G en A con soporte finito) junto con las siguientes operaciones, que hacen de AG un anillo:

$$\alpha + \beta : g \mapsto \alpha(g) + \beta(g), \quad \alpha\beta : g \mapsto \sum_{\substack{h,\, k \in G \\ hk = g}} \alpha(h)\beta(k).$$

Claramente, dado que α y β tienen soporte finito, $\alpha + \beta$ también. Por otro lado, $\alpha\beta$ también tiene soporte finito pues si para un número infinito de $g \in G$ se tuviese que $\alpha\beta(g) \neq 0$, entonces para cada uno de ellos existiría al menos un par $(h, k) \in G \times G$ tal que $\alpha(h) \neq 0 \neq \beta(k)$, luego habría un número infinito de esos pares, lo cual es imposible si α y β tienen soporte finito. Comprobar que es un anillo es fácil, pues basta utilizar que A es un anillo.

Por comodidad, para cada $g \in G$, la aplicación $\delta_g \in AG$, dada por

$$\delta_g(h) = \begin{cases} 1 & \text{si} \quad g = h \\ 0 & \text{si} \quad g \neq h \end{cases}$$

se denotará por g. Además, si se considera la operación externa que lleva $(a, \alpha) \in A \times AG$ en $a\alpha \in AG$, de modo que $a\alpha : g \in G \mapsto a\alpha(g) \in A$, es inmediato que cualquier $\alpha \in AG$ se expresa de forma única como $\sum_{g \in G} a_g g$, donde $a_g = \alpha(g)$ y $a_g = 0\ \forall g \in G$ excepto un número finito. Así, AG es también un A-módulo libre (considerando la suma y la operación externa) con base G.

Usando esta última notación, si consideramos de nuevo la estructura de anillo, la suma se sigue inmediatamente de la expresión $\sum_{g \in G} a_g g$; el producto de elementos de G (esto es, de δ_g) es el mismo que en G, y el elemento neutro de G es también el neutro para el

producto en AG. El producto, llamado también ***convolución***, es la extensión por linealidad del producto en G:

$$\sum_{g\in G} a_g g \sum_{h\in G} b_h h = \sum_{g,h\in G} a_g b_h gh = \sum_{x\in G}(\sum_{g\in G} a_g b_{g^{-1}x})x.$$

Finalmente, la operación externa también se traduce a esta nueva notación de forma inmediata.

Definición 1.8 ([6])**.** Sean G (cuya operación denotaremos por $\cdot$) y K (con operación denotada por $*$) grupos. Una ***acción (por la izquierda) de*** G ***en*** K es una aplicación de $G \times K$ en K, que denotaremos por $(g, k) \mapsto gk$ y que satisface $1k = k$, $(g \cdot h)k = g(hk)$ y, adicionalmente, $g(a * b) = (ga) * (gb)$. Puede comprobarse fácilmente que esto equivale a dar un homomorfismo

$$\varphi : G \longrightarrow \mathrm{Aut}(K)$$

dado por $g \mapsto \varphi_g$, donde $\varphi_g(k) = gk$, por lo que también se dice que G actúa sobre K por automorfismos.

Ejemplo 1.9. La acción (por la izquierda) trivial se define mediante $gk = k$ para todo $g \in G$, $k \in K$. Esta se corresponde con el homomorfismo trivial: $g \mapsto 1_K$ para todo $g \in G$.

Definición 1.10. Sea G un grupo. Un ***G-módulo por la izquierda*** M [2, pág. 186] es un grupo abeliano M junto con un homomorfismo de grupos $\sigma : G \longrightarrow \mathrm{Aut}(M)$. Es decir, G actúa sobre M por automorfismos (o G actúa por la izquierda sobre M).

Diremos que M es un G-módulo ***trivial*** por la izquierda si la acción es trivial, esto es, cada elemento de G actúa como la identidad.

Observación 1.11. Para un grupo G y un grupo abeliano M es especialmente interesante considerar el anillo de grupo $\mathbb{Z}G$, ya que considerar M como G-módulo por la izquierda y como $\mathbb{Z}G$-módulo por la izquierda es, esencialmente, lo mismo. Que M sea un $\mathbb{Z}G$-módulo por la izquierda equivale a la existencia de un homomorfismo de anillos $\mathbb{Z}G \longrightarrow \mathrm{End}(M)$, con $\mathrm{End}(M)$ el anillo de endomorfismos de M (véase [4, pág. 35, Exercises 1.13]). Por otra parte, que sea G-módulo por la izquierda equivale a la existencia de un homomorfismo de grupos $G \longrightarrow \mathrm{Aut}(M)$. Dado un G-módulo por la izquierda M, si σ es el homomorfismo que lo define, como la operación adicional en $\mathrm{End}(M)$ es la suma punto a punto de homomorfismos, el homomorfismo de grupos σ se extiende por linealidad en un homomorfismo de anillos $\overline{\sigma} : \mathbb{Z}G \longrightarrow \mathrm{End}(M)$. Dicho de otra forma, la operación externa se extiende por linealidad de $G \times M$ a $\mathbb{Z}G \times M$ debido a que M es abeliano. Recíprocamente, dado un $\mathbb{Z}G$-módulo por la izquierda M definido por un homomorfismo de anillos φ, debe notarse que φ

lleva unidades en unidades. Como los elementos de G en $\mathbb{Z}G$ son invertibles, también lo son sus imágenes, por lo que estas son automorfismos. De esta manera, $\varphi|_G : G \longrightarrow \mathrm{Aut}(M)$ define un G-módulo por la izquierda. De nuevo, esto equivale a restringir la operación externa del $\mathbb{Z}G$-módulo por la izquierda M a $G \times M$.

Definición 1.12. Sea G un grupo actuando sobre otro grupo H por automorfismos, es decir, un homomorfismo $\varphi : G \longrightarrow \mathrm{Aut}(H)$. El ***producto semidirecto de H y G***, denotado por $H \rtimes G$, es el grupo sobre el conjunto $H \times G$ con la operación definida por

$$(h_1, g_1) \cdot (h_2, g_2) := (h_1\varphi(g_1)(h_2), g_1g_2), \quad h_1,\, h_2 \in H,\; g_1,\, g_2 \in G.$$

Usualmente se denota la operación por $(h_1, g_1) \cdot (h_2, g_2) := (h_1g_1h_2, g_1g_2)$, donde $g_1h_2 = \varphi(g_1)(h_2)$. En ocasiones se denota el producto semidirecto mediante $H \rtimes_\varphi G$ para indicar cuál es la acción de G en H que lo define. Sólo lo indicaremos cuando pueda no estar claro. Nótese que en caso de que H sea abeliano adquiere una estructura de G-módulo por la izquierda.

Ejemplo 1.13. En caso de que la acción sea trivial, esto es, el homomorfismo $\varphi : G \longrightarrow \mathrm{Aut}(H)$ sea trivial ($\varphi(g) = 1_H$ para todo $g \in G$), el producto semidirecto es el producto directo.

Proposición 1.14. *Si G es un grupo actuando sobre otro grupo H por automorfismos, entonces el producto semidirecto de H y G, $H \rtimes G$, es un grupo con la operación definida en la Definición 1.12.*

Demostración. En primer lugar, se tiene asociatividad. Sean (h_1, g_1), (h_2, g_2), $(h_3, g_3) \in H \rtimes K$

$$\begin{aligned}[(h_1, g_1) \cdot (h_2, g_2)] \cdot (h_3, g_3) &= (h_1g_1h_2, g_1g_2) \cdot (h_3, g_3) \\ &= (h_1g_1h_2(g_1g_2)h_3, (g_1g_2)g_3),\end{aligned}$$

$$\begin{aligned}(h_1, g_1) \cdot [(h_2, g_2) \cdot (h_3, g_3)] &= (h_1, g_1) \cdot (h_2g_2h_3, g_2g_3) \\ &= (h_1g_1(h_2g_2h_3), g_1(g_2g_3)),\end{aligned}$$

pero la acción de G en H da lugar a que $g_1(h_2g_2h_3) = (g_1h_2)(g_1(g_2h_3)) = xh_2(g_1g_2)h_3$, luego la primera componente coincide; la segunda componente coincide por la asociatividad de G.

Por otro lado, $(1, 1)$ es el elemento neutro, ya que para $(h, g) \in H \rtimes G$ tenemos

$$\begin{aligned}(h, g) \cdot (1, 1) &= (hg1, g1) = (h, g), \\ (1, 1) \cdot (h, g) &= (1\,1h, 1g) = (h, g).\end{aligned}$$

Finalmente, veamos que el inverso de (h, g) es $((g^{-1}h)^{-1}, g^{-1})$. En efecto,

$$(h,g)\cdot((g^{-1}h)^{-1},g^{-1}) = (hg(g^{-1}h)^{-1}, gg^{-1}) = (h((gg^{-1})h)^{-1},1) = (hh^{-1},1) = (1,1),$$
$$((g^{-1}h)^{-1},g^{-1})\cdot(h,g) = ((g^{-1}h)^{-1}g^{-1}h, g^{-1}g) = (1,1).$$

En consecuencia, $H \rtimes G$ es un grupo. □

Ejemplo 1.15. Denotemos por $C_n = \mathbb{Z}/n\mathbb{Z}$ el subgrupo cíclico de orden n. En primer lugar, $\mathrm{Aut}(C_n) \cong U_n$, donde U_n es el grupo multiplicativo de las unidades de $\mathbb{Z}/n\mathbb{Z}$, cuyo orden, $\phi(n)$, está determinado por la función de Euler. De esta manera, $\mathrm{Aut}(C_2) = \{1\}$ y $\mathrm{Aut}(C_3) \cong \mathbb{Z}/2\mathbb{Z}$. Definamos el producto semidirecto de C_3 y C_4 mediante el único homomorfismo no trivial $\varphi : C_4 \longrightarrow \mathrm{Aut}(C_3) \cong U_3 \cong \mathbb{Z}/2\mathbb{Z}$. Este es $\varphi(x \mod 4) = (-1)^x$ mód 3. Entonces, el producto semidirecto $C_3 \rtimes C_4$ tiene la operación

$$(a,b)\cdot(c,d) = (a + (-1)^b c, b + d).$$

Cambiamos ahora la notación de los grupos utilizados para hablar de sucesiones exactas cortas y mantener la notación indicada en la Observación 1.5. Por tanto, tomaremos grupos K y Q, y siempre definiremos acciones de Q sobre K. Además, en lo que sigue, denotaremos los elementos de K por $a, b, \ldots$ y los de Q por $x, y, \ldots$.

Proposición 1.16. *Sean K y Q grupos. Si $K \rtimes Q$ es el producto semidirecto de K y Q, entonces existe una sucesión exacta corta $1 \to K \xrightarrow{i} K \rtimes Q \xrightarrow{p} Q \to 1$ que escinde por la derecha.*

Demostración. Definir una sucesión exacta corta es inmediato, y pasa por la definición de i y p. Dado que el conjunto subyacente de $K \rtimes Q$ es $K \times Q$, definimos $i : K \longrightarrow K \rtimes Q$ por $a \mapsto (a, 1)$ y $p : K \rtimes Q \longrightarrow Q$ por $(a, x) \mapsto x$. i es un homomorfismo, ya que para a, $b \in K$, $i(ab) = (ab, 1)$, y también $i(a) \cdot i(b) = (a, 1) \cdot (b, 1) = (a\,1b, 1) = (ab, 1)$. Además, es obviamente inyectivo por definición. Por otro lado, p es también un homomorfismo, ya que la operación en $K \rtimes Q$ funciona igual que en Q en la segunda coordenada, y p se olvida de la primera. Dada su definición, p es sobreyectivo. Finalmente, la sucesión es exacta: $\ker p = \{(a, x) \in K \rtimes Q \mid p(a, x) = x = 1\} = \{(a, 1) \mid a \in K\}$, pero es obvio que $\mathrm{Im}\, i = \{(a, 1) \mid a \in K\}$, luego $\mathrm{Im}\, i = \ker p$.

Para ver que escinde por la derecha, sea $j : Q \longrightarrow K \rtimes Q$ dado por $x \mapsto (1, x)$. En primer lugar, $p \circ j(x) = p(1, x) = x$, luego $p \circ j = 1_Q$. En segundo lugar, j es un homomorfismo, pues dados x, $y \in Q$, $j(xy) = (1, xy) = (1, x) \cdot (1, y) = j(x) \cdot j(y)$. Así, se tiene el resultado. □

Proposición 1.17. *Sean K y Q grupos. Si $K \times Q$ es el producto directo de K y Q, entonces existe una sucesión exacta corta $1 \to K \xrightarrow{i} K \times Q \xrightarrow{p} Q \to 1$ que escinde por la derecha y por la izquierda.*

Demostración. La existencia de la sucesión exacta corta y la escisión por la derecha se siguen del Ejemplo 1.13 y de la Proposición 1.16. La escisión por la izquierda se prueba definiendo $\alpha : K \times Q \longrightarrow K$ por $(a, x) \mapsto a$. Claramente, $\alpha \circ i(a) = \alpha(a, 1) = a$, por lo que $\alpha \circ i = 1_K$. Por último, dado que la operación en $K \times Q$ es la dada por la acción trivial, α es un homomorfismo: dados (a, x), $(b, y) \in K \times Q$, $\alpha((a, x) \cdot (b, y)) = \alpha((ab, xy)) = ab = \alpha((a, x))\alpha((b, y))$. □

Se dirá que las sucesiones exactas cortas construidas en las proposiciones anteriores son las sucesiones exactas cortas usuales para el producto semidirecto y el producto directo.

Teorema 1.18 ([1])**.** *Sea $1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ una sucesión exacta corta. Entonces, equivalen:*

(i) La sucesión escinde por la derecha.

(ii) Existe una acción de Q sobre K, es decir, un homomorfismo $\varphi : Q \longrightarrow \mathrm{Aut}(K)$ y un isomorfismo $\theta : G \longrightarrow K \rtimes Q$ de forma que el siguiente diagrama conmuta

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{p} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_K} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle 1_Q} & & \\ 1 & \longrightarrow & K & \longrightarrow & K \rtimes Q & \longrightarrow & Q & \longrightarrow & 1, \end{array}$$

donde la sucesión exacta inferior es la usual para productos semidirectos.

Demostración. Primero, veamos $(i) \implies (ii)$: como la sucesión exacta superior escinde por la derecha, tenemos que existe $j : Q \longrightarrow G$ homomorfismo tal que $p \circ j = 1_Q$. A partir de j definiremos la acción de Q sobre K mediante conjugación. Sean $a \in K$, $x \in Q$, tomamos:

$$j(x)i(a)j(x)^{-1} = j(x)i(a)j(x^{-1}),$$

ya que j es un homomorfismo. Primero, $j(x)i(a)j(x^{-1}) \in \ker p$, pues $p(j(x)i(a)j(x^{-1})) = p(j(x))p(i(a))p(x^{-1}) = xx^{-1} = 1$. Por exactitud, $\ker p = \mathrm{Im}\, i$, luego $j(x)i(a)j(x^{-1}) = i(a')$ para un único $a' \in K$ (debido a la inyectividad de i). Luego, a' está determinado por x y a, y por tanto, definimos

$$\varphi(x)(a) = a',$$

es decir, es el único elemento que verifica $j(x)i(a)j(x^{-1}) = i(\varphi(x)(a))$.

Denotemos $\varphi(x)$ por φ_x y veamos que la aplicación $\varphi_x : K \longrightarrow K$ es tal que $\varphi_x \in \mathrm{Aut}(K)$ y que φ es un homomorfismo, obteniendo así la acción de Q sobre K. Primero, es claro que si $x = 1$ la identidad $j(1)i(a)j(1)^{-1} = i(a) = i(\varphi_x(a))$ implica que $\varphi_x(a) = a$, luego $varphi_1 = 1_K$. Veamos ahora que φ_x es un homomorfismo para cada $x \in Q$. Dados $a, \in K$, $\varphi_x(ab)$ satisface $i(\varphi_x(ab)) = j(x)i(ab)j(x^{-1})$, pero

$$\begin{aligned} j(x)i(ab)j(x^{-1}) &= j(x)i(a)i(b)j(x^{-1}) \\ &= j(x)i(a)j(x^{-1})j(x)i(b)j(x^{-1}) \\ &= i(\varphi_x(a))i(\varphi_x(b)). \end{aligned}$$

La inyectividad de i asegura que $\varphi_x(a)\varphi_x(b) = \varphi_x(ab)$. Probemos ahora que $\varphi_x \circ \varphi_y = \varphi_{xy}$, ya que esto prueba que φ es un homomorfismo y que para $x \in Q$, $\varphi_x \circ \varphi_{x^{-1}} = \varphi_1 = 1_K$, entonces $\varphi_x \in \mathrm{Aut}(K)$. Sean entonces $x, y \in Q$ y consideremos φ_{xy}. Para $a \in K$, debe verificar $j(xy)i(a)j((xy))^{-1} = i(\varphi_{xy}(a))$. Dado que

$$\begin{aligned} j(xy)i(a)j((xy))^{-1} &= j(xy)i(a)j(y^{-1}x^{-1}) \\ &= j(x)j(y)i(a)j(y^{-1})j(x^{-1}) \\ &= j(x)i(\varphi_y(a))j(x^{-1}) \\ &= i(\varphi_x(\varphi_y(a))), \end{aligned}$$

se tiene $\varphi_{xy}(a) = \varphi_x \circ \varphi_y(a)$, luego $\varphi_{xy} = \varphi_x \circ \varphi_y$. En consecuencia, $\varphi : Q \longrightarrow \mathrm{Aut}(K)$ determina una acción de Q sobre K, y entonces podemos definir $K \rtimes_\varphi Q$. Como no puede haber confusión, lo denotaremos por $K \rtimes Q$.

Ahora, construyamos un isomorfismo entre $K \rtimes Q$ y G. Definimos $\gamma : K \rtimes Q \longrightarrow G$ por

$$(a, x) \mapsto \gamma(a, x) = i(a)j(x).$$

γ es un homomorfismo, ya que dados (a, x), $(b, y) \in K \rtimes Q$,

$$\begin{aligned} \gamma((a, x) \cdot (b, y)) &= \gamma((a\varphi_x(b), xy)) \\ &= i(a\varphi_x(b))j(xy) \\ &= i(a)i(\varphi_x(b))j(x)j(y) \\ &= i(a)(j(x)i(b)j(x)^{-1})j(x)j(y) \\ &= i(a)j(x)i(b)j(y) \\ &= \gamma(a, x)\gamma(b, y). \end{aligned}$$

Por otro lado, γ es inyectiva: por ser un homomorfismo, basta comprobar que $\gamma(a, x) = 1$ implica $(a, x) = (1, 1)$. Si se aplica p a $\gamma(a, x) = i(a)j(x) = 1$, obtenemos que $p(i(a))p(j(x)) =$

$1_Q(x) = x = 1 = p(1)$, luego $x = 1$. Entonces, $i(a)j(1) = i(a) = 1$, luego $a = 1$ por la inyectividad de i. Veamos ahora que γ es sobreyectiva. Sea $g \in G$, buscamos $i(a)j(x) = g$ para cierto $a \in K$, $x \in Q$. Aplicando p de nuevo a esa igualdad, obtenemos $x = p(g)$. Pero $p(gj(p(g))^{-1}) = gg^{-1} = 1$, luego $gj(p(g))^{-1} \in \ker p = \operatorname{Im} i$, luego existe un único $a \in K$ tal que $i(a) = gj(p(g))^{-1}$. Entonces, $i(a)j(x) = g$ y γ es un isomorfismo y basta tomar $\theta = \gamma^{-1}$.

Finalmente, la conmutatividad del diagrama del enunciado es equivalente a la conmutatividad del diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{p} & Q & \longrightarrow & 1 \\ & & \uparrow{\scriptstyle 1_K} & & \uparrow{\scriptstyle \gamma} & & \uparrow{\scriptstyle 1_Q} & & \\ 1 & \longrightarrow & K & \longrightarrow & K \rtimes Q & \longrightarrow & Q & \longrightarrow & 1. \end{array}$$

La conmutatividad del primer cuadrado se comprueba viendo que $i \circ 1_k(a) = i(a) \in G$ por la parte superior del mismo, y que la parte inferior da lugar a $a \mapsto (a, 1) \mapsto i(a)j(1) = i(a)$, ya que $j(1) = 1$. La conmutatividad del segundo cuadrado se tiene viendo que, por la parte superior, para $(a, x) \in K \rtimes Q$, obtenemos $p(\gamma(a, x)) = p(i(a)j(x)) = x$, mientras que por la parte inferior se obtiene $(a, x) \mapsto x \mapsto x$.

