



FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Módulos cruzados de grupos

Moira Esperón López

2024/2025

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Módulos cruzados de grupos

Moira Esperón López

Xullo, 2025

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

| |
|---|
| Área de Coñecemento: Álgebra |
| Título: Módulos cruzados de grupos |
| Breve descripción do contido |
| <p>O concepto matemático de módulo cruzado existe para unha gran variedade de estruturas alxébricas. Para a estrutura alxébrica de grupos, un módulo cruzado de grupos é un homomorfismo de grupos $f: M \rightarrow N$ xunto cunha acción do grupo N sobre o grupo M por automorfismos, tal que f é equivariante e satisfai a identidade de Peiffer.</p> <p>Os módulos cruzados pódense ver como unha versión en dimensión 2 do concepto de grupo.</p> <p>Os módulos cruzados de grupos foron inventados nos anos 1940 por J. H. C. Whitehead para modelizar os espazos 2-tipos homotópicos.</p> <p>Neste TFG, a estudante estudará as propiedades básicas dos módulos cruzados, así como a súa relación cos 2-grupos e os Cat^1-grupos.</p> |
| Bibliografía |
| Wagemann, F. (2021). Crossed Modules. De Gruyter Studies in Mathematics 82, De Gruyter. |
| Recomendacións (non vinculantes) |
| |

Índice general

| | |
|--|------------|
| Resumen | VII |
| Introducción | IX |
| 1. Preliminares | 1 |
| 1.1. Grupos | 1 |
| 1.2. Acciones de grupos | 3 |
| 1.3. Extensiones de grupos | 5 |
| 1.4. Introducción a la teoría de categorías | 8 |
| 2. Módulos cruzados de grupos | 15 |
| 3. Definiciones equivalentes de módulos cruzados | 31 |
| 3.1. Cat^1 -grupos y módulos cruzados | 31 |
| 3.2. 2-grupos estrictos y módulos cruzados | 40 |
| 3.3. Grupos categóricos estrictos y módulos cruzados | 45 |
| Bibliografía | 49 |

Resumen

El concepto matemático de módulo cruzado fue introducido por J. H. C. Whitehead en 1949 con el objetivo de modelizar los espacios 2-tipo homotópicos. Los módulos cruzados existen para una gran variedad de estructuras algebraicas; en este trabajo se considerará exclusivamente la estructura de grupo.

En este contexto, un módulo cruzado de grupos es un homomorfismo de grupos $\mu: M \rightarrow N$ junto con una acción del grupo N sobre el grupo M por automorfismos tal que se cumplen dos condiciones fundamentales: la equivarianza de μ y la identidad de Peiffer.

Los módulos cruzados poseen diversas propiedades algebraicas y son equivalentes, en sentido categórico, a estructuras como los \mathbf{Cat}^1 -grupos, los 2-grupos estrictos y los grupos categóricos estrictos. Describir tales propiedades y equivalencias será el objetivo fundamental de este trabajo.

Abstract

The mathematical concept of a crossed module was introduced by J. H. C. Whitehead in 1949 with the aim of modeling spaces of homotopy 2-type. Crossed modules exist for a wide variety of algebraic structures; in this work, we will consider exclusively the group structure.

In this context, a crossed module of groups is a group homomorphism $\mu: M \rightarrow N$ together with an action of the group N on the group M by automorphisms, such that two fundamental conditions are satisfied: the equivariance of μ and the Peiffer identity.

Crossed modules have different algebraic properties and are categorically equivalent to structures such as \mathbf{Cat}^1 -grupos, strict 2-groups, and strict categorical groups. Describing these properties and equivalences will be the main objective of this work.

Introducción

Desde sus inicios, los módulos cruzados han jugado un papel importante en varias áreas de las matemáticas, especialmente en la teoría de homotopía, homología y cohomología de grupos, K -teoría algebraica, homología cíclica, teoría combinatoria de grupos y geometría diferencial.

El origen de esta estructura se remonta a finales de los años 40 del siglo pasado cuando J. H. C. Whitehead, matemático británico, introdujo la noción de módulo cruzado de grupos como un modelo algebraico para espacios de homotopía de tipo 2 (es decir, espacios conexos con grupos de homotopía triviales en dimensión mayor que 2); véase [15, 16]. Más específicamente, al estudiar la homotopía relativa $\pi_2(X, A)$ ¹ junto con su acción por $\pi_1(A)$, Whitehead descubre que $\pi_2(X, A)$ adquiere una estructura algebraica adicional mediante un morfismo de grupos junto con una acción compatible, lo que dará lugar posteriormente a la noción de módulo cruzado, que captura las propiedades de dicha acción.

Desde entonces, los módulos cruzados han adquirido importancia no solo en el ámbito de la topología algebraica, sino también en áreas como la teoría de categorías o la geometría diferencial. Esto se debe a su utilidad para describir estructuras algebraicamente enriquecidas. En el caso particular de los grupos, que será el que nos ocupe en este trabajo, los módulos cruzados se pueden entender como una generalización del concepto de extensión de grupos con una acción compatible. Además, generalizan al mismo tiempo los conceptos de subgrupo normal y módulo sobre un grupo. Cabe destacar que los módulos cruzados no solo han sido estudiados en el contexto de grupos, sino también para álgebras de Lie, álgebras de Leibniz o álgebras asociativas; véase [3, 4].

Los módulos cruzados admiten descripciones equivalentes, en sentido categórico, a diferentes estructuras entre las cuales destacan los Cat^1 -grupos y los 2-grupos estrictos. Los Cat^1 -grupos y, en general, la noción de Cat^n -grupo para $n \geq 1$, fueron introducidos por

¹ $\pi_2(X, A)$ es el segundo grupo de homotopía de un espacio topológico X con base el subespacio A . Dicho grupo clasifica las aplicaciones continuas de la esfera bidimensional S^2 en X , por homotopía relativa con respecto al subespacio A .

J.-L. Loday en [9] motivado por el hecho de que la categoría de CW-complejos² conexos con $\pi_i(X)$ trivial para $i \neq n$ es equivalente a la categoría de grupos si $n = 1$ y a la de grupos abelianos si $n \geq 2$; véase [10]. De manera general, un Cat^n -grupo se trata de un grupo G junto con n subgrupos, $\{N_i\}_{i=1}^n$, de G y $2n$ homomorfismos de grupos $s_i, b_i: G \rightarrow N_i$, $i = 1, \dots, n$, tales que

$$(i) \quad s_i|_{N_i} = b_i|_{N_i} = \text{id}_{N_i},$$

$$(ii) \quad [\ker s_i, \ker b_i] = \{1_G\},$$

$$(iii) \quad s_i s_j = s_j s_i, \quad b_i b_j = b_j b_i \quad \text{y} \quad b_i s_j = s_j b_i \quad \text{para todo } i \neq j, \quad i, j = 1, \dots, n.$$

En la presenta memoria simplemente nos centraremos en estudiar el caso $n = 1$ y su relación con la categoría de módulos cruzados. Por otro lado, la estructura de 2-grupos estrictos fue introducida por R. Brown y C. B. Spencer en 1978 ([2]) mediante un proceso de *categorificación vertical* de la estructura de grupo. A grandes rasgos, la categorificación vertical es un procedimiento a través del cual las estructuras se generalizan del contexto de la teoría de conjuntos a la teoría de categorías, o de la teoría de categorías a la teoría de categorías superiores (n -categorías).

Hoàng Xuân Sinh finalizó su tesis con Grothendieck en el año 1973, donde introdujo los grupos categóricos, bajo el nombre de *gr-categories*. Ella probó que toda *gr-category* es equivalente a un 2-grupo estricto. El término grupo categórico también se conoce como un objeto grupo en la categoría de categorías pequeñas. En el artículo de R. Brown y C. B. Spencer ([2]) no usan el término de grupo categórico. Usan el término de \mathcal{G} -grupoide y prueban la equivalencia entre \mathcal{G} -grupoides y módulos cruzados.

Este manuscrito se estructura de la siguiente manera. Se comienza con un primer capítulo de preliminares el cual está dividido en cuatro secciones donde se presentan conceptos fundamentales para el posterior desarrollo del trabajo. En la primera sección se recuerdan nociones básicas de teoría de grupos, mientras que la segunda está dedicada al estudio de las acciones de grupos. En ella se introduce formalmente el concepto de acción φ de un grupo N sobre un conjunto M y se demuestra que, dada una acción de N sobre M , se obtiene una representación de N por automorfismos de M , y viceversa, de tal manera que dar una acción es equivalente a proporcionar una representación por automorfismos. Además se define el producto semidirecto de grupos, que será importante en ciertas construcciones que se llevarán a cabo en capítulos posteriores. En la tercera sección se introduce la definición de sucesión de grupos y de sucesión exacta corta. La cuarta y última sección de

²Un CW-complejo es un espacio topológico que se construye mediante un proceso inductivo añadiendo discos D^n por pegado a lo largo de sus bordes, que son esferas S^{n-1} .

este capítulo preliminar presenta una introducción a la teoría de categorías, definiendo los conceptos de categoría, funtor, transformación natural y equivalencia de categorías, junto con ejemplos que ilustran tales nociones.

El segundo capítulo está dedicado a la introducción formal del concepto de módulo cruzado de grupos, proporcionando numerosos ejemplos procedentes de diversos contextos, incluyendo casos en los que la acción es trivial, ejemplos con productos semidirectos, con grupos cíclicos o con subgrupos normales con el propósito de mostrar la versatilidad de esta noción. Asimismo, se estudian construcciones adicionales sobre módulos cruzados, tales como la noción de equivalencia y la suma de dos módulos cruzados.

El capítulo final está dedicado al estudio de diferentes descripciones equivalentes de la estructura de módulo cruzado. Se introducirán tres categorías diferentes, Cat^1 -grupos, 2-grupos estrictos y grupos categóricos estrictos, para luego construir funtores que relacionan cada una de ellas con la categoría de módulos cruzados. El objetivo central de este trabajo es demostrar que los funtores en cuestión inducen una equivalencia entre las categorías consideradas y la categoría de módulos cruzados.

Capítulo 1

Preliminares

Este capítulo reúne los conceptos fundamentales que servirán como base para el desarrollo teórico en los capítulos posteriores.