Probemos ahora $(ii) \implies (i)$: Basta definir un homomorfismo $j : Q \longrightarrow G$ que escinda por la derecha la sucesión exacta $1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$. Recordemos que la sucesión exacta corta de la parte inferior del diagrama del enunciado escinde por la derecha por la Proposición 1.16, y que el homomorfismo construido está dado por $x \mapsto (1, x)$ para $x \in Q$. Denotemos dicho homomorfismo por $\overline{j}$. Dada la existencia del homomorfismo $\theta : G \longrightarrow K \rtimes Q$, construimos $j = \theta^{-1} \circ \overline{j}$, que es un homomorfismo por composición de homomorfismos. La conmutatividad del diagrama al invertir las flechas verticales da lugar a la igualdad $p \circ j = 1_Q$. □

Teorema 1.19 ([1])**.** *Sea* $1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ *una sucesión exacta corta. Entonces, equivalen:*

(i) La sucesión escinde por la izquierda.

(ii) Existe un isomorfismo $\theta : G \longrightarrow K \times Q$ *de forma que el siguiente diagrama conmuta*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{p} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_K} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle 1_Q} & & \\ 1 & \longrightarrow & K & \longrightarrow & K \times Q & \longrightarrow & Q & \longrightarrow & 1, \end{array}$$

donde la sucesión exacta inferior es la usual para productos directos.

Demostración. Puede encontrarse esta prueba, más sencilla que la anterior, en [1]. □

Corolario 1.20. *Sea* $1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ *una sucesión exacta corta. Si la sucesión escinde por la izquierda, entonces escinde por la derecha.*

Demostración. Se sigue inmediatamente del Teorema 1.18, el Teorema 1.19 y del hecho de que un producto directo es un producto semidirecto (Ejemplo 1.13). □

Observación 1.21. El recíproco del Corolario 1.20 no es cierto. Como hemos visto en el Ejemplo 1.15, existen productos semidirectos que no son productos directos, pues basta que la acción no sea trivial para ello.

Se tendrá el recíproco requiriendo hipótesis adicionales.

Corolario 1.22 ([1])**.** *Sea* $1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ *una sucesión exacta corta, donde* G *es un grupo abeliano. Entonces, equivalen:*

(i) La sucesión escinde por la izquierda.

(ii) La sucesión escinde por la derecha.

(iii) Existe un isomorfismo $\theta : G \longrightarrow K \times Q$ *de forma que el siguiente diagrama conmuta*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{p} & Q & \longrightarrow & 1 \\ & & {\scriptstyle 1_K}\downarrow & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle 1_Q} & & \\ 1 & \longrightarrow & K & \longrightarrow & K \times Q & \longrightarrow & Q & \longrightarrow & 1, \end{array}$$

donde la sucesión exacta inferior es la usual para productos directos.

Demostración. La construcción de j vista en el Teorema 1.18 para $x \in Q$ y $a \in K$ daba lugar a $j(x)i(a)j(x)^{-1} = i(\varphi_x(a))$, pero, en este caso, la conmutatividad de G reduce dicha expresión a $i(a) = i(\varphi_x(a))$, luego por la inyectividad de i, $a = \varphi_x(a)$ para cualquier $a \in K$, $x \in Q$, por lo que la acción $\varphi : Q \longrightarrow \mathrm{Aut}(K)$ es trivial y $K \rtimes_\varphi Q = K \times Q$, luego todas las condiciones son equivalentes. □

Definición 1.23 ([5])**.** Si G es un grupo y $K \leq G$, $C \leq G$ cumplen $K \cap C = \{1\}$ y $G = KC$, decimos que C es un ***complemento*** de K. Equivalentemente, se dice que K es un complemento de C.

Proposición 1.24. *Sea G un grupo y K un subgrupo. Equivalen:*

(i) K tiene un complemento en G.

(ii) Existe $C \leq K$ tal que todo $g \in G$ tiene una expresión única de la forma $g = kc$, con $k \in K$, $c \in C$.

Demostración. $(i) \implies (ii)$: Sea C un complemento de K. Dado $g \in G$, por tenerse $G = KC$, tenemos que $g = kc$ para $k \in K$, $c \in C$. Comprobemos que la expresión es única. Supongamos que $g = k'c'$, $k' \in K$, $c' \in C$. Entonces, $kc = k'c'$, luego $(k')^{-1}k = c'c^{-1} \in K \cap C = \{1\}$ y, así, $k = k'$, $c = c'$.

$(ii) \implies (i)$: Por tenerse que todo $g \in G$ tiene una expresión única de la forma $g = kc$, $k \in K$, $c \in C$, tenemos $G = KC$. Ahora bien, supongamos que $g \in K \cap C$. En ese caso, $k'\,1 = kc = 1\,c'$ son expresiones para g. Por unicidad de la expresión, la primera igualdad da lugar a $k = k'$ y $c = 1$. Por tanto, ahora tenemos $k\,1 = 1\,c'$, por lo que, por unicidad, $k = 1$ y $c' = 1$. Así, $g = 1$ y $K \cap C = \{1\}$. □

Definición 1.25. Sea G un grupo no abeliano. G se dice ***hamiltoniano*** si todos sus subgrupos son normales.

Ejemplo 1.26. El menor ejemplo de grupo hamiltoniano es el llamado grupo de los cuaternios, Q_8, de orden 8. Usualmente se escribe como el conjunto $Q_8 = \{1, i, j, k, -1, -i, -j, -k, \}$ con la siguiente operación:

$$1x = x1 = x, \quad \forall x \in Q_8$$

$$ij = k,\ jk = i,\ ki = j$$

$$(-1)x = x(-1) = -x, \quad \forall x \in i, j, k.$$

Ejemplo 1.27. El grupo dicíclico Dic_n, también llamado grupo diédrico binario, de orden $4n$, es el producto semidirecto $C_{2n} \rtimes C_2$. Además, Dic_n es isomorfo a Q_{4n}, por lo que $\mathrm{Dic}_2 \cong Q_8$, el grupo de los cuaternios. Por otra parte, $\mathrm{Dic}_3 = C_6 \rtimes C_2 \cong Q_{12}$.

Ejemplo 1.28. El grupo diédrico D_n de las simetrías de un polígono regular de n lados, de orden $2n$, admite la siguiente presentación: $\langle a, b \mid a^n, b^2, bab^{-1}a \rangle$.

Ejemplo 1.29. El grupo de los cuaternios de orden $4n$, denotado por Q_{4n} (el caso $n = 2$, Q_8, fue introducido en el Ejemplo 1.26), puede ser presentado de la siguiente forma: $\langle a, b \mid a^n b^{-2}, a^{2n}, b^{-1}aba \rangle$.

Capítulo 2

Extensiones de grupos y productos semidirectos

Dado un grupo G y un subgrupo normal K, sabemos que podemos "factorizar" dicho grupo en K y G/K. Dicha factorización pasa por considerar una sucesión exacta corta, en la que el homomorfismo inyectivo sea la inclusión, y el sobreyectivo, la proyección cociente. En este capítulo comenzaremos a estudiar el problema inverso: dados dos grupos K y Q, si contamos con una estructura similar a la mencionada, esto es, K es (salvo isomorfismo) subgrupo normal de cierto grupo G, y Q es (salvo isomorfismo) el cociente G/K, ¿es posible conocer G u obtener información sobre él? En el caso finito es conocido el uso del Teorema de Lagrange para obtener $|G|$, pero el objetivo es estudiar si puede obtenerse otra información.

Para ello, introduciremos la noción de extensión de grupos, y daremos algunas propiedades interesantes cuando el grupo K es abeliano, así como las extensiones que escinden por la derecha y su relación con el producto semidirecto, ya que estos serán conceptos clave para intentar dar respuesta al problema en el capítulo siguiente.

Este capítulo se basa mayormente en [5, Section C-3.1] — aunque se ha adaptado debido a los conceptos introducidos en el capítulo previo —, por lo que sólo se referenciarán resultados y definiciones obtenidos de otras fuentes.

2.1. Extensiones generales

Definición 2.1. Sean K y Q dos grupos. Se llama ***extensión* de K por Q** a una sucesión exacta corta

$$1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1.$$

Alternativamente, se dice que el grupo G, en lugar de la sucesión exacta corta, es una ***extensión* de K por Q** si contiene un subgrupo normal H tal que $H \cong K$ y $Q \cong G/H$. Para referirnos al grupo G dentro de una extensión, diremos que es el grupo central de la extensión.

Observación 2.2. Está claro que ambas definiciones son equivalentes. Por un lado, la existencia de la sucesión exacta corta implica que $i(K) = \ker p \lhd G$ y, por la sobreyectividad de p, se tiene $Q \cong G/i(K)$ (véase Observación 1.5). Recíprocamente, basta considerar, por un lado, la composición del isomorfismo entre K y H con la inclusión del subgrupo normal H en G y, por otro, la proyección cociente, obteniendo así la sucesión exacta corta buscada. Nótese entonces que, en adelante, en caso de estar usando la primera definición de extensión, se cometerá un abuso de notación al identificar $i(K)$ con K, denotando dichos elementos como si el homomorfismo i fuese una inclusión; en el caso de usar la segunda definición, se considerará que K es el subgrupo normal de G en lugar de H, siendo i nuevamente una inclusión.

Atendiendo a la Definición 2.1, todo grupo es una extensión de forma trivial: para un grupo G, es obvio que G es una extensión de G por $\{1\}$, y también lo es de $\{1\}$ por G. Sin embargo, estas extensiones no añaden ninguna información nueva y carecen de interés. Por lo tanto, en adelante, cuando se diga que un grupo es una extensión, se entenderá que posee un subgrupo normal propio no trivial del que es una extensión. Siguiendo esta convención, es inmediato ver que un grupo simple G no puede ser una extensión (no trivial), ya que si fuese una extensión de K por Q, entonces $K = \ker p \lhd G$ (cometiendo el abuso de notación mencionado anteriormente), por lo que o bien $K = G$ o bien $K = \{1\}$.

Ejemplo 2.3.

(i) Dados dos grupos K y Q, el producto directo $K \times Q$ es una extensión de K por Q, pues basta considerar $i : K \longrightarrow K \times Q$ dada por $k \mapsto (k, 1)$ y $p : K \times Q \longrightarrow Q$, $(k, q) \mapsto q$. Análogamente, también es una extensión de Q por K. Esto es, para cualesquiera dos grupos K y Q, siempre existe una extensión de K por Q y viceversa.

(ii) Consideremos los grupos $\mathbb{Z}_2$ y $\mathbb{Z}_3$. $\mathbb{Z}_6$ es una extensión de $\mathbb{Z}_3$ por $\mathbb{Z}_2$ y también de $\mathbb{Z}_2$ por $\mathbb{Z}_3$. Para la primera de ellas, tomamos los subgrupos (normales) $2\mathbb{Z}$ y $6\mathbb{Z}$ de $\mathbb{Z}$ y, aplicando el Segundo Teorema de Isomorfía, obtenemos que

$$\frac{\mathbb{Z}_6}{2\mathbb{Z}/6\mathbb{Z}} \cong \mathbb{Z}_2.$$

Así, como $|2\mathbb{Z}/6\mathbb{Z}| = 3$, aplicando la segunda definición, obtenemos el resultado buscado, y de forma análoga se obtiene la extensión $\mathbb{Z}_2$ por $\mathbb{Z}_3$. La obtención de la segunda extensión es completamente análoga.

(iii) En contraste, S_3 es una extensión de $\mathbb{Z}_3$ por $\mathbb{Z}_2$, pero **no es una extensión de** $\mathbb{Z}_2$ **por** $\mathbb{Z}_3$. Sea $H = \langle(1\ 2\ 3)\rangle = A_3 \lhd S_3$, ya que $|H| = 3$ y por tanto $(S_3 : H) = 2$. De esta manera, $H \cong \mathbb{Z}_3$ y $S_3/H \cong \mathbb{Z}_2$. Sin embargo, ninguno de los subgrupos de orden 2 de S_3 es normal, ya que se trata de tres 2-subgrupos de Sylow distintos, luego no puede tenerse la segunda extensión. Nótese, además, que $\mathbb{Z}_2$ y $\mathbb{Z}_3$ son abelianos, y mientras que $\mathbb{Z}_6$ es abeliano, S_3 no lo es.

(iv) En general, S_n es una extensión de A_n por $\mathbb{Z}_2$, pues $(S_n : A_n) = 2$, luego $S_n/A_n \cong \mathbb{Z}_2$.

Los ejemplos anteriores ilustran el problema que resolveremos, aunque imponiendo más condiciones, a partir de este punto. Esto es, dados dos grupos K y Q, llamaremos **el problema de la extensión** a clasificar todas las posibles extensiones de K por Q. Hemos visto que siempre existe el producto directo, y también que existen extensiones con grupos centrales no isomorfos de K por Q, pues $S_3 \ncong \mathbb{Z}_6$ y ambas son extensiones de $\mathbb{Z}_3$ por $\mathbb{Z}_2$. Aunque pueda parecer que la forma de clasificar las extensiones sea mediante la existencia de isomorfismos entre los grupos centrales de las mismas, esto no será suficiente; existe otra noción de equivalencia más fuerte y más natural, que presentaremos en el capítulo siguiente y que será la usada para realizar esta clasificación. Clasificar todas las extensiones posibles de K por Q es un problema difícil, por lo que la mayor parte de los resultados requieren condiciones adicionales sobre la extensión, como puede ser exigir que K sea abeliano, hipótesis con la que contaremos en la mayor parte del trabajo.

Definición 2.4. Sean G un grupo y $H < G$. Una ***transversal por la izquierda de*** H ***en*** G es un subconjunto de G consistente en exactamente un elemento de cada clase por la izquierda correspondiente a la relación de equivalencia determinada por H. Esto es, está formado por exactamente un $\tau(gH) \in gH$, $\forall gH \in G/H$. La definición es análoga en el caso de la transversal por la derecha.

Observación 2.5. Como trabajamos con un subgrupo normal K, hablaremos en este caso de una ***transversal*** de H en G, ya que las clases por la izquierda y derecha coinciden, y usaremos las clases más convenientes en cada caso.

Definición 2.6. Sea

$$1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$$

una extensión. Un ***levantamiento o sección*** es una aplicación $\ell : Q \longrightarrow G$ (no necesariamente un homomorfismo) tal que $p \circ \ell = 1_Q$.

Observación 2.7. Una transversal de K en G determina un levantamiento, y viceversa. Veamos, primero, que dada una transversal, podemos construir un levantamiento. Como p es sobreyectivo por exactitud y, además, $K = \ker p \lhd G$ (cometiendo el abuso de notación mencionado anteriormente), para cada $x \in Q$ existe $g_x \in G$ tal que $p(g_x) = x$, pero como $K = \ker p$, $p(g_x) = p(h)\ \forall h \in Kg_x$. En particular, si tomamos $\ell(x)$ como el único elemento de la transversal en dicha clase de equivalencia, obtenemos que $\ell : Q \longrightarrow G$, $x \mapsto \ell(x)$ es un levantamiento. Recíprocamente, si $\ell : Q \longrightarrow G$ es un levantamiento, veamos que $\operatorname{Im}\ell$ es una transversal. En efecto, por un lado, si Kg es una clase de equivalencia, $p(g) = x \in Q$ y, como $p \circ \ell(x) = x$, obtenemos que $p(g\ell(x)^{-1}) = 1$, por lo que $Kg = K\ell(x)$, luego toda clase de equivalencia tiene un representante en $\operatorname{Im}\ell$. Además, este es único, ya que si $x, y \in Q$ y se tiene $Kl(x) = K\ell(y)$, entonces $p(\ell(x)\ell(y)^{-1}) = 1$ y $x = y$, luego $\ell(x) = \ell(y)$.

A partir de este momento nos centraremos en el caso de que el grupo K sea abeliano, a pesar de que K es arbitrario en las extensiones que acabamos de definir. Por tanto, se utilizará notación aditiva para K y, como subgrupo de G (cometiendo el abuso de notación al identificar $i(K)$ con K si fuese necesario), usaremos dicha notación para G también, teniendo en cuenta que G puede no ser abeliano, con el objetivo de no causar confusión usando notación multiplicativa con G y aditiva con su subgrupo K.

Proposición 2.8. *Sea*

$$0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$$

una extensión de K por Q, con K abeliano, y sea $\ell : Q \longrightarrow G$ un levantamiento.

(i) Para cada $x \in Q$, la conjugación $\theta_x : K \longrightarrow K$ dada por

$$\theta_x : a \mapsto \ell(x) + a - \ell(x)$$

es independiente de la elección del levantamiento $\ell(x)$ de x.

(ii) La aplicación $\theta : Q \longrightarrow \operatorname{Aut}(K)$, dada por $x \mapsto \theta_x$, es un homomorfismo.

(iii) K es un $\mathbb{Z}Q$-módulo por la izquierda con producto por escalares definido por

$$xa = \theta_x(a) = \ell(x) + a - \ell(x).$$

Demostración. Antes de nada, nótese que escribimos a en lugar de $i(a)$ por lo visto en la Observación 2.2.

(i) Sea $\ell' : Q \longrightarrow G$ otro levantamiento. Entonces, $p \circ \ell'(x) = x \ \forall x \in Q$ y se tiene que $-\ell(x) + \ell'(x) \in \ker p = K$, luego $\ell'(x) = \ell(x) + b$, $b \in K$. Finalmente, como K es abeliano,

$$\begin{aligned} \ell'(x) + a - \ell'(x) &= \ell(x) + b + a - b - \ell(x) \\ &= \ell(x) + a - \ell(x). \end{aligned}$$

(ii) En primer lugar, θ está bien definida por *(i)* y porque $K \lhd G$, luego para $k \in K$, cada $\theta_x(k) \in K$. Además, es claro que $\theta_x \in \mathrm{Aut}(K)$ al ser una conjugación.

Veamos ahora que es un homomorfismo. En efecto, dados $x, y \in Q$ y $k \in K$ arbitrarios,

$$\theta_x(\theta_y(a)) = \theta_x(\ell(y) + a - \ell(y)) = \ell(x) + \ell(y) + a - \ell(y) - \ell(x).$$

Por otro lado,

$$\theta_{xy}(a) = \ell(xy) + a - \ell(xy).$$

Por ser p homomorfismo, $p(\ell(x) + \ell(y)) = xy = p(\ell(xy))$, por lo que $\ell(x) + \ell(y)$ y $\ell(xy)$ son levantamientos de xy y por *(i)*, $\theta_x \circ \theta_y(a) = \theta_{xy}(a)$ y $\theta(xy) = \theta(x)\theta(y)$.

(iii) Se obtiene directamente de (i), (ii), la Definición 1.10 y la Observación 1.11.

□

El homomorfismo $\theta : Q \longrightarrow \mathrm{Aut}(K)$ de la Proposición 2.8 define una acción de Q sobre K (Definición 1.8) y, por ser K abeliano, K obtiene una estructura de Q-módulo por la izquierda. Esta estructura se extiende a una de $\mathbb{Z}Q$-módulo por la izquierda al estar el homomorfismo $\mathbb{Z}Q \longrightarrow \mathrm{End}(K)$ completamente determinado por $Q \longrightarrow \mathrm{Aut}(K)$ por ser $\mathrm{Aut}(K)$ el grupo de unidades de $\mathrm{End}(M)$. Si consideramos los elementos de $\mathbb{Z}Q$, cuya forma es $\sum_{x \in Q} m_x x, m_x \in \mathbb{Z} \ \forall x \in Q$ (véase Definición 1.7), está claro que conocer xa para $x \in Q$ determina $(\sum_{x \in Q} m_x x)a$ mediante $\sum_{x \in Q} m_x(xa)$. Es decir, se extiende la operación externa de $Q \times K$ a $\mathbb{Z}Q \times K$.

Por esta razón, a partir de este momento, abreviaremos "$\mathbb{Z}Q$-módulo por la izquierda" mediante "Q-módulo por la izquierda", dada la correspondencia vista en la Observación 1.11. Pese a esta correspondencia, en ocasiones recalcaremos el uso de una de las dos estructuras.