Se comienza con una revisión de la teoría de grupos, una estructura algebraica esencial para el desarrollo del trabajo. Posteriormente, se examinan las acciones y extensiones de grupos, las cuales resultarán fundamentales en la formulación de conceptos posteriores. Finalmente, se presenta una introducción a la teoría de categorías, proporcionando un marco abstracto que permitirá interpretar y conectar diversas construcciones matemáticas.

1.1. Grupos

Con el fin de establecer una base sólida para los conceptos que se desarrollarán en este trabajo, se comenzará recordando algunos resultados fundamentales de la teoría de grupos. Algunas de las definiciones y resultados de esta sección se encuentran desarrolladas con mayor detalle en [7].

Definición 1.1. Un **grupo** es un par (N, \cdot) , donde N es un conjunto y \cdot es una operación interna

$$\begin{aligned} \cdot : N \times N &\rightarrow N \\ (x, y) &\mapsto x \cdot y, \end{aligned}$$

que verifica:

- (i) La propiedad asociativa, es decir, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ para todo $x, y, z \in N$.
- (ii) Tiene elemento neutro, es decir, existe $1 \in N$ tal que $x \cdot 1 = x = 1 \cdot x$ para todo $x \in N$.

(iii) Todo elemento de N tiene inverso, es decir, para todo $x \in N$, existe $x' \in N$ tal que $x \cdot x' = 1 = x' \cdot x$.

Un grupo (N, \cdot) , se dice **abeliano** o **conmutativo** si \cdot también verifica la propiedad conmutativa, i.e., $x \cdot y = y \cdot x$ para todo $x, y \in N$.

Sea $(N', *)$ otro grupo. Una aplicación $f: N \rightarrow N'$ es un **homomorfismo de grupos** si:

$$f(x \cdot y) = f(x) * f(y)$$

para todo $x, y \in N$. Además, se dirá que f es un **endomorfismo de grupos** en el caso de que $N = N'$.

Dado un grupo (N, \cdot) , de ahora en adelante, y siempre que no exista posibilidad de confusión, este se denotará únicamente mediante N y la operación interna del grupo se escribirá mediante yuxtaposición de elementos: $x \cdot y = xy$ para todo $x, y \in N$.

Definición 1.2. Dado un grupo (N, \cdot) y un subconjunto $H \subset N$, se dice que H es un **subgrupo** de N , ($H < N$), si (H, \cdot) es un grupo.

Definición 1.3. Sea N un grupo y H un subgrupo de N . Se dice que H es un **subgrupo normal** de N , ($H \triangleleft N$), si:

$$a H a^{-1} \subset H, \text{ para todo } a \in N.$$

Definición 1.4. El **centro** de un grupo N es el conjunto de los elementos del grupo que conmutan con todos los elementos del mismo:

$$Z(N) := \{x \in N \text{ tal que } x \cdot y = y \cdot x, \text{ para todo } y \in N\}.$$

Definición 1.5. Sea $\mu: M \rightarrow N$ un homomorfismo de grupos, el **conúcleo** de μ es:

$$\text{Coker}(\mu) := N / \text{Im}(\mu).$$

Teorema 1.6 (Primer Teorema de Isomorfía). Sean N y N' dos grupos. Si $f: N \rightarrow N'$ es un homomorfismo de grupos, entonces:

$$\frac{N}{\ker(f)} \simeq \text{Im}(f).$$

1.2. Acciones de grupos

Definición 1.7. Sea N un grupo con neutro 1 y M un conjunto. Una aplicación

$$\begin{aligned}\varphi: N \times M &\rightarrow M \\ (n, m) &\mapsto {}^n m,\end{aligned}$$

es una **acción** de N sobre M si:

$${}^1 m = m, \tag{1.1}$$

$${}^{n_1 n_2} m = {}^{n_1} ({}^{n_2} m), \tag{1.2}$$

para todo $m \in M$ y para todo $n_1, n_2 \in N$. En esta situación se dice que N actúa sobre M a través de la acción φ .

Observación 1.8. Supongamos que N actúa sobre M a través de la acción φ . Para cada $n \in N$ la aplicación $f_n: M \rightarrow M$, $f_n(m) := {}^n m$ es una aplicación biyectiva. En efecto, si $f_n(m_1) = f_n(m_2)$, i.e., ${}^n m_1 = {}^n m_2$, entonces:

$$\begin{aligned}m_1 &\stackrel{(1.1)}{=} {}^1 m_1 = {}^{n^{-1}n} m_1 \stackrel{(1.2)}{=} {}^{n^{-1}} ({}^n m_1) \\ &= {}^{n^{-1}} ({}^n m_2) \stackrel{(1.2)}{=} {}^{n^{-1}n} m_2 = {}^1 m_2 \stackrel{(1.1)}{=} m_2.\end{aligned}$$

Así, f_n es inyectiva. Además, dado $x \in M$, se tiene que:

$$f_n({}^{n^{-1}} x) = {}^n ({}^{n^{-1}} x) \stackrel{(1.2)}{=} {}^{nn^{-1}} x = {}^1 x \stackrel{(1.1)}{=} x.$$

Por lo tanto, f_n es también sobreyectiva.

Sea

$$\text{Aut}(M) := \{f: M \rightarrow M \text{ tal que } f \text{ es biyectiva}\}$$

y considérese la aplicación $\varphi: N \rightarrow \text{Aut}(M)$ tal que $\varphi(n) = f_n$. Esta aplicación se denomina **representación de N por automorfismos de M** y se trata de un homomorfismo de grupos. En primer lugar, veamos que $\text{Aut}(M)$ es un grupo con la operación composición:

- (i) Verifica la propiedad asociativa, es decir, $(f \circ g) \circ h = f \circ (g \circ h)$ para todo $f, g, h \in \text{Aut}(M)$.
- (ii) Tiene elemento neutro, es decir, existe $\text{id}_M \in \text{Aut}(M)$ tal que $f \circ \text{id}_M = f = \text{id}_M \circ f$ para toda $f \in \text{Aut}(M)$.
- (iii) Todo elemento de $\text{Aut}(M)$ tiene inverso, es decir, para todo $f \in \text{Aut}(M)$, existe $f^{-1} \in \text{Aut}(M)$ tal que $f \circ f^{-1} = \text{id}_M = f^{-1} \circ f$.

A continuación, se prueba que, en efecto, φ es un homomorfismo de grupos:

$$\varphi(n_1 n_2)(m) = f_{n_1 n_2}(m) = {}^{n_1 n_2} m \stackrel{(1.2)}{=} {}^{n_1}({}^{n_2} m) = f_{n_1}(f_{n_2}(m)) = (\varphi(n_1) \circ \varphi(n_2))(m)$$

para todo $n_1, n_2 \in N$ y $m \in M$.

Así, dada una acción φ de N en M , tenemos una representación de N por automorfismos de M .

Además, dada cualquier representación φ de N en M , se tiene una acción de N en M , dada por ${}^n m := \varphi(n)(m)$. Lo que indica que se pueden ver las acciones como representaciones y las representaciones como acciones.

Definición 1.9. Sea N un grupo actuando sobre otro grupo M por automorfismos. El **producto semidirecto de M y N** , denotado por $M \rtimes N$, es el grupo sobre el conjunto $M \times N$ con la operación definida por:

$$(m_1, n_1) \cdot (m_2, n_2) := (m_1 {}^{n_1} m_2, n_1 n_2)$$

para todo $m_1, m_2 \in M$ y $n_1, n_2 \in N$.

El neutro del producto semidirecto es $(1_M, 1_N)$ y el inverso de un elemento $(m, n) \in M \rtimes N$ viene dado por

$$(m, n)^{-1} = (\varphi(n^{-1}, m^{-1}), n^{-1}). \quad (1.3)$$

En efecto,

$$\begin{aligned} (m, n) \cdot (\varphi(n^{-1}, m^{-1}), n^{-1}) &= (m, n) \cdot ({}^{n^{-1}} m^{-1}, n^{-1}) \\ &= (m {}^{n(n^{-1})} m^{-1}, n n^{-1}) \\ &\stackrel{(1.2)}{=} (m {}^{n n^{-1}} m^{-1}, n n^{-1}) \\ &= (m m^{-1}, n n^{-1}) \\ &= (1_M, 1_N). \end{aligned}$$

Ejemplo 1.10. Sea la acción trivial, es decir, ${}^n m := m$, (en este caso la representación de dicha acción por automorfismos es $\varphi(n) = \text{id}_M$ para todo $n \in N$), entonces el producto semidirecto es el producto directo:

$$(m_1, n_1) \cdot (m_2, n_2) := (m_1 m_2, n_1 n_2).$$

Ejemplo 1.11. Sea $C_n = \mathbb{Z}/n\mathbb{Z}$ el grupo cíclico de orden n . Consideremos el producto semidirecto de los grupos cíclicos $C_3 = \{0, 1, 2\}$ y $C_4 = \{0, 1, 2, 3\}$, definido mediante un homomorfismo

$$\varphi: C_4 \rightarrow \text{Aut}(C_3)$$

donde $\text{Aut}(C_3)$ es el grupo de automorfismos de C_3 , que se puede identificar con el grupo multiplicativo $(\mathbb{Z}/3\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$.

En este caso, φ es el único homomorfismo no trivial desde C_4 hacia $\text{Aut}(C_3)$. El grupo C_3 tiene solo dos automorfismos: $\text{id}: C_3 \rightarrow C_3$ y $\cdot 2: C_3 \rightarrow C_3$ que lleva:

$$0 \mapsto 0, \quad 1 \mapsto 2, \quad 2 \mapsto 1.$$

Así el homomorfismo φ se define como sigue,

$$\varphi(0) = \text{id}, \quad \varphi(1) = \cdot 2, \quad \varphi(2) = \text{id}, \quad \varphi(3) = \cdot 2.$$

Este comportamiento se puede escribir también como:

$$\varphi(x \bmod 4) = (-1)^x \bmod 3.$$

Entonces el producto semidirecto $C_3 \rtimes C_4$ tiene la siguiente operación:

$$(a, b) \cdot (c, d) := (a + (-1)^b c, b + d), \quad a, c \in C_3, \quad b, d \in C_4.$$

Definición 1.12. Sea N un grupo y $x, y \in N$. El **conmutador** de los elementos x e y es:

$$[x, y] = xyx^{-1}y^{-1},$$

donde

$$[x, y]^{-1} = [y, x] = yxy^{-1}x^{-1}.$$

En el caso de ser M y G dos subgrupos de un grupo N , el subgrupo generado por todos los conmutadores de la forma $[m, g]$ es el **conmutador**. Esto es,

$$[M, G] = \langle [m, g] \text{ tal que } m \in M, g \in G \rangle.$$

1.3. Extensiones de grupos

La presente sección toma como referencia principal [8], cuya formulación teórica ha servido como fundamento para el desarrollo formal de los resultados presentados.