Está claro que si K es un Q-módulo por la izquierda con operación xa para $x \in Q$, $a \in K$, esto equivale a la existencia de un homomorfismo $\theta : Q \longrightarrow \mathrm{Aut}(K)$ por definición. También puede verse directamente, ya que definiendo $\theta(x) = \theta_x : K \longrightarrow K$, con $\theta_x(a) = xa$ para $a \in K$, por las propiedades de Q-módulo, $x(a + b) = xa + xb$ y $(xx^{-1})a = 1a = a$, se

tiene $\theta_x \in \mathrm{Aut}(K)$; por $(xy)a = x(ya)$, se tiene $\theta(xy) = \theta(x) \circ \theta(y)$ y θ es un homomorfismo. Sin embargo, esta no es más que una de las formas en las que K puede ser un Q-módulo por la izquierda. Es posible que la estructura de Q-módulo otorgada por una extensión mediante la conjugación difiera de la estructura de Q-módulo original de K. Por ello, damos la siguiente definición para cuando estas coinciden:

Definición 2.9. Sea K un Q-módulo. Se dice que una extensión de K por Q ***realiza los operadores*** si para cada $x \in Q$ y $a \in K$ se tiene que

$$xa = \ell(x) + a - \ell(x),$$

siendo $\ell : Q \longrightarrow G$ cualquier levantamiento. Esto es, la operación que surge de la extensión de K por Q por ser K abeliano mediante la conjugación y que dota a K de una estructura de Q-módulo por la izquierda coincide con la operación de la estructura original de Q-módulo por la izquierda de K. En definitiva, el homomorfismo $Q \longrightarrow \mathrm{Aut}(K)$ que define la estructura de Q-módulo de K coincide con el homomorfismo θ de la Proposición 2.8. Por la Observación 1.11, esto equivale a que las estructuras de $\mathbb{Z}Q$-módulo por la izquierda coincidan.

Ejemplo 2.10. El grupo de los cuaternios Q_8 es una extensión de $\mathbb{Z}_2$ por $\mathbb{Z}_2 \times \mathbb{Z}_2$, ya que podemos tomar $K = \langle -1 \rangle \cong \mathbb{Z}_2$ y $Q = Q_8/K = \{K, iK, jK, kK\}$, que es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ pues todo elemento no neutro tiene orden 2 y es abeliano. Esta extensión realiza los operadores: la única acción $\mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathrm{Aut}(\mathbb{Z}_2) \cong \{1\}$ es la acción trivial, por lo que tanto la estructura de Q-módulo original y la determinada por la extensión deben coincidir.

2.2. Extensiones que escinden y producto semidirecto

En esta sección se tratarán las extensiones que escinden, que están relacionadas con el producto semidirecto. Estas serán las extensiones más simples que se pueden construir, por lo que tendrán gran importancia en el desarrollo posterior.

Definición 2.11. Una extensión de grupos

$$1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$$

escinde por la derecha si la sucesión exacta corta escinde por la derecha. Es decir, una extensión escinde si y sólo si existe un levantamiento que sea también un homomorfismo.

Dada la equivalencia vista entre sucesiones exactas cortas $1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ que escinden por la derecha y la existencia de una acción $\varphi : Q \longrightarrow \mathrm{Aut}(K)$ y un

isomorfismo $G \longrightarrow K \rtimes_\varphi Q$ de modo que haya conmutatividad en el diagrama planteado en el Teorema 1.18, se establece dicha equivalencia de nuevo en esta sección, para hacer hincapié en este hecho utilizando el lenguaje de extensiones.

Teorema 2.12. *Sea* $1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ *una extensión de grupos. Entonces, equivalen:*

(i) La extensión escinde por la derecha.

(ii) Existe una acción de Q *sobre* K*, es decir, un homomorfismo* $\varphi : Q \longrightarrow \mathrm{Aut}(K)$ *y un isomorfismo* $\theta : G \longrightarrow K \rtimes Q$ *de forma que el siguiente diagrama conmuta*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{\ i\ } & G & \xrightarrow{\ p\ } & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_K} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle 1_Q} & & \\ 1 & \longrightarrow & K & \longrightarrow & K \rtimes Q & \longrightarrow & Q & \longrightarrow & 1, \end{array}$$

donde la extensión de la parte inferior es la usual para productos semidirectos (véase Proposición 1.16).

Demostración. Véase Teorema 1.18. □

En el siguiente resultado se prueba una nueva equivalencia para estas extensiones, pero usando ya la notación que hemos manejado en este capítulo. Escribimos K y G de forma aditiva, Q de forma multiplicativa. Sin embargo, no se exige la conmutatividad de K.

Proposición 2.13. *Sea* G *un grupo. Equivalen:*

(i) Si $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ *es una extensión que escinde por la derecha, donde* $j : Q \longrightarrow G$ *es un homomorfismo satisfaciendo* $p \circ j = 1_Q$*.*

(ii) Existen un subgrupo normal $K' \cong K$ *y un subgrupo* $Q' \cong Q$ *de* G *de modo que* Q' *es un complemento de* K'*.*

Demostración. Antes de comenzar la demostración, nótese que usaremos notación aditiva para G.

$(i) \implies (ii)$: Por ser j un levantamiento, este determina una transversal de $\ker p = i(K)$ en G (véase la Observación 2.7), luego $i(K) \cap \mathrm{Im}\, j = \{j(1)\} = \{0\}$, ya que j es un homomorfismo. Alternativamente, si $g \in i(K) \cap j(Q)$, entonces $g = i(a) = j(x)$ para $a \in K$ y $x \in Q$, luego como $\ker p = i(K)$, $p(i(a)) = 1 = p(j(x)) = x$ y $g = j(x) = j(1) = 0$.

Por otro lado, dado $g \in G$, $p \circ j \circ p(g) = p(g)$ pues $p \circ j = 1_Q$, por lo que $p(g) = p(j \circ p(g))$, lo que implica que $g - j(p(g)) = i(a) \in i(K) = \ker p$ para cierto $a \in K$, obteniendo así que

$g = i(a) + j(p(g))$ y por tanto $G = i(K) + j(Q)$, ya que $p(g) \in Q$. Finalmente, es claro que $i(K)$, $j(Q)$ son subgrupos de G por ser i y j homomorfismos, y dado que son inyectivos, $K \cong i(K)$, $Q \cong j(Q)$.

$(ii) \implies (i)$: Si Q' es un complemento de K', por la Proposición 1.24, cada $g \in G$ tiene expresión única de la forma $g = a+x$, $a \in K'$, $x \in Q'$. Tomamos i el isomorfismo $K \longrightarrow K'$ y j el isomorfismo $Q \longrightarrow Q'$. Ahora, definimos $p : G \longrightarrow Q$ mediante $p(a+x) = j^{-1}(x)$. Por ser la expresión $g = a+x$ única, está bien definida; es sobreyectiva porque j^{-1} lo es. Además, p es un homomorfismo, ya que si consideramos $g = a+x$, $h = b+y$, con $a, b \in K'$, $x, y \in Q'$, entonces $g+h = a+x+b+y$, pero como $K' \lhd G$ y $x+b \in x+K'$, tenemos $x+K = K+x$ y que $x + b = c + x$, $c \in K'$, luego $p(a + x + b + y) = p(a + c + x + y) = j^{-1}(x + y) = j^{-1}(x)j^{-1}(y) = p(a+x)+p(b+y)$ por ser j^{-1} un homomorfismo. Por último, es inmediato que $\ker p = K'$, luego tenemos que la sucesión exacta corta $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 0$ escinde por la derecha, pues $j : Q \longrightarrow G$ es un homomorfismo y claramente $p \circ j = 1_Q$: para cada $x \in Q$, $p(j(x)) = p(0 + j(x)) = j^{-1}j(x) = x$. □

Observación 2.14. Por la Proposición 1.24, se tiene que todo $g \in G$ tiene una expresión única de la forma $g = i(a)+j(x)$, con $a \in K$, $x \in Q$. Esto no dice nada nuevo con respecto a lo que ya sabíamos para cualquier levantamiento $\ell : Q \longrightarrow G$. De hecho, si exigimos que para un levantamiento ℓ se tenga $\ell(1) = 0$, obtenemos que $G = i(K) + j(Q)$ con $i(K) \cap j(Q) = \{0\}$. La diferencia se encuentra en que no podemos asegurar que $j(Q)$ sea un subgrupo de G al no ser ℓ necesariamente un homomorfismo, lo cual es necesario para que sea un complemento de $i(K)$.

Por lo tanto, un grupo G (con notación aditiva) que sea extensión de K por Q es un producto semidirecto si $i(K)$ es un subgrupo normal de G y $j(Q)$ es un complemento de $i(K)$. Por supuesto, en el caso de que K y Q sean subgrupos de K, podemos sustituir $i(K)$ por K y $j(Q)$ por Q. Esto contrasta con el caso de los productos directos, pues en ese caso tanto $i(K)$ como $j(Q)$ deben ser subgrupos normales de G, siéndolo este último porque, por la conmutatividad del diagrama del Teorema 1.19, se tiene que $j(Q) \cong \{0\} \times Q \lhd K \times Q$, luego el isomorfismo θ asegura su normalidad. El recíproco también es cierto: si $i(K)$ y $j(Q)$ son subgrupos normales y $i(K) \cap j(Q) = \{0\}$, entonces $G = i(K) + j(Q) \cong i(K) \times j(Q)$. En un producto semidirecto, el subgrupo $j(Q)$, complemento de $i(K)$, no tiene que serlo; esto es, existen productos semidirectos que no son productos directos, pues la acción por automorfismos de Q sobre K no tiene que ser trivial. Un ejemplo sencillo es S_3: como hemos visto en el Ejemplo 2.3, S_3 es una extensión de $A_3 \cong \mathbb{Z}_3$ por $Q = \langle \tau \rangle$, siendo τ cualquier trasposición, luego $Q \cong \mathbb{Z}_2$. S_3 es un producto semidirecto, ya que $A_3 \cap Q = \{1\}$ y, además, $A_3Q = S_3$, luego Q es un complemento de A_3, con $A_3 \lhd S_3$, pero $Q \not\lhd S_3$ al no ser el único 2-Sylow.

Ejemplo 2.15.

(i) El grupo de simetrías S_n es un producto semidirecto de A_n por $Q = \langle \tau \rangle \cong \mathbb{Z}_2$, para τ cualquier trasposición, ya que $A_n \cap Q = \{1\}$, lo cual implica que $|A_n||Q| = |A_nQ| = |S_n|$, y por tanto $A_nQ = S_n$. Aunque en el caso de S_3 el subgrupo normal A_3 es abeliano por ser cíclico, en general el subgrupo alternado A_n no es abeliano, ya que no lo es para $n \geq 4$. Por tanto, como se establece en la Definición 2.11, **el subgrupo normal K no tiene por qué ser abeliano**, aunque trabajaremos con dicha hipótesis habitualmente.

(ii) El grupo diédrico D_n es un producto semidirecto de $\mathbb{Z}_n$ por $\mathbb{Z}_2$. En primer lugar, dada su presentación (véase Ejemplo 1.28) es claro que $\langle a \rangle \cong \mathbb{Z}_n$ y $\langle b \rangle \cong \mathbb{Z}_2$. $(D_n : \langle a \rangle) = 2$, luego $\langle a \rangle$ es un subgrupo normal; de $bab^{-1}a = 1$ obtenemos que $ba = a^{-1}b = a^{n-1}b$, por lo que todo elemento se puede acabar expresando de forma única como a^ib^j, $0 \leq i \leq n-1$, $0 \leq j \leq 1$ y así $\langle b \rangle$ es un complemento de $\langle a \rangle$.

(iii) Un grupo cíclico de orden primo no es un producto semidirecto, ya que no puede ser producto directo de dos subgrupos propios al ser un grupo simple. Nótese, además, que si un grupo abeliano es un producto semidirecto, sería también un producto directo.

Ahora, regresamos a las hipótesis previas: esto es, K será abeliano o un Q-módulo por la izquierda si se considera con dicha estructura previamente a considerar una extensión. Por otro lado, G se continúa escribiendo aditivamente y Q, multiplicativamente.

Recordemos que, en este caso, la acción de K sobre Q por automorfismos determina una estructura de Q-módulo por la izquierda en K al ser abeliano (Definición 1.10). Por tanto, será importante ver si las estructura de Q-módulo por la izquierda coincide con la original.

Observación 2.16. El uso de notación aditiva para K permite escribir el producto semidirecto de K y Q, $K \rtimes Q$, siendo K un Q-módulo por la izquierda, con la siguiente notación, que usaremos en adelante:

$$(a, x) + (b, y) := (a + xb, xy),$$

donde xb es la operación externa de Q-módulo por la izquierda. Como no hay confusión posible, la escribimos como xy en lugar de $x \circ y$. Con esta nueva notación, el neutro es $(0, 1)$ y el inverso de (a, x) es $(-x^{-1}a, x^{-1})$.

Proposición 2.17. *Dados un grupo Q y un Q-módulo por la izquierda K, $K \rtimes Q$ es una extensión de K por Q que escinde por la derecha y que realiza los operadores.*

Demostración. Sólo es necesario probar que realiza los operadores, pues lo demás se obtiene de la Proposición 1.16 adaptando la notación. Por tanto, tomamos la extensión usual para productos semidirectos. Veamos entonces que la extensión realiza los operadores. Para ello, debemos ver que para $a \in K$ y $x \in Q$ se tiene que $i(xa) = \ell(x) + i(a) - \ell(x)$ para cualquier levantamiento $\ell : Q \longrightarrow G$ de x, pues en este caso no se realiza la identificación de $i(K)$ con K como subgrupo de G. Para empezar, dado $x \in Q$, puede tomarse $\ell(x) = (b, x)$ para cualquier $b \in K$. Entonces,

$$\begin{aligned}
\ell(x) + i(a) - \ell(x) &= (b, x) + (a, 1) + (-x^{-1}b, x^{-1}) \\
&= (b + xa, x) + (-x^{-1}b, x^{-1}) \\
&= (b + xa - xx^{-1}b, xx^{-1}) \\
&= (b + xa - b, 1) \\
&= (b - b + xa, 1) \\
&= (xa, 1) \\
&= i(xa),
\end{aligned}$$

donde la igualdad $(b + xa - b, 1) = (b - b + xa, 1)$ se da por ser K abeliano, probando así que la extensión realiza los operadores. □

Como hemos visto, una extensión con un producto semidirecto es muy sencilla de construir (véase Proposición 1.16). El Teorema 2.12 establece una equivalencia entre extensiones de K por Q que escinden por la derecha y extensiones cuyos grupos centrales son productos semidirectos de K y Q. La acción por automorfismos de Q en K utilizada para construir el producto semidirecto es precisamente la determinada por la extensión por conjugación (Proposición 2.8). Por lo tanto, si K es un Q-módulo por la izquierda, la extensión realiza los operadores. Esto refleja la facilidad que presentan este tipo de extensiones para la clasificación que pretendemos realizar, pues si una extensión de K por Q que realice los operadores escinde por la derecha, esta es equivalente a la extensión usual del producto semidirecto de K y Q dado por dicha acción. Es decir, se resuelve el problema de la extensión para extensiones de K (un Q-módulo) por Q que realizan los operadores. Esta noción de equivalencia (más fuerte que el isomorfismo, dada por el diagrama del Teorema 2.12), que se presentará en el capítulo siguiente, será la que se utilizará para clasificar extensiones.

Ejemplo 2.18. El grupo de los cuaternios, Q_8, como hemos visto, es una extensión de $\mathbb{Z}_2$ por $\mathbb{Z}_2 \times \mathbb{Z}_2$ que realiza los operadores. Sin embargo, Q_8 no es un producto semidirecto, ya que sólo posee un elemento de orden 2, mientras que el producto semidirecto (directo en este caso) tiene siete. Por esta razón, esta extensión no escinde por la derecha.

Capítulo 3

Cohomología

En este capítulo se tratará el problema de la extensión de manera más general (es decir, más que para el caso de los productos semidirectos), pero tomando algunas de las hipótesis que habíamos utilizado ya en el capítulo anterior: dados un grupo Q y un grupo abeliano K, debemos encontrar todas las distintas extensiones

$$0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1,$$

y no únicamente las que escindan por la derecha. Ya hemos visto en la Proposición 2.8 que estas extensiones determinan una estructura de Q-módulo por la izquierda sobre K, luego también asumiremos en K una estructura de Q-módulo. Además, en el caso de las extensiones que escinden por la derecha, dicha estructura realiza los operadores y, como hemos clasificado dichas extensiones, lo haremos para todas las extensiones que queremos tratar en este capítulo utilizando también esta hipótesis.

Schreier dio solución a este problema en 1926, y será esa solución la que se presentará en este capítulo. Esta solución se alcanza mediante la construcción del segundo grupo de cohomología de Q con coeficientes en K. Por lo tanto, se dará primero una definición general para los grupos de cohomología de cualquier dimensión y después se realizará una interpretación de los grupos de cohomología de dimensiones bajas: dimensiones 2, 1 y 0, siendo la interpretación del segundo grupo de cohomología la solución de Schreier. De esta manera, puede observarse cómo estas interpretaciones coinciden con la noción general.

La interpretación de los grupos de cohomología de dimensión baja se basa en [5, Section C-3.3], mientras que la definición por fuerza bruta de los grupos de cohomología se basa en [3].

3.1. Definición de $H^n(Q, K)$ por fuerza bruta

Como se ha comentado, partimos de un grupo Q y un Q-módulo por la izquierda K (denotamos la acción que lo define por φ). Denotemos por Q^n el producto cartesiano de n copias de Q.

Definición 3.1. Una ***n*-cocadena** es una aplicación $f : Q^n \longrightarrow K$ tal que $f(x_1, \ldots, x_n) = 0$ si $x_i = 1$ para algún $i \in \{1, \ldots, n\}$. El conjunto de las n-cocadenas se denota por $C^n(Q, K)$. En el caso $n = 0$, decimos que $Q^0 = \{0\}$, luego $C^0(Q, K) \cong K$.

La condición $f(x_1, \ldots, x_n) = 0$ si $x_i = 1$ para algún $i \in \{1, \ldots, n\}$ significa que las cocadenas son normalizadas. Aunque se puede trabajar sin esta condición, resulta conveniente.

Observación 3.2. $C^n(Q, K)$ es un grupo abeliano con la suma punto a punto. Esto resulta evidente al tratarse de operaciones punto a punto en un grupo abeliano K. La función idénticamente nula es el elemento neutro, y $-f$ el inverso de $f \in C^n(Q, K)$.

Definición 3.3. Para $n \geq 0$, se define la aplicación $\delta^n_\varphi := \delta^n : C^n(Q, K) \longrightarrow C^{n+1}(Q, K)$ por

$$f \in C^n(Q, K) \mapsto \delta^n(f) : Q^{n+1} \longrightarrow K,$$

donde

$$\begin{aligned}\delta^n(f)(x_1, \ldots, x_{n+1}) =& x_1 f(x_2, \ldots, x_{n+1}) \\ &+ \sum_{1 \leq i \leq n} (-1) f(x_1, \ldots, x_{i-1}, x_i x_{i+1}, x_{i+2}, \ldots, x_{n+1}) \\ &+ (-1)^n f(x_1, \ldots, x_n).\end{aligned}$$

Proposición 3.4. *δ^n es un homomorfismo de grupos para todo $n \geq 0$.*

Demostración. El resultado es inmediato teniendo en cuenta que $f + g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n)$. El único sumando que requiere aplicar algo más es el primero: $x_1(f + g)(x_2, \ldots, x_n) = x_1(f(x_2, \ldots, x_n) + g(x_2, \ldots, x_n))$, pero por ser K un Q-módulo por la izquierda, esta última expresión es igual a $x_1 f(x_2, \ldots, x_n) + x_1 g(x_2, \ldots, x_n)$. □

Definición 3.5. Sean $n \geq 0$ y $C^n(Q, K)$, $C^{n+1}(Q, K)$ los grupos de n-cocadenas y $(n+1)$-cocadenas, respectivamente. Se dice que $f \in C^n(Q, K)$ es un ***n*-cociclo** si $\delta^n(f) = 0$. Es decir, $f \in \ker \delta^n$. El conjunto de los n-cociclos es un subgrupo de $C^n(Q, K)$ y se denota por

$$Z^n(Q, K) := \ker \delta^n.$$

Definición 3.6. Sean $n \geq 1$ y $C^{n-1}(Q,K)$, $C^n(Q,K)$ los grupos de $(n-1)$-cocadenas y n-cocadenas, respectivamente. Se dice que $f \in C^n(Q,K)$ es una n-***cofrontera*** si $f = \delta^{n-1}(g)$ para $g \in C^{n-1}(Q,K)$. Es decir, $f \in \operatorname{Im}\delta^{n-1}$. El conjunto de las n-cofronteras es un subgrupo de $C^n(Q,K)$ y se denota por

$$B^n(Q,K) := \operatorname{Im}\delta^{n-1}.$$

Diremos que $B^0(Q,K) = \{0\}$.

Proposición 3.7. *Para $n \geq 0$, $\delta^{n+1} \circ \delta^n = 0$, luego $B^{n+1}(Q,K) \leq Z^{n+1}(Q,K)$.*

Demostración. Esta demostración requiere únicamente una larga secuencia de cálculos, por lo que, si se desea, puede consultarse en [7]. □

Definición 3.8. Llamamos n-ésimo grupo de cohomología de Q con coeficientes en K (con la acción φ) al grupo

$$H^n(Q,K) = Z^n(Q,K)/B^n(Q,K).$$

Está bien definido porque $B^n(Q,K) \leq Z^n(Q,K)$ por la proposición anterior para $n > 0$ y porque $B^0(Q,K) = \{0\}$. Sus elementos son clases de n-cociclos módulo n-cofronteras.