Definición 1.13. Una **sucesión de grupos** es una secuencia de grupos N_n con homomorfismos entre ellos α_n , de forma que $\text{Im}(\alpha_{n-1}) \subset \ker(\alpha_n)$.

$$\dots \xrightarrow{\alpha_{n-2}} N_{n-1} \xrightarrow{\alpha_{n-1}} N_n \xrightarrow{\alpha_n} N_{n+1} \xrightarrow{\alpha_{n+1}} \dots$$

La sucesión de grupos N_n junto con los homomorfismos α_n se dice que es **una sucesión exacta en N_n** si $\text{Im}(\alpha_{n-1}) = \ker(\alpha_n)$. La sucesión se dice **exacta** si es exacta en cada N_n . Una sucesión exacta de término finito del tipo:

$$1 \xrightarrow{f} H \xrightarrow{\alpha} N \xrightarrow{\beta} K \xrightarrow{g} 1,$$

con el 1 representando el grupo trivial, es llamada una **sucesión exacta corta**.

Así, decir que la sucesión anterior es exacta implica que, por un lado, $\text{Im}(f) = 1_H = \ker(\alpha)$, lo que equivale a decir que α es inyectiva, y por otro lado, que $\text{Im}(\beta) = \ker(g) = K$, lo que conlleva que β sobreyectiva.

En particular, se probará a continuación que $\alpha(H)$ es un subgrupo normal de N .

Como H es un grupo y α un homomorfismo, se tiene que $\alpha(H)$ es un subgrupo de N , en efecto:

- (i) $\alpha(H) \subset N$.
- (ii) Dados $h_1, h_2 \in H$ entonces $\alpha(h_1 h_2) = \alpha(h_1)\alpha(h_2) \in \alpha(H)$.
- (iii) Sea el neutro de H : 1_H , se tiene que $\alpha(1_H) = 1_N$, pues α es un homomorfismo de grupos.
- (iv) Para $h \in H$, se tiene que h^{-1} es su inverso, luego como α es un homomorfismo: $\alpha(h^{-1}) = \alpha(h)^{-1} \in \alpha(H)$.

Visto que $\alpha(H)$ es un subgrupo de N , faltaría ahora probar que dicho subgrupo es normal.

Para que $\alpha(H)$ sea normal en N se debe verificar que para todo $n \in N$ y para todo $h \in H$:

$$n\alpha(h)n^{-1} \in \alpha(H).$$

Ahora bien, por ser la sucesión exacta $\ker(\beta) = \text{Im}(\alpha)$, luego:

$$\alpha(H) = \ker(\beta) = \{n \in N \text{ tal que } \beta(n) = 1_K\}.$$

Queremos ver $n\alpha(h)n^{-1} \in \ker(\beta)$ para todo $n \in N$ y $h \in H$. En efecto, por ser β un homomorfismo:

$$\beta(n\alpha(h)n^{-1}) = \beta(n)\beta(\alpha(h))\beta(n^{-1}) = \beta(n)\beta(\alpha(h))\beta(n)^{-1}.$$

Como $\alpha(H) = \ker(\beta)$ tenemos que $\beta(\alpha(h)) = 1_K$. Luego:

$$\beta(n\alpha(h)n^{-1}) = \beta(n)1_K\beta(n)^{-1} = 1_K.$$

Llegando así a que $n\alpha(h)n^{-1} \in \ker(\beta) = \alpha(H)$.

La sucesión exacta corta anterior es también denominada como **una extensión de H por K** .

Ejemplo 1.14. Sea $S_3 = \{\text{id}, (12), (1, 3), (2, 3), (123), (132)\}$ el grupo de todas las permutaciones de tres elementos y $A_3 = \{\text{id}, (123), (132)\}$ el subgrupo de S_3 formado por las permutaciones pares. Se tiene la siguiente sucesión exacta:

$$1 \rightarrow A_3 \xrightarrow{i} S_3 \xrightarrow{\chi} \{1, -1\} \rightarrow 1,$$

donde i es la aplicación inclusión y χ es la aplicación que toma los valores 1 o -1. Notar que A_3 es un grupo cíclico de orden 3 y $\{1, -1\}$ es un grupo cíclico de orden 2.

Otra extensión de un grupo cíclico de orden 3 por un grupo cíclico de orden 2 es:

$$1 \rightarrow \mathbb{Z}_3 \xrightarrow{i} \mathbb{Z}_6 \xrightarrow{q} \mathbb{Z}_2 \rightarrow 1,$$

donde \mathbb{Z}_3 está incluido como un grupo de orden 3 en \mathbb{Z}_6 y q es la correspondiente aplicación cociente. Notar que S_3 no es isomorfo a \mathbb{Z}_6 .