3.2. Interpretación de $H^2(Q,K)$

La motivación para la construcción de este grupo de forma alternativa es la siguiente. Un determinado grupo G es una extensión de K por Q, y buscamos obtener propiedades suficientes de dicha extensión para reconstruirlo, pues queremos clasificar la extensión. Además, suponemos que K es un Q-módulo por la izquierda y la extensión realiza los operadores. Fijemos un levantamiento $\ell : Q \longrightarrow G$ para la extensión; este determina la transversal $\operatorname{Im}\ell$ (Observación 2.7). Por tanto, se tiene la unión disjunta $G = \cup_{x\in Q} K + \ell(x)$, y así todo $g \in G$ posee una expresión única de la forma

$$g = a + \ell(x),\ a \in K,\ x \in Q.$$

Además, por ser p un homomorfismo, $\ell(x)+\ell(y)$ y $\ell(xy)$ son levantamientos de $xy \in Q$ (son representantes de la misma clase), por lo que $\ell(x) + \ell(y) - \ell(xy) = b \in K$, luego $\ell(x) + \ell(y) = b + \ell(xy)$. Si para cada $xy \in Q$ denotamos ese $b \in K$ por $f(x,y)$, podemos hacer la siguiente definición:

Definición 3.9. Dada una extensión G de K por Q y un levantamiento $\ell : Q \longrightarrow G$ tal que $\ell(1) = 0$, diremos que un ***cociclo*** (o *factor set*, en terminología antigua) es una función $f : Q \times Q \longrightarrow K$ tal que

$$\ell(x) + \ell(y) = f(x,y) + \ell(xy),\ \text{para todo } x,\ y \in Q.$$

Observación 3.10. Puede definirse un cociclo para un levantamiento $\ell : Q \longrightarrow G$ sin exigir que $\ell(1) = 0$. Los cociclos que sí cumplen esa condición se llaman ***cociclos normalizados***. Como resulta natural tomar un levantamiento cumpliendo esa condición, utilizaremos el término cociclo para referirnos a los cociclos normalizados.

Debe notarse que una extensión puede poseer muchos levantamientos ℓ, y la definición de cociclo depende de la elección de levantamiento. En particular, si G es un producto semidirecto, sabemos que la extensión escinde por la derecha, es decir, existe un levantamiento ℓ que es un homomorfismo. En ese caso, $\ell(xy) = \ell(x) + \ell(y)$ y el cociclo asociado es idénticamente nulo. Un levantamiento que sea homomorfismo no tiene por qué ser único: por ejemplo, para S_3 (extensión de $\mathbb{Z}_3$ por $\mathbb{Z}_2$), podemos tomar ℓ_1 dado por $\ell_1(\overline{0}) = id$, $\ell_1(\overline{1}) = (1\,2)$; ℓ_2 dado por $\ell_2(\overline{0}) = id$, $\ell_2(\overline{1}) = (1\,3)$; ℓ_3 dado por $\ell_3(\overline{0}) = (1\,2\,3)$, $\ell_3(\overline{1}) = (1\,2)$, y tenemos que ℓ_1 y ℓ_2 son levantamientos (diferentes) que son homomorfismos, mientras que ℓ_3 es un levantamiento que no es un homomorfismo. Con lo cual, un cociclo puede interpretarse como una obstrucción a que un levantamiento sea un homomorfismo, y el conjunto de todos los cociclos para una extensión indica cómo una extensión escinde por la derecha o no.

Proposición 3.11. *Sea Q un grupo, K un Q-módulo por la izquierda y $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ una extensión que realiza los operadores. Si $\ell : Q \longrightarrow G$ es un levantamiento con $\ell(1) = 0$ y $f : Q \times Q \longrightarrow K$ su correspondiente cociclo, entonces*

(i) para todo x, $y \in Q$,

$$f(1, y) = 0 = f(x, 1);$$

*(ii) se cumple la **identidad del cociclo**: para todo x, $y \in Q$,*

$$f(x, y) + f(xy, z) = xf(y, z) + f(x, yz).$$

Demostración.

(i) Dado que se tiene $\ell(x) + \ell(y) = f(x, y) + \ell(xy)$ y que $\ell(1) = 0$ por ser un cociclo (normalizado), fijando $x = 1$ obtenemos $0 + \ell(y) = f(1, y) + \ell(1y)$, luego $f(1, y) = 0$. Fijando $y = 1$ se obtiene $f(x, 1) = 0$ de forma análoga.

(ii) Se sigue de aplicar la definición de cociclo y de la asociatividad de G. Para x, y, $z \in Q$, se tiene, por un lado,

$$\begin{aligned}(\ell(x) + \ell(y)) + \ell(z) &= f(x, y) + \ell(xy) + \ell(z) \\ &= f(x, y) + f(xy, z) + \ell(xyz).\end{aligned}$$

Por otro,

$$\begin{aligned}\ell(x)+(\ell(y)+\ell(z)) &= \ell(x)+f(y,z)+\ell(yz)\\ &= \ell(x)+f(y,z)-\ell(x)+\ell(x)+\ell(xyz)\\ &= xf(y,z)+\ell(x)+\ell(yz)\\ &= xf(y,z)+f(x,yz)+\ell(xyz),\end{aligned}$$

donde la penúltima igualdad se tiene porque la extensión realiza los operadores. Entonces, $f(x,y)+f(xy,z)=xf(y,z)+f(x,yz)$.

□

Resulta más interesante ver que el recíproco también es cierto, como se muestra a continuación. Este resultado generaliza también la construcción de $K \rtimes Q$ vista en la Observación 2.16.

Teorema 3.12. *Sean un grupo Q, un Q-módulo por la izquierda K, y una función $f : Q\times Q \longrightarrow K$. f es un cociclo si, y sólo si, satisface la identidad del cociclo*

$$xf(y,z)-f(xy,z)+f(x,yz)-f(x,y)=0$$

y, además, $f(1,y)=0=f(x,1)\ \forall x,y,z\in Q$. Es más, existe una extensión G de K por Q que realiza los operadores que posee un levantamiento $\ell : Q\longrightarrow G$ cuyo cociclo asociado es f, si, y sólo si, f satisface dichas identidades.

Demostración. La necesidad es la Proposición 3.11. Para ver la suficiencia, realicemos una construcción que generalice a la vista en la Observación 2.16. Sean G el conjunto de todos los pares ordenados $(a,x)\in K\times Q$ junto con la operación definida por

$$(a,x)+(b,y)=(a+xb+f(x,y),xy).$$

Es decir, f indica cómo difiere esta construcción de ser un producto semidirecto, ya que si $f=0$, tenemos que $G=K\rtimes Q$. Probemos que G es un grupo: en primer lugar, hay asociatividad, ya que

$$\begin{aligned}((a,x)+(b,y))+(c,z) &= (a+xb+f(x,y),xy)+(c,z)\\ &= (a+xb+f(x,y)+xyc+f(xy,z),xyz),\end{aligned}$$

pero también

$$\begin{aligned}(a,x)+((b,y)+(c,z)) &= (a,x)+(b+yc+f(y,z),yz)\\ &= (a+xb+xyc+xf(y,z)+f(x,yz),xyz).\end{aligned}$$

Por ser K abeliano, se obtiene, para la primera expresión, $(a + xb + xyc + f(x, y) + f(xy, z), xyz)$, y la identidad del cociclo prueba la asociatividad.

Veamos que existe elemento neutro y un inverso para cada elemento de G. Para el neutro, tomamos, como en el caso del producto semidirecto, $(0, 1)$, ya que

$$\begin{aligned}(0,1) + (a,x) &= (0 + 1a + f(1,x), 1x) = (a,x),\\ (a,x) + (0,1) &= (a + x0 + f(x,1), x1) = (a,x),\end{aligned}$$

pues se tiene que $f(1, y) = 0 = f(x, 1)\ \forall x, y \in Q$. Por otro lado, dado (a, x), veamos que su inverso es $(-x^{-1}a - x^{-1}f(x, x^{-1}), x^{-1})$. En efecto,

$$\begin{aligned}(a,x) + (-x^{-1}a - x^{-1}f(x,x^{-1}), x^{-1}) &= (a + x(-x^{-1}a - x^{-1}f(x,x^{-1})) + f(x,x^{-1}), xx^{-1})\\ &= (a - a - f(x,x^{-1}) + f(x,x^{-1}), 1)\\ &= (0,1),\end{aligned}$$

y también

$$\begin{aligned}(-x^{-1}a - x^{-1}f(x,x^{-1}), x^{-1}) + (a,x) &= (-x^{-1}a - x^{-1}f(x,x^{-1}) + x^{-1}a + f(x^{-1},x), x^{-1}x)\\ &= (-x^{-1}a + x^{-1}a - x^{-1}f(x,x^{-1}) + f(x^{-1},x), 1)\\ &= (0 - x^{-1}f(x,x^{-1}) + f(x^{-1},x), 1)\\ &= (0,1),\end{aligned}$$

ya que tomando x^{-1}, x y x^{-1} en la identidad del cociclo obtenemos que $-x^{-1}f(x, x^{-1}) + f(x^{-1}, x) = -f(x^{-1}x, x^{-1}) + f(x^{-1}, xx^{-1})$ y entonces $-f(1, x^{-1}) + f(x^{-1}, 1) = 0 + 0 = 0$. Por lo tanto, G es un grupo.

Ahora, tomando $p : G \longrightarrow Q$ definida por $p(a, x) = x$, obtenemos un homomorfismo sobreyectivo, pues la operación en la segunda componente es la misma que en Q. Además, es obvio que $\ker p = \{(a, 1) \mid a \in K\}$. Por otra parte, se toma $i : K \longrightarrow G$ definida por $i(a) = (a, 1)$, obtenemos también un homomorfismo inyectivo (pues $i(a) + i(b) = (a + 1b + f(1, 1), 1) = (a + b, 1) = i(a + b)$) y entonces se tiene una extensión $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$. De nuevo, la forma de construir la extensión es la usual.

Ahora debe verse que esta extensión realiza los operadores. Para ello, debemos ver que $i(xa) = \ell(x) + i(a) - \ell(x)$ para cualquier levantamiento $\ell : Q \longrightarrow G$. Para $x \in Q$, un

levantamiento es de la forma $(b,x),\ b\in K$ dada la expresión de p. Entonces,

$$\begin{aligned}\ell(x)+i(a)-\ell(x) &= (b,x)+(a,1)-(b,x)\\ &= (b+xa+f(x,1),x1)+(-x^{-1}b-x^{-1}f(x,x^{-1}),x^{-1})\\ &= (b+xa,x)+(-x^{-1}b-x^{-1}f(x,x^{-1}),x^{-1})\\ &= (b+xa+x(-x^{-1}b-x^{-1}f(x,x^{-1}))+f(x,x^{-1}),xx^{-1})\\ &= (b-b+xa-f(x,x^{-1})+f(x,x^{-1}),1)\\ &= (xa,1)\\ &= i(xa),\end{aligned}$$

y se tiene entonces que la extensión realiza los operadores.

Por último, probemos que f es el cociclo asociado a un levantamiento ℓ de la extensión que acabamos de definir. Sea ℓ tal que $\ell(x)=(0,x)\ \forall x\in Q$. Entonces, sea f' el cociclo determinado por ℓ. Se tiene que, por definición, para $x,\ y\in Q$,

$$\begin{aligned}f'(x,y) &= \ell(x)+\ell(y)-\ell(xy)\\ &= (0,x)+(0,y)-(0,xy)\\ &= (0+x0+f(x,y),xy)+(-(xy)^{-1}0-(xy)^{-1}f(xy,(xy)^{-1}),(xy)^{-1})\\ &= (f(x,y),xy)+(-(xy)^{-1}f(xy,(xy)^{-1}),(xy)^{-1})\\ &= (f(x,y)+xy(-(xy)^{-1}f(xy,(xy)^{-1}))+f(xy,(xy)^{-1}),xy(xy)^{-1})\\ &= (f(x,y)-f(xy,(xy)^{-1})+f(xy,(xy)^{-1}),1)\\ &= (f(x,y),1)\\ &= i(f(x,y)),\end{aligned}$$

luego se tiene el resultado. □

Observación 3.13. La identidad del cociclo indica que los cociclos reciben este nombre porque, precisamente, son 2-cociclos por la Definición 3.5. Nótese que $f(1,y)=0=f(x,1)\ \forall x,y\in Q$ indica que son n-cocadenas normalizadas.

Definición 3.14. Dados un grupo Q, un Q-módulo por la izquierda K y un cociclo f, diremos que $G(K,Q,f)$ es el grupo central de la extensión de K por Q definida en el Teorema 3.12.

Como sabemos, una extensión tiene muchos levantamientos diferentes, y a cada uno de ellos le corresponde un cociclo. El resultado anterior asegura que para Q un grupo y K con cierta estructura fijada de Q-módulo, para un cociclo determinado existe una extensión

con un levantamiento asociado a él. Esto da lugar a dos preguntas: primero, si se toman dos cociclos asociados a la misma extensión, ¿son los grupos centrales de las extensiones resultantes de aplicar el Teorema 3.12 a esos cociclos isomorfos? Y, más importante, si un cociclo proviene de una extensión, ¿es la extensión que se construye en el Teorema 3.12 la misma que la extensión de partida? La segunda de las preguntas contesta a la primera en caso afirmativo, pero es interesante explorar la primera por separado para entender cómo dos estructuras sobre $K \times Q$ definidas mediante operaciones que dependen del cociclo escogido son equivalentes.

Lema 3.15. *Sean Q un grupo, K un Q-módulo por la izquierda y G una extensión de K por Q que realiza los operadores. Sean, además, ℓ y ℓ' levantamientos y f y f' sus correspondientes cociclos. Entonces, existe una función $h : Q \longrightarrow K$ tal que $h(1) = 0$ y para cualesquiera x, $y \in Q$,*

$$f'(x,y) - f(x,y) = xh(y) - h(xy) + h(x).$$

Demostración. Primero, definamos h. Para $x \in Q$, se tiene que $\ell'(x) - \ell(x) \in K$, ya que ambos son levantamientos. Entonces, definamos $h(x) = \ell'(x) - \ell(x)$. De esta definición se obtiene inmediatamente que $h(1) = \ell'(1) - \ell(1) = 0 + 0 = 0$ pues ℓ y ℓ' son levantamientos asociados a cociclos.

Ahora bien,

$$\begin{aligned} f'(x,y) - f(x,y) &= \ell'(x) + \ell'(y) - \ell'(xy) - f(x,y) \\ &= h(x) + \ell(x) + h(y) + \ell(y) - \ell'(xy) - f(x,y), \end{aligned}$$

ya que para $x \in Q$ se tiene $\ell'(x) = h(x) + \ell(x)$. Como la extensión realiza los operadores, podemos escribir

$$\begin{aligned} f'(x,y) - f(x,y) &= h(x) + \ell(x) + h(y) + (-\ell(x) + \ell(x)) + \ell(y) - \ell'(xy) - f(x,y) \\ &= h(x) + xh(y) + \ell(x) + \ell(y) - \ell'(xy) - f(x,y) \\ &= h(x) + xh(y) + \ell(x) + \ell(y) - (h(xy) + \ell(xy)) - f(x,y) \\ &= h(x) + xh(y) + \ell(x) + \ell(y) - \ell(xy) - h(xy) - f(x,y), \end{aligned}$$

pero dado que $\ell(x) + \ell(y) - \ell(xy) = f(x,y) \in K$, $\operatorname{Im} h \subset K$ y K es un grupo abeliano, se obtiene

$$\begin{aligned} f'(x,y) - f(x,y) &= h(x) + xh(y) - h(xy) + f(x,y) - f(x,y) \\ &= h(x) + xh(y) - h(xy) \\ &= xh(y) - h(xy) + h(x). \end{aligned}$$

□

La diferencia entre dos cociclos de una extensión da lugar a la siguiente definición.

Definición 3.16. Sean Q un grupo y K un Q-módulo por la izquierda. Se dice que una aplicación $g : Q \times Q \longrightarrow K$ es una ***cofrontera*** (o *principal factor set*, en terminología antigua) si existe una aplicación $h : Q \longrightarrow K$ tal que $h(1) = 0$ y para cada x, $y \in Q$,

$$g(x,y) = xh(y) - h(xy) + h(x).$$

Observación 3.17. Igual que en el caso de los cociclos, existe una correspondencia entre las cofronteras y las 2-cofronteras vistas en la Definición 3.6. De nuevo, $h(1) = 0$ garantiza que se trata de n-cocadenas normalizadas.

Observación 3.18. Está claro que si f y f' son dos cociclos de una extensión G, entonces por el Lema 3.15, $f - f'$ (y también $f' - f$) es una cofrontera. Además, el hecho de que sean cofronteras **nos permite responder a la primera de las preguntas planteadas anteriormente**, ya que, entonces, se tiene que $G(K,Q,f) \cong G(K,Q,f')$.

En efecto, la igualdad $f'(x,y) - f(x,y) = xh(y) - h(xy) + h(x)$ nos permite definir un isomorfismo φ entre $G(K,Q,f)$ y $G(K,Q,f')$. En primer lugar, reescribiremos la igualdad anterior como $f'(x,y) - h(x) - xh(y) = f(x,y) - h(xy)$, en la que el orden de los operandos es irrelevante, ya que todo operando está en K y este es un grupo abeliano. Con esto, basta definir $\varphi : G(K,Q,f) \longrightarrow G(K,Q,f')$ mediante

$$(a,x) \mapsto (a - h(x), x).$$

Esto es, utilizamos la función h que hace de $f' - f$ una cofrontera. Así, tenemos que, por un lado

$$\begin{aligned}\varphi((a,x) + (b,y)) &= \varphi((a + xb + f(x,y), xy)) \\ &= (a + xb + f(x,y) - h(xy), xy),\end{aligned}$$

usando la definición de φ y la operación en $G(K,Q,f)$. Pero, por otro lado, usando simplemente la operación en $G(K,Q,f')$ y que K es un grupo abeliano:

$$\begin{aligned}\varphi((a,x)) + \varphi((b,y)) &= (a - h(x), x) + (b - h(y), y) \\ &= (a - h(x) + x(b - h(y)) + f'(x,y), xy) \\ &= (a + xb - h(x) - xh(y) + f'(x,y), xy).\end{aligned}$$

Finalmente, la igualdad $f'(x,y) - h(x) - xh(y) = f(x,y) - h(xy)$ permite concluir que la primera componente también coincide, por lo que φ es un homomorfismo. Es también una biyección, pues es inyectivo por definición y también es sobreyectivo, pues para $(a,x) \in G(K,Q,f')$ basta tomar $(a + h(x), x) \in G(K,Q,f)$, luego φ es un isomorfismo.

Demos respuesta ahora a la segunda de las preguntas. Su importancia recae en que, de ser la respuesta afirmativa, habremos asegurado haber encontrado todas las extensiones posibles de K por Q que realicen los operadores (con K un Q-módulo por la izquierda), ya que podemos encontrar una extensión $G(K, Q, f)$ para algún cociclo f de forma que $G \cong G(K, Q, f)$. De nuevo, es necesario recalcar que el isomorfismo no será la noción de equivalencia utilizada para clasificar extensiones. El siguiente resultado responde afirmativamente a la pregunta, y además indica que f es cualquier cociclo asociado a un levantamiento ℓ de la extensión tal que $\ell(1) = 0$.