Definición 1.15. Una extensión E de H por K dada por

$$E \equiv 1 \rightarrow H \xrightarrow{\alpha} N \xrightarrow{\beta} K \rightarrow 1,$$

se denomina **extensión central** si $\alpha(H) \subseteq Z(N)$.

Sea (M, \cdot) un grupo. Se denota mediante conj_m el siguiente $\text{Aut}(M)$:

$$\begin{aligned} \text{conj}_m: M &\rightarrow M \\ n &\mapsto \text{conj}_m(n) := mn m^{-1}. \end{aligned}$$

Esto define un homomorfismo de grupos,

$$\begin{aligned} \text{conj}: M &\rightarrow \text{Aut}(M) \\ m &\mapsto \text{conj}_m \end{aligned}$$

cuyo núcleo es:

$$\begin{aligned} \ker(\text{conj}) &= \{m \in M \mid \text{conj}_m = \text{id}_M\} \\ &= \{m \in M \mid \text{conj}_m(n) = \text{id}_M(n), n \in M\} \\ &= \{m \in M \mid mn m^{-1} = n, n \in M\} \\ &= \{m \in M \mid mn = nm, n \in M\} \\ &= Z(M). \end{aligned}$$

Se tiene entonces la siguiente sucesión exacta corta:

$$\begin{array}{ccccccc} \ker(\text{conj}) = Z(M) & \xrightarrow{i} & M & \xrightarrow{\text{conj}} & \text{Aut}(M) & \xrightarrow{p} & \frac{\text{Aut}(M)}{\text{Inn}(M)} := \text{Out}(M) \\ & & & & \uparrow & & \\ & & & & \text{Inn}(M) & & \end{array}$$

donde i es la inclusión de $Z(M)$ en M y p es la proyección canónica al cociente, mientras que $\text{Inn}(M)$ y $\text{Out}(M)$ se definen como sigue:

Definición 1.16. El conjunto de **automorfismos internos** de M , denotado por $\text{Inn}(M)$, está formado por los automorfismos definidos por conjugación en M :

$$\text{Inn}(M) := \{\text{conj}_m \text{ tal que } m \in M\},$$

es decir, $\text{Inn}(M)$ es la imagen de conj .

Definición 1.17. El cociente entre los automorfismos de M , $\text{Aut}(M)$ y los automorfismos internos de M , $\text{Inn}(M)$, son los **automorfismos externos** de M :

$$\text{Out}(M) := \frac{\text{Aut}(M)}{\text{Inn}(M)}.$$

1.4. Introducción a la teoría de categorías

En esta sección se dará una breve introducción a la teoría de categorías describiendo los conceptos necesarios para el desarrollo de la memoria. Para ello se ha empleado fundamentalmente [12].

Definición 1.18. Una **categoría** \mathcal{C} consiste en:

- una colección $\text{Ob}(\mathcal{C})$ cuyos elementos se denominan **objetos** de la categoría,
- una colección $\text{Mor}(\mathcal{C})$ constituida por los **morfismos** de la categoría,

verificando los siguientes axiomas:

- existe $\text{id}_X: X \rightarrow X$ el morfismo identidad para todo $X \in \text{Ob}(\mathcal{C})$,
- si $f: X \rightarrow Y, g: Y \rightarrow Z \in \text{Mor}(\mathcal{C})$, entonces existe $g \circ f: X \rightarrow Z \in \text{Mor}(\mathcal{C})$ el morfismo composición. Además, la composición debe cumplir las siguientes propiedades:
 - si $f: X \rightarrow Y \in \text{Mor}(\mathcal{C})$, entonces $\text{id}_Y \circ f = f = f \circ \text{id}_X$,
 - es asociativa, es decir, si $f: X \rightarrow Y, g: Y \rightarrow Z, h: Z \rightarrow W \in \text{Mor}(\mathcal{C})$, entonces $h \circ (g \circ f) = (h \circ g) \circ f$.

Dados $X, Y \in \text{Ob}(\mathcal{C})$, se denotará mediante $\text{Hom}_{\mathcal{C}}(X, Y)$ a la subcolección de $\text{Mor}(\mathcal{C})$ tales que X es el dominio e Y es el codominio.

Ejemplo 1.19.

- (i) La categoría de conjuntos **Set**, donde los objetos son los conjuntos y los morfismos son las aplicaciones entre conjuntos.
- (ii) La categoría de grupos, **Grp**, donde los objetos son los grupos y los morfismos son los homomorfismos de grupos.
- (iii) La categoría de espacios vectoriales, \mathbf{Vect}_K , donde los objetos son los K -espacios vectoriales y los morfismos las aplicaciones K -lineales.