Teorema 3.19. *Sean Q un grupo, K un Q-módulo por la izquierda y G una extensión de K por Q que realiza los operadores. Entonces, para cualquier cociclo $f : Q \times Q \longrightarrow K$ asociado a un levantamiento de la extensión, se tiene que*

$$G \cong G(K, Q, f).$$

Demostración. Sea $\ell : Q \longrightarrow G$ un levantamiento de la extensión G y $f : Q \times Q \longrightarrow K$ su cociclo asociado. Esto es, para todo x, $y \in Q$ se tiene que

$$\ell(x) + \ell(y) = f(x, y) + \ell(xy).$$

Por ser K un subgrupo de G y ℓ determinar una transversal de K en G, G es la unión disjunta $G = \cup_{x \in Q} K + \ell(x)$, y en consecuencia todo $g \in G$ tiene una expresión única de la forma $g = a + \ell(x)$ para ciertos $a \in K$, $x \in Q$. Si se define la aplicación $\varphi : G \longrightarrow G(K, Q, f)$ por

$$g = a + \ell(x) \mapsto (a, x),$$

es evidente que la unicidad de dichas expresiones para $g \in G$ hacen de φ una aplicación bien definida. Además, por definición, es una biyección. Sólo resta comprobar que se trata de un homomorfismo. Sean entonces $g = a + \ell(x)$ y $h = b + \ell(y)$, a, $b \in K$ y x, $y \in Q$:

$$\begin{aligned}
\varphi(a + \ell(x) + b + \ell(y)) &= \varphi(a + \ell(x) + b - \ell(x) + \ell(x) + \ell(y)) \\
&= \varphi(a + xb + \ell(x) + \ell(y)) \\
&= \varphi(a + xb + f(x, y) + \ell(xy)) \\
&= (a + xb + f(x, y), xy) \\
&= (a, x) + (b, y) \\
&= \varphi(a + \ell(x)) + \varphi(b + \ell(y)),
\end{aligned}$$

pues la extensión realiza los operadores. Así, φ es un isomorfismo. □

Observación 3.20. El Teorema 3.19 es similar al Teorema 2.12, visto en el capítulo anterior para las extensiones que escinden por la derecha. Aunque en este caso no se indica que el diagrama análogo al del Teorema 2.12 sea conmutativo, se verá más adelante que sí lo es. En este caso, se establece un isomorfismo para cualquier extensión que realice los operadores (K es un Q-módulo por la izquierda). Este teorema es crucial para el estudio del problema de la extensión, ya que describe toda extensión con las condiciones que hemos impuesto en términos de cociclos. Sin embargo, el resultado asegura que podemos describir la extensión en términos de cualquier cociclo asociado a un levantamiento de la extensión. Con lo cual, cada extensión admite una descripción en términos de cociclos, pero con repeticiones, pues todos los grupos $G(K,Q,f)$ para f un cociclo asociado a un levantamiento de la extensión son isomorfos por el Teorema 3.19 (y hemos visto cómo en la Observación 3.18). Además, también indica que una extensión de K por Q que realice los operadores para una estructura de Q-módulo por la izquierda fijada no puede poseer un cociclo que también lo sea para una extensión con grupo central no isomorfo al de la original. En definitiva, una extensión está definida por varios cociclos (repeticiones), y estos no pueden definir otras extensiones con grupos centrales no isomorfos.

La anterior observación da lugar a las siguientes definiciones, que permitirán clasificar todas las extensiones bajo las hipótesis que consideramos.

Definición 3.21. Sean Q un grupo y K un Q-módulo por la izquierda. Se definen

$$Z^2(Q,K) = \{f : Q \times Q \longrightarrow K \mid f \text{ es un cociclo}\},$$

$$B^2(Q,K) = \{g : Q \times Q \longrightarrow K \mid g \text{ es una cofrontera}\},$$

los conjuntos de cociclos y cofronteras, respectivamente.

Proposición 3.22. *Dados Q un grupo y K un Q-módulo por la izquierda, entonces $Z^2(Q,K)$ es un grupo abeliano cuya operación es la suma punto a punto*

$$f + f' : (x,y) \in Q \times Q \mapsto f(x,y) + f'(x,y),$$

y, además, $B^2(Q,K)$ es un subgrupo de $Z^2(Q,K)$.

Demostración. Probemos primero que es un grupo abeliano. Como se trata de una suma punto a punto de aplicaciones con codominio un grupo abeliano, K, está claro que la conmutatividad y asociatividad no es necesario comprobarlas. Por otro lado, es inmediato comprobar que 0 (la aplicación idénticamente nula) es un cociclo y que para un cociclo f, $-f$ también lo es, ya que satisfacen las identidades de la Proposición 3.11. Finalmente, $f+f'$

también satisface las identidades: $(f+f')(1,y) = f(1,y)+f'(1,y) = 0 = f(x,1)+f'(x,1) = (f+f')(x,1)$ para todo x, $y \in Q$ y

$$f(x,y) + f(xy,z) = xf(y,z) + f(x,yz),$$

$$f'(x,y) + f'(xy,z) = xf'(y,z) + f'(x,yz)$$

implican

$$(f+f')(x,y) + (f+f')(xy,z) = x(f+f')(y,z) + (f+f')(x,yz).$$

Por tanto, $Z^2(Q,K)$ es un grupo abeliano.

Para ver que $B^2(Q,K)$ es un subgrupo, primero debe comprobarse que $B^2(Q,K) \subset Z^2(Q,K)$. Sea $g \in B^2(Q,K)$ una cofrontera. Entonces, se tiene que existe una aplicación $h : Q \longrightarrow K$ tal que $h(1) = 0$ y para cada x, $y \in Q$, $g(x,y) = xh(y) - h(xy) + h(x)$. En primer lugar, $g(1,y) = 1h(y) - h(1y) + h(1) = 0 = xh(1) - h(x1) + h(x) = g(x,1)$ para todo x, $y \in Q$. En segundo lugar, se tiene la identidad del cociclo:

$$\begin{aligned} g(x,y) + g(xy,z) &= xh(y) - h(xy) + h(x) + xyh(z) - h(xyz) + h(xy) \\ &= xh(y) + h(x) + xyh(z) - h(xyz), \end{aligned}$$

ya que K es un grupo abeliano. Por otro lado, de nuevo por la conmutatividad de la suma en K,

$$\begin{aligned} xg(y,z) + g(x,yz) &= x(yh(z) - h(yz) + h(y)) + xh(yz) - h(xyz) + h(x) \\ &= xyh(z) - xh(yz) + xh(y) + xh(yz) - h(xyz) + h(x) \\ &= xyh(z) + xh(y) - h(xyz) + h(x), \end{aligned}$$

por lo que las expresiones son iguales y se cumple la identidad del cociclo. Ahora, $B^2(Q,K)$ es no vacío, ya que $g = 0$ es una cofrontera (la aplicación h asociada también es idénticamente nula). Sólo resta comprobar que, dadas $g, g' \in B^2(Q,K)$, $g - g' \in B^2(Q,K)$. Es claro que si h, $h' : Q \longrightarrow K$ son las aplicaciones que hacen de g y g' cofronteras, entonces

$$g(x,y) = xh(y) - h(xy) + h(x),$$

$$g'(x,y) = xh'(y) - h'(xy) + h'(x)$$

implican, al considerar la suma punto a punto (también para aplicaciones de Q en K),

$$(g-g')(x,y) = x(h-h')(y) - (h-h')(xy) + (h-h')(x),$$

y es obvio que $(h-h')(1) = h(1) - h'(1) = 0$. □

Como todas las extensiones con K por Q, siendo Q un grupo y K un Q-módulo por la izquierda, estaban definidas en términos de cociclos y, además, habíamos visto que todo cociclo de una extensión define dicha extensión (salvo isomorfismo) y que la diferencia entre dos de esos cociclos es una cofrontera, es evidente que la siguiente definición elimina las repeticiones.

Definición 3.23. Sea Q un grupo y K un Q-módulo por la izquierda. Se define el ***segundo grupo de cohomología de*** Q ***con coeficientes en*** K como

$$H^2(Q,K) = Z^2(Q,K)/B^2(Q,K).$$

Observación 3.24. Las definiciones de $Z^2(Q,K)$ y $B^2(Q,K)$ coinciden con las dadas en la Definición 3.5 y la Definición 3.6, por lo visto anteriormente. Entonces, el grupo $H^2(Q,K)$ es equivalente al visto en la Definición 3.8.

Definición 3.25. Sean Q un grupo y K un Q-módulo por la izquierda. Se dice que dos extensiones G y G' de K por Q que realizan los operadores ***son equivalentes*** si existen un cociclo f de G y un cociclo f' de G' tales que $f - f'$ es una cofrontera.

Ser extensiones equivalentes es una relación de equivalencia en el conjunto de las extensiones de K por Q que realizan los operadores:

(i) Obviamente se tiene la propiedad reflexiva. Tomando cualquier cociclo f, $f - f = 0$ es una cofrontera.

(ii) Si G es equivalente a G', entonces existen un cociclo f de G y un cociclo f' de G' tales que $f - f' \in B^2(Q,K)$. Pero $B^2(Q,K)$ es un subgrupo de $Z^2(Q,K)$ y entonces $-(f - f') = f' - f \in B^2(Q,K)$, por lo que G' es equivalente a G.

(iii) Supongamos que G es equivalente a G' y G' lo es a G''. Entonces, se tienen sendos cociclos f, f' y f'' tales que $f - f', f' - f'' \in B^2(Q,K)$. De nuevo, como $B^2(Q,K)$ es un subgrupo de $Z^2(Q,K)$, $(f - f') + (f' - f'') = f - f'' \in B^2(Q,K)$ y G es equivalente a G''.

Observación 3.26. Utilizando también que $B^2(Q,K)$ es un subgrupo de $Z^2(Q,K)$, puede verse que en la Definición 3.25 puede tomarse realmente cualquier par de cociclos de las dos extensiones. Si tenemos que f y f' son tales que $f - f'$ es una cofrontera, podemos tomar $\overline{f}$ un cociclo de G y $\hat{f}$ un cociclo de G' y, por el Lema 3.15, se tiene que $\overline{f} - f \in B^2(Q,K)$, $f' - \hat{f} \in B^2(Q,K)$. De esta manera, $(\overline{f} - f) + (f - f') + (f' - \hat{f}) = \overline{f} - \hat{f}$ es una cofrontera, luego puede tomarse cualquier cociclo para cada extensión.

Proposición 3.27. *Sean Q un grupo, K un Q-módulo por la izquierda y G y G' dos extensiones de K por Q que realizan los operadores. Las extensiones G y G' son equivalentes si, y sólo si, existe un isomorfismo $\gamma : G \longrightarrow G'$ que hace conmutativo el siguiente diagrama:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{p} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_K} & & \vdots{\scriptstyle \gamma} & & \downarrow{\scriptstyle 1_Q} & & \\ 0 & \longrightarrow & K & \xrightarrow{i'} & G' & \xrightarrow{p'} & Q & \longrightarrow & 1 \end{array}$$

Demostración. Veamos, primero, que **cualquier homomorfismo que haga que el diagrama conmute debe ser un isomorfismo**. Supongamos que para el homomorfismo γ el diagrama conmuta.

En primer lugar, γ es inyectivo. Sean $g, g' \in G$ tales que $\gamma(g) = \gamma(g')$ (es decir, $\gamma(g) - \gamma(g') = \gamma(g - g') = 0$ ya que γ es un homomorfismo). Entonces, como el diagrama conmuta, $\gamma(g - g') = 0$ implica que $p(g - g') = p'(\gamma(g - g')) = 1 \in Q$, luego $g - g' \in \ker p = i(K)$. Es decir, existe $a \in K$ tal que $i(a) = g - g'$. De nuevo, por conmutatividad del diagrama, $i'(a) = \gamma(i(a)) = \gamma(g - g') = 0$, por lo que, $a = 0$ al ser i e i' homomorfismos inyectivos. Entonces, $g - g' = i(0) = 0$ y $g = g'$.

En segundo lugar, γ es sobreyectivo. Sea $g' \in G'$ y busquemos un elemento $g \in G$ tal que $\gamma(g) = g'$. Como $p'(g') \in Q$ y p y p' son sobreyectivos, entonces existe $h \in G$ tal que $p(h) = p'(g')$. Por la conmutatividad del diagrama, se tiene que $p'(g') = p(h) = p'(\gamma(h))$, por lo que $p'(g' - \gamma(h)) = 1$ y $g' - \gamma(h) \in \ker p' = i'(K)$. Así, existe $a \in K$ tal que $i'(a) = g' - \gamma(h)$. De nuevo aplicando la conmutatividad del diagrama, obtenemos que $g' - \gamma(h) = i'(a) = \gamma(i(a))$ y, como γ es un homomorfismo, $g' = \gamma(i(a)) + \gamma(h) = \gamma(i(a) + h)$, por lo que $g = i(a) + h \in G$ es el antecedente buscado.

Una vez probado lo anterior, veamos la necesidad de la existencia del homomorfismo γ y la conmutatividad del diagrama en caso de que G y G' sean equivalentes. Aunque para probar que γ resulta ser un isomorfismo no hemos realizado la identificación de K con $i(K)$ e $i'(K)$ por claridad, sí lo haremos ahora. Si G y G' son equivalentes, entonces por definición existen f cociclo de G y f' cociclo de G' tales que $f - f'$ es una cofrontera. Por lo tanto, $f' - f$ también lo es. Esto es, existe una aplicación $h : Q \longrightarrow K$ tal que $h(1) = 0$ y para todo x, $y \in Q$,

$$f'(x, y) - f(x, y) = xh(y) - h(xy) + h(x).$$

Además, f y f' están asociados a sus respectivos levantamientos $\ell : Q \longrightarrow G$ y $\ell' : Q \longrightarrow G'$ y verifican

$$\ell(x) + \ell(y) = f(x, y) + \ell(xy),$$

$$\ell'(x)+\ell'(y)=f'(x,y)+\ell(xy)$$

para todo $x,\ y\in Q$. Por último, dado que G y G' vienen dados por las uniones disjuntas $G=\cup_{x\in Q}K+\ell(x)$ y $G'=\cup_{x\in Q}K+\ell'(x)$, respectivamente, se tiene que cada $g\in G$ y $g'\in G'$ tienen expresiones únicas de la forma $g=a+\ell(x)$, $g'=b+\ell'(y)$, para $a,\ b\in K$ y $x,\ y\in Q$. Construyamos ahora el homomorfismo γ. Esta construcción generaliza la realizada en el Teorema 3.19, y es completamente análoga a la realizada en la Observación 3.18. Se define $\gamma: G\longrightarrow G'$ por

$$a+\ell(x)\mapsto\gamma(a+\ell(x))=a-h(x)+\ell'(x).$$

Con esta definición, como $\ell(1)=0=\ell'(1)$, tenemos que $a\in K$ se escribe como $a+\ell(1)$ en G y $a+\ell'(1)$ en G'. De esta forma, la primera parte del diagrama conmuta, pues

$$\gamma(i(a))=\gamma(a)=\gamma(a+\ell(1))=a-h(1)+\ell'(1)=a=i'(a).$$

Con respecto a la segunda parte del diagrama, se tiene que, para $g=a+\ell(x)\in G$,

$$p'(\gamma(a+\ell(x)))=p'(a-h(x)+\ell'(x))=x=p(a+\ell(x)),$$

ya que $a,h(x)\in K$, $p\circ\ell=1_Q$ y $p'\circ\ell'=1_Q$.

Para terminar, γ es un homomorfismo, ya que, por un lado,

$$\begin{aligned}\gamma((a+\ell(x))+(b+\ell(y)))&=\gamma(a+\ell(x)+b+(-\ell(x)+\ell(x))+\ell(y))\\&=\gamma(a+xb+\ell(x)+\ell(y))\\&=\gamma(a+xb+f(x,y)+\ell(xy))\\&=a+xb+f(x,y)-h(xy)+\ell'(xy)\end{aligned}$$

al ser G una extensión que realiza los operadores. Por otro,

$$\begin{aligned}\gamma(a+\ell(x))+\gamma(b+\ell(y))&=a-h(x)+\ell'(x)+b-h(y)+\ell'(y)\\&=a-h(x)+\ell'(x)+b+(-\ell'(x)+\ell'(x))-h(y)+\ell'(y)\\&=a-h(x)+xb+\ell'(x)-h(y)+(-\ell'(x)+\ell'(x))+\ell'(y)\\&=a-h(x)+xb-xh(y)+\ell'(x)+\ell'(y)\\&=a-h(x)+xb-xh(y)+f'(x,y)+\ell'(xy).\end{aligned}$$

Reordenando ambas expresiones por ser K un grupo abeliano, obtenemos

$$\gamma((a+\ell(x))+(b+\ell(y)))=a+xb+f(x,y)-h(xy)+\ell'(xy),$$

$$\gamma(a+\ell(x))+\gamma(b+\ell(y))=a+xb+f'(x,y)-xh(y)-h(x)+\ell'(xy),$$

y ambas expresiones son iguales en virtud de la identidad $f'(x,y) - f(x,y) = xh(y) - h(xy) + h(x)$, luego γ es un homomorfismo (y por tanto un isomorfismo).

Veamos ahora la suficiencia. Supongamos que existe un isomorfismo γ que hace que el diagrama conmutativo. Es decir, $\gamma(i(a)) = \gamma(a) = a = i'(a)$ para todo $a \in K$ y $p(g) = p'(\gamma(g))$ para todo $g \in G$. En particular, para $x \in Q$ se tiene

$$p(\ell(x)) = x = p'(\gamma(\ell(x))),$$

lo cual indica que $\gamma \circ \ell : Q \longrightarrow G'$ es un levantamiento para la extensión G'. Para encontrar su cociclo asociado, basta aplicar el homomorfismo γ a la ecuación $\ell(x) + \ell(y) = f(x,y) + \ell(xy)$, pues se obtiene $\gamma \circ \ell(x) + \gamma \circ \ell(y) = \gamma \circ f(x,y) + \gamma \circ \ell(xy)$, lo cual indica que $\gamma \circ f$ es dicho cociclo. Como $f(x,y) \in K$, la conmutatividad del primer cuadrado del diagrama implica que $\gamma(f(x,y)) = f(x,y)$ para todo x, $y \in Q$. Por tanto, f es también un cociclo de la extensión G. Entonces, si se considera cualquier otro cociclo f' de la extensión G', por el Lema 3.15 se tiene que $f' - f \in B^2(Q,K)$, luego las extensiones G y G' son equivalentes. □

Observación 3.28. La última parte de la demostración de la suficiencia de la Proposición 3.27 indica que si existe un isomorfismo γ tal que el diagrama es conmutativo, entonces ambas extensiones poseen levantamientos que dan lugar al mismo cociclo. En caso de intentar probar la necesidad usando esa hipótesis, se tendría h idénticamente nula y la definición de γ no involucraría a h. De esta manera, esta es una definición equivalente de equivalencia de extensiones. Por esta razón, en algunas referencias, como Weibel [8], se definen la equivalencia de extensiones mediante la existencia de los levantamientos que dan lugar al mismo cociclo.

Nótese también que el hecho de que ambas extensiones posean levantamientos que dan lugar al mismo cociclo implica que las dos extensiones poseen los mismos cociclos. Por la Observación 3.26, pueden tomarse cualesquiera dos cociclos de G y G' para definir la equivalencia, por lo que puede verse que cualquier cociclo de G es cociclo de G' y viceversa.

Se dice que el isomorfismo γ de la Proposición 3.27 **implementa** la equivalencia de extensiones. Por ejemplo, el isomorfismo $\varphi : G \longrightarrow G(K,Q,f)$ construido en el Teorema 3.19 implementa la equivalencia, ya que el diagrama es conmutativo debido a que $\ell(1) = 0$, pues $\varphi(i(a)) = \varphi(a) = \varphi(a + \ell(1)) = (a,1) = i'(a)$ para todo $a \in K$ (conmutatividad del primer cuadrado del diagrama) y, si $g = a + \ell(x)$ para cierto $a \in K$ y $x \in Q$, $p(g) = x = p'(a,x) = p'(\varphi(a + \ell(x))) = p'(\varphi(g))$ (conmutatividad del segundo cuadrado).

Ejemplo 3.29. Hemos visto que si dos extensiones de K por Q que realizan los operadores, con K un Q-módulo por la izquierda, son equivalentes, existe un isomorfismo entre los

grupos centrales de las extensiones. Sin embargo, este ejemplo ilustra que el recíproco no es cierto: **dos extensiones cuyos grupos son isomorfos no son necesariamente equivalentes**. Por ejemplo, sea q un primo impar. Consideremos el siguiente diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{p} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_K} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle 1_Q} & & \\ 0 & \longrightarrow & K & \xrightarrow{i'} & G' & \xrightarrow{p'} & Q & \longrightarrow & 1, \end{array}$$

donde $K = \langle a \rangle$ es un grupo cíclico de orden q, $G = \langle g \rangle = G'$ es un grupo cíclico de orden q^2 y $Q = \langle x \rangle$, siendo $x = g + K$ (luego $Q = G/K$ identificando K con $i(K)$ e $i'(K)$), todos aditivos. Definimos $i(a) = qg$ para $a \in K$ y p como la proyección cociente; $i'(a) = 2qg$ para $a \in K$ y p' como la proyección cociente. Evidentemente, i es inyectiva, y también lo es i', ya que $|2qg| = q^2/\operatorname{mcd}(q^2, 2q) = q^2/q = q$, ya que q es impar.

Si existiese un isomorfismo $\gamma : G \longrightarrow G'$ que hiciese el diagrama conmutativo, entonces se tendría que $\gamma(i(a)) = \gamma(g) = 2qg = i'(a)$ por la conmutatividad del primer cuadrado. De esta manera, necesariamente debe ser $\gamma(g) = 2g$ (véase [5, Exercises C-3.12]). En consecuencia, la conmutatividad del segundo cuadrado del diagrama da lugar a $g + K = p(g) = p'(\gamma(g)) = 2g + K$. Como el único elemento idempotente de un grupo es el neutro, debe tenerse que $g + K = K$, o lo que es lo mismo, $g \in K$. Con lo cual, la conmutatividad del segundo cuadrado del diagrama no se da para todo elemento de G, y así las extensiones no son equivalentes.

A continuación se presenta el Teorema de Schreier, que resume todos los resultados vistos hasta ahora en la sección, dando por fin una clasificación de las extensiones que hemos estado estudiando.

Teorema 3.30 (**Schreier**). *Sea Q un grupo, K un Q-módulo por la izquierda, y $e(Q,K)$ la familia de todas las clases de equivalencia de extensiones de K por Q que realizan los operadores. Entonces, existe una biyección*

$$\varphi : H^2(Q,K) \longrightarrow e(Q,K),$$

en la que se lleva el 0 a la clase de la extensión que escinde por la derecha, es decir, la del producto semidirecto.

Demostración. Denotemos la clase de una extensión $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ por $[G] \in e(Q,K)$. Denotaremos también $B^2(Q,K)$ por B^2 por comodidad. Entonces, definimos $\varphi : H^2(Q,K) \longrightarrow e(Q,K)$ mediante

$$f + B^2 \mapsto [G(K,Q,f)],$$

donde f es un cociclo asociado a la extensión anterior y $G(K,Q,f)$ es la extensión construida en el Teorema 3.12. Como hemos visto después de la Observación 3.28, la extensión G es equivalente a $G(K,Q,f)$, luego $[G] = [G(K,Q,f)]$.

φ es una aplicación bien definida. En efecto, sean f y g dos cociclos tales que $f + B^2 = g + B^2$. Entonces, lo anterior equivale a que $f - g \in B^2$, por lo que cualquier par de extensiones en el que el f sea cociclo de la primera y g de la segunda serán equivalentes por la Definición 3.25. En particular, $[G(K,Q,f)] = [G(K,Q,g)]$. Al tratarse de una equivalencia, se ha probado la inyectividad también. Además, φ es sobreyectiva, ya que si tomamos $[G] \in e(Q,K)$, para cualquier cociclo f de G se tiene por el Teorema 3.19 y los comentarios posteriores a la Observación 3.28 que $[G] = [G(K,Q,f)]$ (también en la propia observación se indica que como poseen levantamientos que dan lugar al mismo cociclo, son equivalentes), por lo que $\varphi(f + B^2) = [G(K,Q,f)] = [G]$. Por último, el cociclo nulo se corresponde con el producto semidirecto, como ya se ha visto. □

Observación 3.31. Aunque el Teorema de Schreier permite clasificar todas las extensiones de K por Q que realizan los operadores, **no indica cuántas extensiones equivalentes existen**. Para ello, deben utilizarse otros resultados.

Observación 3.32. Con respecto a la clase del producto semidirecto, debe notarse que no todos los cociclos cuya imagen por φ es dicha clase son el cociclo idénticamente nulo. Cualquier cociclo $f \in B^2(Q,K)$, es decir, cualquier cofrontera, es tal que $\varphi(f+B^2(Q,K)) = [K \rtimes Q]$, y viceversa. Obsérvese, además, que para eso cociclos f (para los que se tiene que $[G(K,Q,f)] = [K \rtimes Q]$), el grupo $G(K,Q,f)$ es también una extensión que escinde por la derecha: por lo visto en la Observación 3.28, el cociclo idénticamente nulo también es cociclo de $G(K,Q,f)$ al tenerse la equivalencia, luego la extensión escinde por la derecha. Por tanto, en la clase de extensiones equivalentes a la del producto semidirecto sólo hay extensiones que escindan por la derecha y todas las sucesiones que escinden por la derecha están en esa clase.

Corolario 3.33. *Si Q es un grupo, K un Q-módulo por la izquierda y $H^2(Q,K) = \{0\}$, entonces toda extensión de K por Q que realiza los operadores escinde por la derecha.*

Demostración. Por el Teorema de Schreier 3.30, $e(Q,K)$ posee un único elemento. Como $H^2(Q,K) = Z^2(Q,K)/B^2(Q,K)$, todo cociclo de una extensión de K por Q es una cofrontera, luego por la Observación 3.32, estas extensiones (equivalentes) escinden por la derecha y su grupo central es isomorfo a un producto semidirecto. Alternativamente, sabemos que la extensión usual del producto semidirecto siempre existe, por lo que el elemento de $e(Q,K)$ es su clase de equivalencia, y entonces toda extensión de K por Q que

realiza los operadores escinde por la derecha y su grupo central es isomorfo a un producto semidirecto. □

Ejemplo 3.34. Veamos cómo es $H^2(Q, K)$ para algunas extensiones de K por Q que realizan los operadores. Denotemos el grupo cíclico de orden n por $C_n = \mathbb{Z}/n\mathbb{Z}$.

(i) Tomemos $Q = C_2$, $K = C_2$. Entonces, como los automorfismos de un grupo cíclico son $\mathrm{Aut}(C_n) \cong U_n$, siendo U_n las unidades módulo n, sólo existe la acción trivial sobre C_2. Luego, sólo tenemos un grupo de cohomología $H^2(C_2, C_2) \cong C_2$ (por [2, VI. Proposition 7.1]). Realizando la identificación de $H^2(C_2, C_2)$ con $e(C_2, C_2)$, tenemos $H^2(C_2, C_2) = \{[0 \to C_2 \to G \to C_2 \to 0] \mid G \text{ es una extensión de } C_2 \text{ por } C_2\} = \{[0 \to C_2 \to C_2 \times C_2 \to C_2 \to 0],\ [0 \to C_2 \to C_4 \to C_2 \to 0]\}$.

(ii) Para extensiones de C_3 por C_2, aplicando los argumentos anteriores, sabemos que existen dos acciones de C_2 en C_3. Por tanto, para la acción trivial, el resultado utilizado anteriormente da lugar a $H^2(C_2, C_3) = \{0\}$. Como la extensión que escinde por la derecha siempre existe, debe ser la clase del producto directo (véase Corolario 3.33), es decir $H^2(C_2, C_3) = \{[0 \to C_3 \to C_3 \times C_2 \to C_2 \to 0]\}$. Por otro lado, para la estructura de C_2-módulo no trivial de C_3, se obtiene $H^2(C_2, C_3) = \{0\}$. De nuevo, la clase es la del producto semidirecto, en este caso S_3, como hemos visto en el Capítulo 2. Así, $H^2(C_2, C_3) = \{[0 \to C_3 \to S_3 \to C_2 \to 0]\}$.

3.3. Interpretación de $H^1(Q, K)$

Como hasta ahora, consideremos un grupo Q, un Q-módulo por la izquierda K y $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ una extensión que realiza los operadores. Tomando un levantamiento $\ell : Q \longrightarrow G$, sabemos que cada $g \in G$ tiene una expresión única de la forma

$$g = a + \ell(x),$$

para $a \in K$, $x \in Q$.

Definición 3.35. Un automorfismo φ de un grupo G **estabiliza una extensión** $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ si el siguiente diagrama es conmutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{p} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_K} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_Q} & & \\ 0 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{p} & Q & \longrightarrow & 1. \end{array}$$

También se le llama a φ un **automorfismo estabilizador** de dicha extensión. Está claro que un automorfismo estabilizador es un isomorfismo que implementa la equivalencia de una extensión con ella misma. Denotaremos el conjunto de todos los automorfismos estabilizadores de una extensión de K por Q, donde K es un Q-módulo por la izquierda, por $\mathrm{Stab}(Q, K)$.

Se probará en la Proposición 3.42 que $\mathrm{Stab}(Q, K)$ no depende de la extensión, razón por la cual no se incluye ninguna referencia a la extensión en la notación.

Observación 3.36. Se tiene que $\mathrm{Stab}(Q, K)$ forma un grupo con la composición como operación: en primer lugar, es necesario notar que si φ es un automorfismo estabilizador, entonces la conmutatividad del primer cuadrado del diagrama implica $\varphi(i(a)) = \varphi(a) = a = i(a)$, es decir, $\varphi|_K = 1_K$. Por otra parte, la conmutatividad del segundo cuadrado da lugar a (tomando $g = a + \ell(x)$) $x = p(g) = p(\varphi(g))$, luego $\varphi(\ell(x)) = \ell'(x)$ para $\ell' : Q \longrightarrow G$ otro levantamiento.

Por un lado, podemos ver que la composición en una operación interna: si φ y ψ son automorfismos estabilizadores, cumplen las identidades que acabamos de ver, por lo que $\psi \circ \varphi(i(a)) = a$ y $\psi \circ \varphi(\ell(x)) = \ell'(x)$ para algún levantamiento $\ell'(x)$ de $x \in Q$. Por otro, está claro que el neutro es 1_G, ya que para 1_G el diagrama conmuta de forma trivial. Además, φ^{-1} es el inverso de φ, por lo que sólo resta ver que está en $\mathrm{Stab}(Q, K)$, pero dichas comprobaciones son triviales por lo que hemos visto. Finalmente, se tiene asociatividad porque la composición de aplicaciones es asociativa.

Proposición 3.37. *Sean Q un grupo, K un Q-módulo por la izquierda y*

$$0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$$

una extensión que realiza los operadores, siendo i la inclusión.

(i) Si $\ell : Q \longrightarrow G$ es un levantamiento, entonces todo automorfismo estabilizador $\varphi : G \longrightarrow G$ tiene la forma única

$$\varphi(a + \ell(x)) = a + d(x) + \ell(x), \tag{3.1}$$

donde $d(x) \in K$ es independiente de la elección del levantamiento ℓ.

(ii) La Ecuación (3.1) *define un automorfismo estabilizador si, y sólo si, para todo $x, y \in Q$, la aplicación $d : Q \longrightarrow K$ satisface*

$$d(xy) = d(x) + xd(y). \tag{3.2}$$

Demostración.

(i) Como $\ell : Q \longrightarrow G$ es un levantamiento, $\operatorname{Im}\ell$ es una transversal de K (i es la inclusión por conveniencia, como llevamos haciendo hasta ahora) en G, y así todo $g \in G$ tiene una expresión única de la forma $g = a + \ell(x)$, para $a \in K$, $x \in Q$. Ahora, por ser φ un homomorfismo, $\varphi(a + \ell(x)) = \varphi(a) + \varphi(\ell(x))$. Por ser φ un automorfismo estabilizador, la conmutatividad del primer cuadrado del diagrama implica $\varphi \circ i = i$, y la del segundo, $p \circ \varphi = p$. En consecuencia, $\varphi(a) = a$ para todo $a \in K$, y para $p \circ \varphi = p$ (dado que se tiene que $p(a + \ell(x)) = p(a) + p(\ell(x)) = x$, ya que $a \in K = \ker p$), se tiene que $\varphi(\ell(x)) = x$. Si lo escribimos como un elemento cualquiera de g mediante $\varphi(\ell(x)) = d(x) + \ell(y)$, con $x, y \in Q$, obtenemos que $p(d(x) + \ell(y)) = p(d(x)) + p(\ell(y)) = y$, pues de nuevo $d(x) \in \ker p$. Así, $x = y$ y $d(x) + \ell(x)$ es un levantamiento de $x \in Q$. Todo lo obtenido es análogo a lo razonado en la Observación 3.36. De esta manera, se cumple la Ecuación (3.1). Su unicidad es obvia, pues proviene de la unicidad de la expresión de cada elemento de G como $g = a + \ell(x)$ por ser G la unión disjunta $G = \cup_{x \in Q} K + \ell(x)$.

Para asegurar que d no depende del levantamiento ℓ escogido, tomemos $\ell' : Q \longrightarrow G$ otro levantamiento. De nuevo por la conmutatividad del segundo cuadrado del diagrama, tendríamos que $\varphi(\ell'(x)) = d'(x) + \ell'(x)$ para algún $d'(x) \in K$. Por ser $\ell(x)$ y $\ell'(x)$ levantamientos de $x \in Q$, se tiene que $\ell'(x) = k + \ell(x)$ para un $k \in K$. Por tanto, $k + \ell(x) - \ell'(x) = 0$, y entonces

$$\begin{aligned} d'(x) &= \varphi(\ell'(x)) - \ell'(x) \\ &= \varphi(k + \ell(x)) - \ell'(x) \\ &= \varphi(k) + \varphi(\ell(x)) - \ell'(x) \\ &= k + d(x) + \ell(x) - \ell'(x) \\ &= d(x). \end{aligned}$$

(ii) Supongamos primero que la Ecuación (3.1) define un automorfismo estabilizador y veamos que entonces d verifica la Ecuación (3.2). Por (i), d es independiente de la elección de levantamiento ℓ. Tomemos un levantamiento ℓ, por lo que $\ell(x) + \ell(y) = f(x, y) + \ell(xy)$. Entonces, podemos calcular $\varphi(\ell(x) + \ell(y))$ de ambas maneras: por

un lado,

$$\begin{aligned}\varphi(\ell(x)+\ell(y)) &= \varphi(\ell(x))+\varphi(\ell(y))\\ &= d(x)+\ell(x)+d(y)+\ell(y)\\ &= d(x)+\ell(x)+d(y)+(-\ell(x)+\ell(x))+\ell(y)\\ &= d(x)+xd(y)+\ell(x)+\ell(y)\\ &= d(x)+xd(y)+f(x,y)+\ell(xy).\end{aligned}$$

Por otro,

$$\begin{aligned}\varphi(\ell(x)+\ell(y)) &= \varphi(f(x,y)+\ell(xy))\\ &= f(x,y)+d(xy)+\ell(xy),\end{aligned}$$

ya que $f(x,y)\in K$ para todo x, $y\in Q$. Por tanto, al igualar ambas expresiones y cancelar $\ell(xy)+f(x,y)$ se obtiene el resultado.

Recíprocamente, supongamos que d satisface la Ecuación (3.2). Debemos ver que $\varphi: G\longrightarrow G$, cuya definición está dada por la Ecuación (3.1), es un automorfismo estabilizador. Recordemos que para cualquier levantamiento $\ell: Q\longrightarrow G$ cada $g\in G$ tiene una expresión única de la forma $g=a+\ell(x)$ para $a\in K$, $x\in Q$. Además, análogamente a lo visto en la demostración de la Proposición 3.27, por caza de diagrama (ver en la Definición 3.35) se puede mostrar que si φ es un homomorfismo que hace el diagrama conmutativo, entonces es un automorfismo. Comprobemos entonces que es un homomorfismo. Por un lado,

$$\begin{aligned}\varphi(a+\ell(x)+b+\ell(y)) &= \varphi(a+\ell(x)+b-\ell(x)+\ell(x)+\ell(y))\\ &= \varphi(a+xb+\ell(x)+\ell(y))\\ &= \varphi(a+xb+f(x,y)+\ell(xy))\\ &= a+xb+f(x,y)+d(xy)+\ell(xy),\end{aligned}$$

siendo $f: Q\times Q\longrightarrow K$ el cociclo asociado a ℓ (por lo que $\ell(x)+\ell(y)=f(x,y)+\ell(xy)$). Por otro lado,

$$\begin{aligned}\varphi(a+\ell(x))+\varphi(b+\ell(y)) &= a+d(x)+\ell(x)+b+d(y)+\ell(y)\\ &= a+d(x)+xb+\ell(x)+d(y)+\ell(y)\\ &= a+d(x)+xb+xd(y)+\ell(x)+\ell(y)\\ &= a+d(x)+xb+xd(y)+f(x,y)+\ell(xy),\end{aligned}$$

pues la extensión realiza los operadores. Ahora bien, K es un grupo abeliano, luego reordenando los términos en K puede verse que las expresiones son iguales al verificarse la Ecuación (3.2) y entonces φ es un homomorfismo.

Finalmente, para ver que estabiliza la extensión, tomamos un levantamiento con $\ell(1) = 0$, ya que la Ecuación (3.1) es independiente del levantamiento escogido, por lo que $\varphi(i(a)) = \varphi(a + \ell(1)) = a + d(1) + \ell(1) = a$. Debe notarse que $d(1) = 0$ porque $d(1) = d(1 \cdot 1) = d(1) + d(1)$. También se tiene que $p(a + \ell(x)) = x = p'(a + d(x) + \ell(x)) = p'(\varphi(a + \ell(x)))$ al tenerse que a, $d(x) \in K = \ker p = \ker p'$. □

Nos interesa definir aplicaciones cuyo comportamiento sean como el de d:

Definición 3.38. Sean Q un grupo y K un Q-módulo por la izquierda. Una ***derivación*** (u homomorfismo cruzado) es una aplicación $d : Q \longrightarrow K$ tal que

$$d(xy) = d(x) + xd(y)$$

para todo x, $y \in Q$. El conjunto de todas las derivaciones se denotada por $\mathrm{Der}(Q, K)$.

Observación 3.39. $\mathrm{Der}(Q, K)$ es un grupo abeliano con la suma punto a punto. Primero, $\mathrm{Der}(Q, K)$ es cerrado para la suma punto a punto, ya que si $d, d' \in \mathrm{Der}(Q, K)$, entonces $(d+d')(xy) = d(x)+xd(y)+d'(x)+xd'(y) = d(x)+d'(x)+xd(y)+xd'(y) = (d+d')(x)+x(d+d')(y)$ por ser K un Q-módulo por la izquierda. El elemento neutro es claramente $d = 0$, ya que es trivialmente una derivación, y el inverso de d es $-d$, que también es una derivación (basta invertir la ecuación y reordenar al ser K abeliano). La asociatividad y conmutatividad son consecuencias directas de que K sea grupo abeliano.

Si K es un Q-módulo trivial, entonces $\mathrm{Der}(Q, K) = \mathrm{Hom}(Q, K)$. En efecto, si es Q-módulo trivial, la condición $d(xy) = d(x) + xd(y)$ se convierte en $d(xy) = d(x) + d(y)$, luego d es un homomorfismo.

Además, debe verse que, de nuevo, escribir $xd(y) - d(xy) + d(x) = 0$ muestra que una derivación es un 1-cociclo según la Definición 3.5. Además, de nuevo se ha visto que $d(1) = 0$, por lo que es una 1-cocadena normalizada.

Ejemplo 3.40.

(i) Si Q es un grupo y K un Q-módulo por la izquierda, entonces una función $u : Q \longrightarrow K$ dada por $u(x) = xa_0 - a_0$, donde $a_0 \in K$, es una derivación:

$$\begin{aligned} u(x) + xu(y) &= xa_0 - a_0 + x(ya_0 - a_0) \\ &= xa_0 - a_0 + xya_0 - xa_0 \\ &= xya_0 - a_0 \\ &= u(xy), \end{aligned}$$

ya que K es un grupo abeliano. Las derivaciones de la forma $u(x) = xa_0 - a_0$ se llaman ***derivaciones principales***. Un caso particular de derivación principal se da cuando consideramos Q un subgrupo de G y la acción de Q sobre K es la conjugación, es decir, $xa = x + a - x$, pues entonces

$$u(x) = xa_0 - a_0 = x + a_0 - x - a_0$$

y $u(x)$ es el conmutador de x y a_0.

(ii) Si denotamos el conjunto de las derivaciones principales por $\mathrm{PDer}(Q, K)$, puede verse que son un subgrupo de $\mathrm{Der}(Q, K)$. En efecto, si $u, v \in \mathrm{PDer}(Q, K)$, entonces $u(x) = xa_0 - a_0$ y $v(x) = xb_0 - b_0$ para todo $x \in Q$ y ciertos $a_0, b_0 \in K$. Como K es abeliano, $(u - v)(x) = u(x) - v(x) = xa_0 - a_0 - xb_0 + b_0 = xa_0 - xb_0 - a_0 + b_0 = x(a_0 - b_0) - (a_0 - b_0)$, por lo que $u - v$ es una derivación principal, pues $a_0 - b_0 \in K$.

Observación 3.41. Recordemos que una 0-cocadena f se correspondía con un elemento de K. Sea ese elemento a_0. Entonces, al aplicarle δ da lugar a una derivación principal, pues es la ecuación $\delta(f)(x) = xa_0 - a_0$. Con lo cual, una derivación principal es una 1-cofrontera de acuerdo con la Definición 3.6. Que en 1 vale 0 es también evidente, luego es una 1-cocadena.

Veamos ahora lo que enunciaba en la Definición 3.35. Aunque $\mathrm{Stab}(Q, K)$ es el conjunto de los automorfismos estabilizadores de una extensión, realmente es independiente de la extensión.

Proposición 3.42. *Sean Q un grupo, K un Q-módulo por la izquierda, y $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ una extensión que realiza los operadores. Entonces, existe un isomorfismo* $\mathrm{Stab}(Q, K) \longrightarrow \mathrm{Der}(Q, K)$.