Ejemplo 1.20. Sean \mathcal{C} y \mathcal{D} categorías. La categoría producto cartesiano $\mathcal{C} \times \mathcal{D}$ es aquella donde:

- la colección $\text{Ob}(\mathcal{C} \times \mathcal{D}) = \text{Ob}(\mathcal{C}) \times \text{Ob}(\mathcal{D})$,
- la colección $\text{Mor}(\mathcal{C} \times \mathcal{D})$ verifica:

$$\text{Hom}_{\mathcal{C} \times \mathcal{D}}((X, Y), (X', Y')) = \text{Hom}_{\mathcal{C}}(X, X') \times \text{Hom}_{\mathcal{D}}(Y, Y'), \quad (X, Y), (X', Y') \in \text{Ob}(\mathcal{C} \times \mathcal{D}).$$

Definición 1.21. Sean \mathcal{C} , \mathcal{D} categorías. Un **functor** $F: \mathcal{C} \rightarrow \mathcal{D}$ consiste en un par de aplicaciones:

$$F: \text{Ob}(\mathcal{C}) \rightarrow \text{Ob}(\mathcal{D}) \text{ y } F: \text{Mor}(\mathcal{C}) \rightarrow \text{Mor}(\mathcal{D}),$$

verificando las propiedades siguientes:

- $F(\text{id}_X) = \text{id}_{F(X)}$, para todo $X \in \text{Ob}(\mathcal{C})$,
- si $f: X \rightarrow Y \in \text{Mor}(\mathcal{C})$, entonces $F(f): F(X) \rightarrow F(Y) \in \text{Mor}(\mathcal{D})$,
- si $f: X \rightarrow Y, g: Y \rightarrow Z \in \text{Mor}(\mathcal{C})$, entonces $F(g \circ f) = F(g) \circ F(f)$.

Ejemplo 1.22.

- (i) El functor partes de un conjunto.

Sea $\mathcal{P}: \text{Set} \rightarrow \text{Set}$ la correspondencia dada por la expresión:

$$\mathcal{P}(A \xrightarrow{f} B) = \mathcal{P}A \xrightarrow{\mathcal{P}f} \mathcal{P}B,$$

donde $\mathcal{P}A$ es el conjunto de partes de A (es decir el conjunto de todos los subconjuntos de A) y $\mathcal{P}f$ es una aplicación definida por:

$$\mathcal{P}f(X) := f(X) := \{y \in B \text{ tal que existe } x \in X \wedge f(x) = y\}, \quad \text{para todo } X \subset A.$$

- (ii) El functor producto $G \times - : \mathbf{Grp} \rightarrow \mathbf{Grp}$, $(G \times -)(H) := G \times H$, donde para todo grupo H , la estructura de grupo sobre $G \times H$ está definida componente a componente, i.e, $G \times H$ está dotado de la estructura de producto directo, y dado un homomorfismo de grupos $f: H_1 \rightarrow H_2$, $(G \times -)(f) := 1_G \times f$, donde $(1_G \times f)(g, h) := (g, f(h))$.
- (iii) El functor producto tensor $V \otimes - : \mathbf{Vect}_K \rightarrow \mathbf{Vect}_K$, $(V \otimes -)(W) := V \otimes W$, donde para todo espacio vectorial W , la estructura de espacio vectorial $V \otimes W$ está definida por el producto tensor, y dada una aplicación lineal $f: W_1 \rightarrow W_2$, $(V \otimes -)(f) := 1_V \otimes f$, donde $(1_V \otimes f)(v, w) := v \otimes f(w)$.
- (iv) El functor doble dual $(-)^{**} : \mathbf{Vect}_K \rightarrow \mathbf{Vect}_K$, $(-)^{**}(V) := V^{**}$, donde para todo espacio vectorial V , y dada una aplicación lineal $f: V \rightarrow W$, $f^{**}: V^{**} \rightarrow W^{**}$, donde $f^{**}(\tau) := \tau \circ f^*$, con $\tau \in V^{**}$, y $f^*: W^* \rightarrow V^*$, definida para $\beta \in W^*$, $f^*(\beta) := \beta \circ f$.

Definición 1.23. Sean $F, G: \mathcal{C} \rightarrow \mathcal{D}$ funtores. Una **transformación natural** $\alpha: F \Rightarrow G$ es una familia de morfismos en \mathcal{D}

$$\{\alpha_X: F(X) \rightarrow G(X)\}_{X \in \text{Ob}(\mathcal{C})}$$

de tal manera que, dado cualquier $f: X \rightarrow Y \in \text{Mor}(\mathcal{C})$, es conmutativo el diagrama siguiente:

$$\begin{array}{ccc} F(X) & \xrightarrow{F(f)} & F(Y) \\ \downarrow \alpha_X & & \downarrow \alpha_Y \\ G(X) & \xrightarrow{G(f)} & G(Y). \end{array}$$

Se dice que $\alpha: F \Rightarrow G$ es un **isomorfismo natural** si α_X es un isomorfismo en \mathcal{D} , para todo $X \in \text{Ob}(\mathcal{C})$.

Ejemplo 1.24.

- (i) Sean los funtores $\text{id}_{\text{Set}}, \mathcal{P}: \text{Set} \rightarrow \text{Set}$, identidad y conjunto de partes. Existe una transformación natural $\alpha: \text{id}_{\text{Set}} \Rightarrow \mathcal{P}$ tal que $\alpha_A: A \rightarrow \mathcal{P}(A)$, $\alpha_A(a) := \{a\}$, para cada $a \in A$.
- (ii) Sean los funtores $1_{\text{Vect}}, (-)^{**}: \mathbf{Vect}_K \rightarrow \mathbf{Vect}_K$, identidad y doble dual. Existe una transformación natural $\alpha: 1_{\text{Vect}} \Rightarrow (-)^{**}$ tal que $\alpha_V: V \rightarrow V^{**}$, $\alpha_V(v) := v^{**}$, donde $v^{**}(\sigma) := \sigma(v)$, para cada $\sigma \in V^*$.