Demostración. Basta aplicar la Proposición 3.37. Sea φ un automorfismo estabilizador. Dado un levantamiento $\ell : Q \longrightarrow G$, la Proposición 3.37 *(i)* indica que φ tiene la expresión única $\varphi(a + \ell(x)) = a + d(x) + \ell(x)$ y por *(ii)* se deduce que d es una derivación, por lo que es una derivación única. Así, definimos la aplicación $\mathrm{Stab}(Q, K) \longrightarrow \mathrm{Der}(Q, K)$ mediante $\varphi \mapsto d$, y se tiene automáticamente que está bien definida por dicha unicidad. Además, es un homomorfismo, ya que para φ, ψ automorfismos estabilizadores, si denotamos por d y d' las respectivas derivaciones únicas dadas por la Proposición 3.37, tenemos $\varphi(\psi(a + \ell(x))) = \varphi(a + d'(x) + \ell(x)) = a + d'(x) + d(x) + \ell(x)$, ya que $a + d'(x) \in K$. Por tanto, reordenando por ser K abeliano, $d + d'$ es una derivación por ser $\mathrm{Der}(Q, K)$ un grupo y es la única derivación asociada a $\varphi \circ \psi$. De esta manera, si denotamos por F la aplicación $\mathrm{Stab}(Q, K) \longrightarrow \mathrm{Der}(Q, K)$ que hemos construido. $F(\varphi \circ \psi) = d + d'$ y $F(\varphi) + F(\psi) = d + d'$ y F es un homomorfismo.

Finalmente, veamos que F es un isomorfismo. Para ello, se construye la inversa tomando para $d \in \mathrm{Der}(Q,K)$ una aplicación $\varphi : G \longrightarrow G$ que definimos por $\varphi(a+\ell(x)) = a + d(x) + \ell(x)$, pues la Proposición 3.37 *(ii)* asegura que φ estabiliza la extensión. Por tanto, la aplicación dada por $d \mapsto \varphi$ es la inversa buscada. □

Observación 3.43. Aunque al definir $\mathrm{Stab}(Q,K)$ no se veía que fuese un grupo abeliano al tener la composición con la operación, el isomorfismo anterior indica que sí lo es al serlo $\mathrm{Der}(Q,K)$.

Lema 3.44. *Sean Q un grupo, K un Q-módulo por la izquierda y $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ una extensión que realiza los operadores. Entonces, una aplicación φ es un automorfismo estabilizador interior para algún $a_0 \in K$ si, y sólo si,*

$$\varphi(a+\ell(x)) = a + xa_0 - a_0 + \ell(x).$$

Demostración. Recordemos que un automorfismo interior es un automorfismo definido mediante la conjugación por un elemento (en este caso, $a_0 \in K$).

Si tomamos $d(x) = xa_0 - a_0$, tenemos que d es una derivación principal, entonces $\varphi(a+\ell(x)) = a+d(x)+\ell(x)$ y por la Proposición 3.37 φ es un automorfismo estabilizador. Además, es interior, ya que

$$a+xa_0-a_0+\ell(x) = -a_0+a+xa_0+\ell(x) = -a_0+a+\ell(x)+a_0-\ell(x)+\ell(x) = -a_0+a+\ell(x)+a_0,$$

pues K es abeliano y la extensión realiza los operadores. Entonces, $\varphi(a+\ell(x)) = -a_0 + a + \ell(x) + a_0$ y es la conjugación por $-a_0 \in K$.

Recíprocamente, si φ es un automorfismo estabilizador, por la Proposición 3.37 es tal que $\varphi(a+\ell(x)) = a + d(x) + \ell(x)$. Si además es un automorfismo interior para $a_0 \in K$, entonces $\varphi(a+\ell(x)) = a_0 + a + \ell(x) - a_0$. Pero la extensión realiza los operadores, luego $a_0+a+\ell(x)-a_0 = a_0+a-xa_0+\ell(x) = a+a_0-xa_0+\ell(x)$ y si tomamos $d(x) = a_0 - xa_0$ hemos terminado. □

Definición 3.45. Sean Q un grupo, K un Q-módulo por la izquierda. Se define el ***primer grupo de cohomología de Q con coeficientes en K*** como

$$H^1(Q,K) = \mathrm{Der}(Q,K)/\,\mathrm{PDer}(Q,K).$$

Observación 3.46. El primer grupo de cohomología clasifica los automorfismos estabilizadores de todas las extensiones de K por Q. Para un grupo G, $\mathrm{Inn}(G)$ es el subgrupo normal de automorfismos — llamados automorfismos interiores — dados por conjugación por un elemento de G y $\mathrm{Out}(G) = \mathrm{Aut}(G)/\,\mathrm{Inn}(G)$ se conoce como el grupo de automorfismos exteriores. Es decir, clases de equivalencia módulo G-conjugación. En este caso, la

Proposición 3.42 indica que $\mathrm{Der}(Q,K) \cong \mathrm{Stab}(Q,K)$, mientras que el Lema 3.44 permite afirmar que, si se define $\mathrm{Inn}(Q,K) = \mathrm{Inn}(G) \cap \mathrm{Stab}(Q,K)$ como el conjunto de los automorfismos estabilizadores interiores, entonces $\mathrm{PDer}(Q,K) \cong \mathrm{Inn}(Q,K)$ (véase [4, Lemma 9.19]), por lo que $H^1(Q,K) \cong \mathrm{Stab}(Q,K)/\mathrm{Inn}(Q,K)$, luego clasifica los automorfismos estabilizadores en clases de Q-conjugación.

3.4. Interpretación de $H^0(Q,K)$

El grupo de dimensión 0 no es un grupo complicado. De hecho, en la Sección 3.1 se pudo ver que son un subgrupo del propio K, ya que $C^0(Q,K) \cong K$. Es fácil ver que la definición que se dará a continuación es equivalente a la de la Sección 3.1.

Definición 3.47. Si Q es un grupo y K es un Q-módulo por la izquierda, definimos ***el submódulo de elementos invariantes*** por

$$K^Q = \{a \in K \mid xa = a \ \forall x \in Q\}.$$

Esto es, es el submódulo de K dado por los elementos sobre los cuales la acción de Q sobre K es trivial.

Observación 3.48. K^Q es un Q-módulo por la izquierda trivial. De hecho, es el Q-submódulo por la izquierda trivial maximal de K. Primero, veamos que es un submódulo de K. Sean $a, b \in K^Q$, $x \in Q$. Por un lado, $a + b \in K^Q$ ya que $x(a+b) = xa + xb = a + b$ por tener $a, b \in K^Q$ y ser K un Q-módulo por la izquierda. Por otra parte, $xa \in K^Q$ porque $xa = a \in K^Q$. Ver que es un Q-módulo trivial es inmediato por la propia definición de K^Q: la acción de Q sobre los elementos de K^Q es la trivial. Además, también la propia definición indica que es el Q-submódulo trivial maximal de K.

Definición 3.49. Sean Q un grupo, K un Q-módulo por la izquierda. Se define el ***grupo de cohomología de dimensión 0 de Q con coeficientes en K*** como

$$H^0(Q,K) = K^Q.$$

Observación 3.50. Como se introducía al comenzar el capítulo, es evidente que $\ker \delta^0 = K^Q$ pues, como ya se ha comentado, aplicarle δ^0 a una 0-cocadena (un elemento de K) da lugar a una derivación principal; que esta se anule indica que sobre el elemento $a_0 \in K$ que la define actúan trivialmente todos los $x \in Q$.

Capítulo 4

Aplicaciones y computación de la cohomología

En este último capítulo se mostrarán resultados útiles que se obtienen por conocer el primer o segundo grupo de cohomología de Q con coeficientes en K. En particular, estos resultados pueden aplicarse para probar el Teorema de Schur-Zassenhaus cuando se impone que K sea abeliano. Se muestra así cómo estos resultados facilitan la prueba con respecto a cuando no pueden aplicarse.

Por otra parte, se mostrará una forma más eficiente de calcular los grupos de cohomología de Q con coeficientes en K. Esta presenta similitudes con la forma general y las interpretaciones vistas en el capítulo anterior, pero se diferencia de estas en que ofrece una forma eficiente de calcular los grupos de cohomología. Nuevamente, nos centraremos en los grupos de dimensión baja.

El contenido de este capítulo se basa en [5, Section C-3.3].

4.1. El Teorema de Schur-Zassenhaus

En primer lugar, veamos cómo el Teorema de Schreier permite dar solución sencilla a otros problemas cuando el segundo grupo de cohomología de Q con coeficientes en K es conocido. Recordemos que el Corolario 3.33 establece que si $H^2(Q, K) = \{0\}$, toda extensión de K por Q que realiza los operadores escinde por la derecha.

Teorema 4.1. *Sea G un grupo finito de orden mn, con $\mathrm{mcd}(m, n) = 1$. Si K es un subgrupo normal y abeliano de orden m, entonces K tiene un complemento y G es isomorfo a un producto semidirecto.*

Demostración. Definamos el grupo $Q = G/K$. Por el Corolario 3.33, basta probar que todo cociclo $f : Q \times Q \longrightarrow K$ asociado a la extensión es una cofrontera. Para ello, dado un cociclo f arbitrario, se define $\sigma : Q \longrightarrow K$ como

$$x \in Q \mapsto \sigma(x) = \sum_{y \in Q} f(x, y).$$

σ es una aplicación bien definida, ya que la suma es finita al serlo Q y K es abeliano.

Si se suma la identidad del cociclo

$$xf(y, z) - f(xy, z) + f(x, yz) - f(x, y) = 0$$

en todo $z \in Q$, se obtiene, por ser K un Q-módulo como resultado de la extensión,

$$x\sigma(y) - \sigma(xy) + \sigma(x) - n\sigma(x) = 0,$$

ya que yz también varía en todo Q por ser la traslación por y (la aplicación de Q en Q dada por $x \mapsto yx$) una biyección, $|Q| = (G : K) = n$ y $\sum_{z \in Q} xf(y, z) = x(\sum_{z \in Q} f(y, z))$. Ahora bien, $\text{mcd}(m, n) = 1$, luego por el Teorema de Bézout existen s, $t \in \mathbb{Z}$ tales que $sm + tn = 1$. Si se define $h : Q \longrightarrow K$ por

$$h(x) = t\sigma(x),$$

se tiene que $h(1) = 0$ (ya que $f(1, y) = 0 \,\forall\, y \in Q$). Si sumamos t veces la última ecuación obtenida, tenemos (aplicando de nuevo que K es un Q-módulo),

$$xh(y) - h(xy) + h(x) = tnf(x, y),$$

luego

$$xh(y) - h(xy) + h(x) = f(x, y) - msf(x, y).$$

Sin embargo, como $sf(x, y) \in K$ y el orden de K es m, $msf(x, y) = 0$. Con lo cual, por la existencia de la aplicación h, todo f es una cofrontera. □

El siguiente resultado sólo difiere del anterior en que se elimina la hipótesis de que K sea abeliano. Por tanto, no podemos aplicar el Teorema de Schreier, lo cual complica la demostración.

Teorema 4.2 (**Teorema de Schur-Zassenhaus**). *Sea G un grupo finito de orden mn, con* $\text{mcd}(m, n) = 1$. *Si K es un subgrupo normal de orden m, entonces K tiene un complemento y G es isomorfo a un producto semidirecto.*

Demostración. Por un resultado que puede encontrarse en [5, pág. 235, Exercises C-3.2], K tiene un complemento si, y sólo si, existe un subgrupo de G de orden n. Por tanto, probaremos que dicho subgrupo existe por inducción en $m \geq 1$. Para $m = 1$ es obviamente cierto.

Sea entonces $m > 1$ y supongamos que existe un subgrupo de orden n para $m' < m$. Supongamos en primer lugar que K no es un subgrupo normal minimal, es decir, existe un subgrupo propio no trivial T de K tal que $\{1\} \subset T \lhd G$. Entonces, $K/T \lhd G/T$ por el Teorema de Correspondencia y $(G/T)/(K/T) \cong G/K$ por el Segundo Teorema de Isomorfía. Además, $|G/K| = n$. Como $T \subset K$, se tiene que $|K/T| < |K| = m$, por lo que la hipótesis de inducción asegura la existencia de un subgrupo N/T de G/T (ya que este tiene orden $m'n$, con $m/|T| = m' < m$) cuyo orden es $|N/T| = n$. Entonces, $|N| = n|T|$ y como $|T| \mid |K| = m$, se tiene que $\text{mcd}(|T|, n) = 1$, por lo que T es un subgrupo normal de N (al serlo de G) cuyo índice y orden son coprimos. Ahora bien, como $|T| < |K| = m$, la hipótesis de inducción da un subgrupo C de N, y por tanto de G, con orden n.

Por lo tanto, supongamos ahora que K es un subgrupo normal minimal de G, es decir, no existe ningún $T \lhd G$ con $\{1\} \subset T \subset K$. Sea p un divisor primo de $|K|$ y P un p-subgrupo de Sylow de K. Por el argumento de Frattini [5, pág. 38, Lemma C-1.56], tenemos que $G = KN_G(P)$, con $N_G(P) = \{g \in G \mid gPg^{-1} = P\}$, y entonces, por el Tercer Teorema de Isomorfía,

$$\begin{aligned} G/K &= KN_G(P)/K \\ &\cong N_G(P)/(K \cap N_G(P)) \\ &= N_G(P)/N_K(P). \end{aligned}$$

Con lo cual, $|N_G(P)|/|N_K(P)| = |G/K| = n$ y $|N_G(P)| = n|N_K(P)|$. Ahora bien, si $N_G(P)$ es un subgrupo propio de G, se tiene que $|N_K(P)| < m$ y por la hipótesis de inducción existe un subgrupo de $N_G(P) \leq G$ con orden n.

Supongamos entonces que $N_G(P)$ no es un subgrupo propio, es decir $N_G(P) = G$, por lo que $P \lhd G$. Como $\{1\} \leq P \leq K$, tenemos que $P = K$, pues de lo contrario K no sería un subgrupo normal minimal de G. Por ser P un p-grupo, su centro $Z(P)$ es no trivial. Por [5, pág. 32, Exercises C-1.36], tenemos que $Z(P) \lhd G$, y por el mismo argumento, $Z(P) = P = K$, o de lo contrario K no sería un subgrupo normal minimal de G. Pero en este caso, el subgrupo K es abeliano y por tanto el Teorema 4.1 nos permite obtener el resultado buscado. □

Corolario 4.3. *Si un grupo finito G tiene un p-subgrupo de Sylow normal P para algún divisor p primo de $|G|$, entonces G es isomorfo a un producto semidirecto; es decir, P tiene un complemento.*

Demostración. El resultado se obtiene directamente al observar que el orden y el índice de P son coprimos al ser un subgrupo de Sylow ($|G| = |P|(G : P)$ y $\text{mcd}(|P|, (G : P)) = 1$). □

Por otro lado, resultados sobre el primer grupo de cohomología anulándose permiten probar que los complementos mencionados en los resultados anteriores son conjugados.

Proposición 4.4. *Sean Q un grupo, K un Q-módulo por la izquierda y $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ una extensión que escinde por la derecha y que realiza los operadores. Si C y C' son complementos de K en G y $H^1(Q, K) = \{0\}$, entonces C y C' son conjugados.*

Demostración. Por ser una extensión que escinde por la derecha, G es un producto semidirecto, luego por la Proposición 2.13, existen levantamientos $\ell : Q \longrightarrow G$ y $\ell' : Q \longrightarrow G$, ambos homomorfismos, tales que $\operatorname{Im} \ell = C$ e $\operatorname{Im} \ell' = C'$. Si f y f' son los cociclos determinados por estos homomorfismos, f y f' son idénticamente 0, luego $f' - f = 0$. Por el Lema 3.15, existe $h : Q \longrightarrow G$ definida por $h(x) = \ell'(x) - \ell(x)$, tal que $f' - f$ es una cofrontera:

$$0 = f'(x, y) - f(x, y) = xh(y) - h(xy) + h(x).$$

Reordenando, es inmediato ver que h es una derivación. Por ser $H^1(Q, K) = \{0\}$, h debe ser una derivación principal, y entonces existe $a_0 \in K$ tal que

$$\ell'(x) - \ell(x) = h(x) = xa_0 - a_0$$

para todo $x \in Q$. Dado que la extensión realiza los operadores, $\ell'(x) - a_0$ en G es lo mismo que $x(-a_0) + \ell'(x) = -xa_0 + \ell'(x)$, y entonces

$$\ell(x) = a_0 - xa_0 + \ell(x) = a_0 + \ell'(x) - a_0.$$

Como las imágenes de ℓ y ℓ' son C y C', respectivamente, se concluye que estos dos últimos son conjugados por a_0. □

Podemos usar ahora este nuevo resultado para obtener un resultado adicional en el Teorema de Schur-Zassenhaus cuando imponemos que K sea abeliano.

Teorema 4.5. *Sea G un grupo finito de orden mn, con $\text{mcd}(m, n) = 1$. Si K es un subgrupo normal y abeliano de orden m, entonces G es isomorfo a un producto semidirecto de K por G/K y cualesquiera dos complementos de K son conjugados.*

Demostración. Por la Proposición 4.4 y la Proposición 2.13, basta probar que $H^1(Q, K) = \{0\}$, donde $Q = G/K$. Por supuesto, $|Q| = |G|/|K| = n$. Sea entonces $d : Q \longrightarrow K$ una derivación. Entonces,

$$d(xy) = d(x) + xd(y)$$

para todo $x, y \in Q$. Veamos que es una derivación principal. Si sumamos la ecuación anterior para todo $y \in Q$, obtenemos

$$\Delta = nd(x) + x\Delta,$$

con $\Delta = \sum_{y \in Q} d(y)$, ya que xy varía en todo Q al hacerlo y y K es un Q-módulo como resultado de la extensión. Como $\text{mcd}(m, n) = 1$, por el Teorema de Bézout, existen $s, t \in \mathbb{Z}$ tales que $sm + tn = 1$. Entonces, como $\text{Der}(Q, K)$ es un grupo,

$$d(x) = smd(x) + tnd(x) = tnd(x),$$

puesto que $d(x) \in K$, luego $md(x) = 0$ por ser m el orden de K. Sumando t veces la ecuación $\Delta = nd(x) + x\Delta$ se obtiene

$$t\Delta = tnd(x) + xt\Delta,$$

por lo que

$$d(x) = t\Delta - xt\Delta.$$

Con lo cual, si tomamos $a_0 = -t\Delta \in K$, tenemos que d es una derivación principal. □

El caso con K no abeliano resulta más complicado en este caso, por lo que no se expondrá. En [5, pág. 250] se dan indicaciones sobre cómo probarlo.

4.2. Computación de la cohomología

De nuevo, sean Q un grupo, K un Q-módulo por la izquierda y consideremos las extensiones de K por Q que realicen los operadores.

Para realizar el cálculo de la cohomología, dado que nos centraremos en dimensión baja (aunque puede extenderse a cualquier dimensión), se utilizarán las expresiones que se han ido obteniendo a lo largo de las Secciones 3.2, 3.3 y 3.4. Por tanto, para dimensión n se necesitarían expresiones de n-cociclos y n-cofronteras como los vistos en la Sección 3.1. Se irán mostrando los paralelismos con dichas expresiones para ver que se está calculando lo mismo, aunque de forma más eficiente. La principal diferencia será que, en lugar de utilizar aplicaciones de Q^n en K para calcular los grupos, se utilizarán homomorfismos de Q-módulos. De esa manera, se aprovecha también la estructura de Q-módulo del dominio,

que será un módulo libre, en lugar de únicamente la de K. Para ver en más detalle este cómputo puede consultarse [4, Section 9.3].

Como decíamos, usaremos las expresiones obtenidas en el capítulo anterior. Las expresiones obtenidas al interpretar $H^2(Q,K)$, $H^1(Q,K)$ y $H^0(Q,K)$ fueron:

$$\begin{aligned}\text{Identidad del cociclo} &: 0 = xf(y,z) - f(xy,z) + f(x,yz) - f(x,y),\\ \text{Cofrontera} &: f(x,y) = xh(y) - h(xy) + h(x),\\ \text{Derivación} &: 0 = xd(y) - d(xy) + d(x),\\ \text{Derivación principal} &: d(x) = xa_0 - a_0.\end{aligned}$$

Todas ellas están dadas por sumas alternadas; además, tanto los cociclos como las derivaciones están en el núcleo de alguna aplicación, y las cofronteras y derivaciones principales están en la imagen de otra. Evidentemente, por lo visto en el capítulo anterior, estas expresiones son análogas a las de la Sección 3.1 para n-cociclos y n-cofronteras.

Denotemos por Q^n el producto cartesiano de n copias de Q. Denotaremos los elementos de Q^n por $[x_1 \mid \cdots \mid x_n]$ en lugar de $(x_1,\ldots,x_n)$, teniendo en cuenta que cuando $n=0$, $Q^0 = \{[\,]\}$ es un conjunto de un único elemento denotado por $[\,]$. Con esta notación, los cociclos y las cofronteras son ciertas aplicaciones $Q^2 \longrightarrow K$, mientas que las derivaciones son aplicaciones $Q^1 \longrightarrow K$.

Sea ahora B_n el $\mathbb{Z}Q$-módulo libre por la izquierda con base Q^n; en particular, B_0 tiene una base de un elemento, por lo que es $B_0 \cong \mathbb{Z}Q$. Por ser Q^n una base de B_n, se tiene que existe una biyección entre las aplicaciones $f : Q^n \longrightarrow K$ y los Q-homomorfismos (dado que son ambos $\mathbb{Z}Q$-módulos por la izquierda, son Q-módulos por la izquierda, luego abreviamos los $\mathbb{Z}Q$-homomorfismos así). A cada aplicación $f : Q^n \longrightarrow K$ le corresponde un único homomorfismo $\overline{f} : B_n \longrightarrow K$. Es decir, si denotamos los morfismos del conjunto Q^n al conjunto K de la categoría de conjuntos, **Sets**, mediante $\mathrm{Hom}_{\mathbf{Sets}}(Q^n,K) = \mathbf{Fun}(Q^n,K)$ y los morfismos entre los $\mathbb{Z}Q$-módulos B_n y K de la categoría de $\mathbb{Z}Q$-módulos, $\mathbb{Z}Q$-**Mod**, mediante $\mathrm{Hom}_{\mathbb{Z}Q\text{-}\mathbf{Mod}}(B_n,K)$, tenemos que la aplicación $f \mapsto \overline{f}$ da lugar a una biyección

$$\mathbf{Fun}(Q^n,K) \longrightarrow \mathrm{Hom}_{\mathbb{Z}Q\text{-}\mathbf{Mod}}(B_n,K),$$

donde la inversa es la restricción a Q^n de los Q-homomorfismos. Es una aplicación

$$\mathrm{res} : \mathrm{Hom}_{\mathbb{Z}Q\text{-}\mathbf{Mod}}(B_n,K) \longrightarrow \mathbf{Fun}(Q^n,K)$$

dada por $g \mapsto g|_{Q^n}$.

Definamos ahora aplicaciones según las identidades vistas anteriormente para los Q-módulos que hemos considerado. Para ello, basta definirlas sobre una base, como acabamos

de ver, pues se extienden por linealidad a Q-homomorfismos:

$$\begin{aligned} d_3 &: B_3 \longrightarrow B_2 : d_3[x \mid y \mid z] = x[y \mid z] - [xy \mid z] + [x \mid yz] - [x \mid y] \\ d_2 &: B_2 \longrightarrow B_1 : d_2[x \mid y] = x[y] - [xy] + [x] \\ d_1 &: B_1 \longrightarrow B_0 : d_1[x] = x[\,] - [\,] \end{aligned} \tag{4.1}$$

Proposición 4.6. *Para Q un grupo existe un isomorfismo $\mathbb{Z}Q/\ker\varepsilon' \cong \mathbb{Z}$, donde $\mathbb{Z}$ se considera como un Q-módulo trivial y $\varepsilon' : \mathbb{Z}Q \longrightarrow \mathbb{Z}$ se define como*

$$\varepsilon' : \sum_{x\in Q} m_x x \in \mathbb{Z}Q \mapsto \sum_{x\in Q} m_x \in \mathbb{Z}.$$

Demostración. Primero, debe notarse que cualquier grupo abeliano puede considerarse como un G-módulo trivial por la izquierda o por la derecha. En particular, podemos considerar $\mathbb{Z}$ como un Q-módulo trivial por la izquierda. Por otra parte, $\mathbb{Z}Q$ puede considerarse como un $\mathbb{Z}Q$-módulo por la izquierda (libre con base $\{1\}$), luego es también un Q-módulo por la izquierda. Entonces, para comprobar que se tiene tal isomorfismo, basta con probar que ε' es un homomorfismo de Q-módulos, ya que ε' es evidentemente sobreyectivo. Por definición de ε' se tiene que para $x \in Q$ $\varepsilon'(x) = 1$, ya que $m_y = 1$ si $y = x$ y $m_y = 0$ en otro caso. Por otra parte, $\varepsilon'(x) = \varepsilon'(x \cdot 1) = x\varepsilon'(1) = 1$, utilizando que la acción de Q sobre $\mathbb{Z}$ es trivial. El resto del comportamiento de la aplicación puede obtenerse extendiendo por linealidad, luego es un homomorfismo de Q-módulos. □

Observación 4.7. A la aplicación ε' anterior se le conoce como **aumentación** de $\mathbb{Z}Q$ (véase [2, pág. 187]). Cuando se considera como homomorfismo de anillos se le llama a $\ker\varepsilon'$ el **ideal aumentación** de Q. Nosotros la consideramos como homomorfismo de Q-módulos por la izquierda por conveniencia.

Proposición 4.8. *Si $\mathbb{Z}$ es un Q-módulo trivial por la izquierda, entonces la sucesión*

$$B_3 \xrightarrow{d_3} B_2 \xrightarrow{d_2} B_1 \xrightarrow{d_1} B_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0 \tag{4.2}$$

es una sucesión exacta de Q-módulos por la izquierda, donde $\varepsilon : B_0 \longrightarrow \mathbb{Z}$ viene dada por

$$\varepsilon : \sum_{x\in Q} m_x x[\,] \mapsto \sum_{x\in Q} m_x.$$

Observación 4.9. La sucesión dada por la Ecuación (4.2) es una resolución libre sobre $\mathbb{Z}$, ya que todos los demás Q-módulos son libres. Además, se conoce como *la resolución barra* [4] por el hecho de denotar los elementos de la base de los módulos como hemos indicado antes (para Q^n, se denotan como $[x_1|\ldots|x_n]$)

Demostración. No se dará una prueba completa para este resultado. Concretamente, comprobaremos que $\varepsilon \circ d_1 = 0$, $d_1 \circ d_2 = 0$, $d_2 \circ d_3 = 0$, es decir, $\operatorname{Im} d_1 \subset \ker \varepsilon$, $\operatorname{Im} d_2 \subset \ker d_1$, $\operatorname{Im} d_3 \subset \ker d_2$. Las inclusiones recíprocas, que también son ciertas, pero más complicadas, pueden verse en [5, pág. 319, Theorem C-3.121]. Antes de probar dichas inclusiones, puede verse que ε es un homomorfismo sobreyectivo. La razón es que $\varepsilon = \varepsilon' \circ \alpha$, donde $\alpha : B_0 \longrightarrow \mathbb{Z}Q$ es el isomorfismo dado por $u[\,] \mapsto u$, para todo $u \in \mathbb{Z}Q$.

Ahora, consideremos, en primer lugar, $\varepsilon \circ d_1$:

$$\varepsilon \circ d_1[x] = \varepsilon(x[\,] - [\,]) = \varepsilon(x[\,]) - \varepsilon([\,]) = \varepsilon'(x) - \varepsilon'(1) = 1 - 1 = 0.$$

Por otro lado, $d_1 \circ d_2$:

$$\begin{aligned} d_1 \circ d_2[x \mid y] &= d_1(x[y] - [xy] + [x]) \\ &= d_1 x[y] - d_1[xy] + d_1[x] \\ &= x d_1[y] - d_1[xy] + d_1[x] \\ &= x(y[\,] - [\,]) - (xy[\,] - [\,]) + (x[\,] - [\,]) \\ &= xy[\,] - x[\,] - xy[\,] + [\,] + x[\,] - [\,] \\ &= 0, \end{aligned}$$

donde la segunda y tercera igualdades se tienen por ser d_1 homomorfismo de Q-módulos (así, en la tercera, $d_1 x[y] = x d_1[y]$).

Finalmente, $d_2 \circ d_3$:

$$\begin{aligned} d_2 \circ d_3[x \mid y \mid z] &= d_2(x[y \mid z] - [xy \mid z] + [x \mid yz] - [x \mid y]) \\ &= x d_2[y \mid z] - d_2[xy \mid z] + d_2[x \mid yz] - d_2[x \mid y] \\ &= x(y[z] - [yz] + [y]) - (xy[z] - [xyz] + [xy]) \\ &\quad + (x[yz] - [xyz] + [x]) - (x[y] - [xy] + [x]) \\ &= 0, \end{aligned}$$

aplicando de nuevo que es un homomorfismo de Q-módulos en la segunda igualdad. Las operaciones realizadas para $d_2 \circ d_3$ son análogas a las de la Proposición 3.22 al comprobar la identidad del cociclo. □

Como ya se ha comentado antes, si X es un conjunto y K un módulo, es lo mismo hablar de funciones $X \longrightarrow K$ que de homomorfismos $B \longrightarrow K$ si B es el módulo libre con base X. De forma más precisa, los funtores covariantes $\mathbf{Fun}(X, \quad) : \mathbb{Z}Q\text{-}\mathbf{Mod} \longrightarrow \mathbf{Sets}$ y $\operatorname{Hom}_{\mathbb{Z}Q\text{-}\mathbf{Mod}}(B, \quad) : \mathbb{Z}Q\text{-}\mathbf{Mod} \longrightarrow \mathbf{Sets}$ son equivalentes. Si aplicamos otro funtor —

el funtor contravariante $\mathrm{Hom}_{\mathbb{Z}Q\text{-}\mathbf{Mod}}(\ \ , K) : \mathbb{Z}Q\text{-}\mathbf{Mod} \longrightarrow \mathbf{Sets}$, ya que K es un $\mathbb{Z}Q$-módulo por la izquierda — a la sucesión exacta dada por la Ecuación (4.2), obtenemos otra sucesión, no necesariamente exacta, dada por

$$\mathrm{Hom}(B_3, K) \xleftarrow{d_3^*} \mathrm{Hom}(B_2, K) \xleftarrow{d_2^*} \mathrm{Hom}(B_1, K) \xleftarrow{d_1^*} \mathrm{Hom}(B_0, K),$$

donde d_1^*, d_2^*, y d_3^* toman homomorfismos de B_0, B_1 y B_2, respectivamente, en K, y los llevan en homomorfismos de B_1, B_2 y B_3, respectivamente, en K, mediante $d_1^*(f) = f \circ d_1$ para $f \in \mathrm{Hom}(B_0, K)$ (y análogamente para d_2^*, y d_3^*). Además, escribimos $\mathrm{Hom}(B_n, K)$ en lugar de $\mathrm{Hom}_{\mathbb{Z}Q\text{-}\mathbf{Mod}}(B_n, K)$ por sencillez, dado que sabemos que son homomorfismos de $\mathbb{Z}Q$-módulos.

Si ahora consideramos la restricción res de B_n a Q^n, que hemos visto que es una biyección, obtenemos un diagrama conmutativo:

$$\begin{array}{ccccccc}
\mathbf{Fun}(Q^3, K) & \longleftarrow & \mathbf{Fun}(Q^2, K) & \longleftarrow & \mathbf{Fun}(Q^1, K) & \longleftarrow & \mathbf{Fun}(\{[\,]\}, K) \\
\uparrow{\scriptstyle \mathrm{res}} & & \uparrow{\scriptstyle \mathrm{res}} & & \uparrow{\scriptstyle \mathrm{res}} & & \uparrow{\scriptstyle \mathrm{res}} \\
\mathrm{Hom}(B_3, K) & \xleftarrow{d_3^*} & \mathrm{Hom}(B_2, K) & \xleftarrow{d_2^*} & \mathrm{Hom}(B_1, K) & \xleftarrow{d_1^*} & \mathrm{Hom}(B_0, K)
\end{array} \tag{4.3}$$

Este diagrama nos permitirá obtener las identidades que considerábamos al comienzo de esta sección, lo cual nos permitirá obtener los grupos de cohomología vistos de esta manera.

Como ya hemos comentado, denotemos por $f : Q^n \longrightarrow K$ las aplicaciones dadas sobre la base de B_n, y por $\overline{f} : B_n \longrightarrow K$ los homomorfismos de Q-módulos obtenidos al extender esas aplicaciones.

En primer lugar, consideremos $\overline{f} \in \ker d_3^*$. Es decir, $d_3^*(\overline{f}) = \overline{f} \circ d_3 = 0$. En ese caso, por la conmutatividad del Diagrama (4.3), se tiene que $\mathrm{res} \circ d_3^*(\overline{f}) = 0$ y $\mathrm{res}(\overline{f}) \in \ker(\mathbf{Fun}(Q^2, K) \to \mathbf{Fun}(Q^3, K))$, por lo que, para todo x, y, $z \in Q$ se tiene

$$\begin{aligned}
0 &= f \circ d_3[x \mid y \mid z] \\
&= f(x[y \mid z] - [xy \mid z] + [x \mid yz] - [x \mid y]) \\
&= xf[y \mid z] - f[xy \mid z] + f[x \mid yz] - f[x \mid y].
\end{aligned}$$

Es decir, consideramos d_3 sobre la base de B_3, Q^3, y luego aplicamos la restricción f al resultado. Por ser f la restricción del homomorfismo de Q-módulos $\overline{f}$, la igualdad $fx[y \mid z] = xf[y \mid z]$ es cierta. En consecuencia, $f : Q^2 \longrightarrow K$ es un cociclo.

En segundo lugar, consideremos $\overline{f} \in \mathrm{Im}\, d_2^*$. Por lo tanto, existe $\overline{h} : B_1 \longrightarrow K$ tal que $d_2^*(\overline{h}) = \overline{f}$. Pero $d_2^*(\overline{h}) = \overline{h} d_2$, luego considerando de nuevo la conmutatividad del diagrama

(esta vez del segundo cuadrado) de forma análoga, obtenemos la siguiente ecuación para las correspondientes restricciones:

$$\begin{aligned} f[x \mid y] &= h \circ d_2[x \mid y] \\ &= h(x[y] - [xy] + [x]) \\ &= xh[y] - h[xy] + h[x], \end{aligned}$$

donde, las propiedades de los homomorfismos de Q-módulos se conservan para h por ser la restricción del homomorfismo $\overline{h}$. En este caso, obtenemos que f es un cofrontera.

A continuación, tomamos $\overline{g} \in \ker d_2^*$ para $\overline{g} : B_1 \longrightarrow K$. De nuevo, si aplicamos argumentos análogos de conmutatividad del diagrama (para el segundo cuadrado) y consideramos las restricciones adecuadas, obtenemos:

$$0 = g \circ d_2[x \mid y] = g(x[y] - [xy] + [x]) = xg[y] - g[xy] + g[x],$$

por lo que

$$g[xy] = xg[y] + g[x].$$

Como en los casos anteriores, $xg[y] = gx[y]$ es cierto al ser g la restricción de un homomorfismo de Q-módulos. Por cumplirse esa identidad, g es una derivación.

Finalmente consideremos $\overline{k} \in \operatorname{Im} d_1^*$, es decir, $\overline{k} = d_1^*(\overline{u})$ para $\overline{u} : B_0 \longrightarrow K$. En este caso, la restricción de $u : \{[\,]\} \longrightarrow K$ de $\overline{u}$ sólo escoge un elemento de K, es decir, $u([\,]) = a_0 \in K$. Por tanto, aplicando los mismos argumentos que en los casos anteriores, obtenemos, para todo $x \in Q$:

$$k[x] = u \circ d_1[x] = u(x[\,] - [\,]) = xu([\,]) - u([\,]) = xa_0 - a_0,$$

ya que u es la restricción del homomorfismo de Q-módulos $\overline{u}$. Con lo cual, k es una derivación principal.

Por otra parte, debe observarse que $d_2 \circ d_3 = 0$ implica que $d_3^* \circ d_2^* = 0$, pues $d_3^* \circ d_2^*(f) = d_3^*(f \circ d_2) = f \circ d_2 \circ d_3 = f \circ 0 = 0$ para cualquier $f \in \operatorname{Hom}(B_1, K)$. Así, se tiene que $\operatorname{Im} d_2^* \subset \ker d_3^*$, y obtenemos que toda cofrontera es un cociclo, como hicimos en la Proposición 3.22. De igual manera, se obtiene que $\operatorname{Im} d_1^* \subset \ker d_2^*$ a partir de $d_1 \circ d_2 = 0$, y obtenemos que toda derivación principal es una derivación, como vimos en el Ejemplo 3.40.

Un cálculo adicional con el diagrama conmutativo dará lugar al último grupo que queremos obtener. En este caso, queremos calcular $\ker d_1^*$. En el último cálculo realizado, vimos que $u \circ d_1[x] = xa_0 - a_0$ para $a_0 \in K$, con $u([\,]) = a_0$. Si $\overline{u} \in \ker d_1^*$, entonces $0 = u \circ d_1[x] = xa_0 - a_0$, luego $a_0 = xa_0$ para todo $x \in Q$. Las extensiones de las aplicaciones como u son los homomorfismos que forman $\ker d_1^*$.

La construcción realizada mediante una resolución libre nos permite obtener los grupos de cohomología de una forma distinta a la vista en el capítulo anterior, mediante la aplicación del funtor contravariante $\mathrm{Hom}_{\mathbb{Z}Q\text{-}\mathbf{Mod}}(\ \ , K)$ a la sucesión exacta de la Ecuación (4.2). Únicamente nos hemos centrado en los grupos de dimensión baja al ser los que hemos interpretado en el capítulo anterior, pero todos los demás se obtienen de forma análoga. Como hemos visto, existe una correspondencia biunívoca entre los homomorfismos presentes en núcleos o imágenes de d_1^*, d_2^* y d_3^* y sus restricciones a Q^1, Q^2 y Q^3, según corresponda. Con lo cual, $\ker d_3^*$ está formado por todas las extensiones lineales de cociclos, $\operatorname{Im} d_2^*$ son las extensiones lineales de las cofronteras, y análogamente para el resto. Sin embargo, puede apreciarse la diferencia con respecto a lo visto en el capítulo anterior en el Diagrama (4.3): el cálculo por fuerza bruta visto en la Sección 3.1 o las interpretaciones vistas en las Secciones 3.2, 3.3 y 3.4 se realiza mediante núcleos e imágenes de la sucesión superior del diagrama. Es decir, se trabaja con aplicaciones que no poseen estructura en el dominio. Sin embargo, este cálculo se realiza calculando núcleos e imágenes de homomorfismos de Q-módulos, en los que sí podemos utilizar la estructura de Q-módulo (libre) del dominio, dando lugar a cálculos más eficientes.

$$\begin{aligned} H^2(Q,K) &= \ker d_3^* / \operatorname{Im} d_2^*, \\ H^1(Q,K) &= \ker d_2^* / \operatorname{Im} d_1^*, \\ H^0(Q,K) &= \ker d_1^*. \end{aligned}$$

Observación 4.10. Se tiene que $H^0(Q,K) = \ker d_1^* \cong K^Q$, siendo K^Q un Q-módulo trivial (lo cual se ha probado en la Observación 3.48). Para ver que son isomorfos como Q-módulos, basta observar que las restricciones de los homomorfismos $\overline{u} \in \ker d_1^*$ son aplicaciones que asignan el único elemento de Q^0 a un elemento $a_0 \in K$ tal que $xa_0 = a_0$ para todo $x \in Q$. Con lo cual, se define $\varphi : K^Q \longrightarrow H^0(Q,K)$ por

$$\varphi(a) = \overline{u_a} : B_0 \longrightarrow K,$$

donde la restricción u_a de $\overline{u_a}$ viene dada por $u_a([\,]) = a \in K^Q$. Luego, hay una correspondencia biunívoca entre aplicaciones en $\ker d_1^*$ y elementos en K^Q, por lo que φ es una biyección. Además, por ser K^Q un Q-módulo, es un homomorfismo de Q-módulos, y por tanto un isomorfismo.

Bibliografía

[1] K. Conrad, *Splitting of short exact sequences for groups*. https://kconrad.math.uconn.edu/blurbs/grouptheory/splittinggp.pdf.

[2] P. J. Hilton and U. Stammbach, *A Course in Homological Algebra*, vol. 4, Springer, New York, NY, 1971.

[3] J. P. May, *Reu 2013: The cohomology of groups*. http://math.uchicago.edu/~may/REU2013/GroupCohomology.pdf.

[4] J. J. Rotman, *An introduction to homological algebra*, Universitext, Springer, New York, second ed., 2009.

[5] ——, *Advanced modern algebra. Part 2*, vol. 180 of Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, third ed., 2017.

[6] J.-P. Serre, *Local fields*, vol. 67, Springer, New York, NY, 1979.

[7] M. Tsiang, *Group extensions*. http://www.geocities.ws/gnaist4/mythesis.pdf.

[8] C. A. Weibel, *An introduction to homological algebra*, vol. 38, Cambridge: Cambridge University Press, 1994.

[9] ——, *History of homological algebra*, in History of topology, North-Holland, Amsterdam, 1999, pp. 797–836.