Definición 1.25. Sea $F: \mathcal{C} \rightarrow \mathcal{D}$ un functor. F es una **equivalencia de categorías** si existe $G: \mathcal{D} \rightarrow \mathcal{C}$ un functor e isomorfismos naturales $\alpha: G \circ F \Rightarrow \text{id}_{\mathcal{C}}$ y $\beta: \text{id}_{\mathcal{D}} \Rightarrow F \circ G$. En este caso, se dice que las categorías \mathcal{C} y \mathcal{D} son equivalentes.

Ejemplo 1.26. Sea la categoría ${}^f\mathbf{Vect}_K$ la categoría de espacios vectoriales finitos sobre el cuerpo K . Sea \mathbf{Mat}_K la categoría de matrices sobre K , cuyos objetos son el conjunto de los números naturales \mathbb{N} y los morfismos entre dos objetos m y n , $A: m \rightarrow n$, son todas las matrices $n \times m$ con entradas en K . La composición $m \xrightarrow{A} n \xrightarrow{B} p = m \xrightarrow{BA} p$ viene dada por el producto de matrices.

Las categorías ${}^f\mathbf{Vect}_K$ y \mathbf{Mat}_K son equivalentes. El funtor $F: \mathbf{Mat}_K \rightarrow {}^f\mathbf{Vect}_K$ dado por:

$$\begin{aligned} F(n) &:= K^n, \text{ el espacio vectorial de vectores columna sobre } K, \\ F(A) &:= M_A, \text{ para todos los morfismos } m \xrightarrow{A} n, M_A: K^m \rightarrow K^n, \\ &\text{está dado por } M_A(v) := Av, v \in K^m, \end{aligned}$$

y el funtor $G: {}^f\mathbf{Vect}_K \rightarrow \mathbf{Mat}_K$ dado por:

$$\begin{aligned} G(V) &= \dim(V), \text{ donde } V \text{ es un espacio vectorial de dimensión finita sobre } K, \\ G(f) &= M_f, \text{ donde } M_f \text{ es la matriz de la aplicación lineal } f: V \rightarrow W, \\ &\text{con respecto a las bases elegidas } \mathcal{B}_V \text{ y } \mathcal{B}_W \text{ de } V \text{ y } W, \text{ respectivamente,} \end{aligned}$$

definen la equivalencia de categorías.

Definición 1.27. Sea \mathcal{C} una categoría y dado un diagrama en \mathcal{C} de la forma,

$$\begin{array}{ccc} & X & \\ & \downarrow f & \\ Y & \xrightarrow{g} & Z \end{array}$$

se denomina **pullback** a un objeto $P \in \text{Ob}(\mathcal{C})$ acompañado de morfismos

$$\alpha: P \rightarrow X \quad \text{y} \quad \beta: P \rightarrow Y$$

haciendo el siguiente diagrama conmutativo:

$$\begin{array}{ccc} P & \xrightarrow{\alpha} & X \\ \downarrow \beta & & \downarrow f \\ Y & \xrightarrow{g} & Z. \end{array}$$

es decir, $g \circ \beta = f \circ \alpha$, y verificando la siguiente propiedad universal: si existe $P' \in \text{Ob}(\mathcal{C})$ junto con morfismos $\alpha': P' \rightarrow X$ y $\beta': P' \rightarrow Y$ tal que $f \circ \alpha' = g \circ \beta'$, entonces existe un único $h: P' \rightarrow P$ tal que $\alpha \circ h = \alpha'$ y $\beta \circ h = \beta'$. Usualmente P se denota por $X \times_Z Y$.

Observación 1.28. En Set , Grp y Vect_K , el pullback viene dado por:

$$P = \{(x, y) \mid f(x) = g(y)\} \subset X \times Y,$$

donde $X \times Y$ es el producto directo.

Con el fin de hacer más sencilla la notación, denótese por G_0 la clase de todos los objetos en \mathcal{C} , y por G_1 la clase de todos los morfismos en \mathcal{C} . Considérense las aplicaciones *target*, *source* e *identity* como sigue:

$$s: G_1 \rightarrow G_0 \quad t: G_1 \rightarrow G_0 \quad i: G_0 \rightarrow G_1,$$

donde

$$s(x \xrightarrow{f} y) = x, \quad t(x \xrightarrow{f} y) = y, \quad i(x) = x \xrightarrow{\text{id}_x} x.$$

Además, si se denota como $G_1 \times_{G_0} G_1$, al pullback del diagrama:

$$\begin{array}{ccc} & & G_1 \\ & & \downarrow s \\ G_1 & \xrightarrow{t} & G_0 \end{array}$$

se define la aplicación *composición* como

$$\circ: G_1 \times_{G_0} G_1 \rightarrow G_1$$

Con esta notación, los axiomas para que \mathcal{C} sea una categoría introducidos en la Definición 1.18, pueden expresarse únicamente en términos de diagramas. Estos axiomas son equivalentes a la conmutatividad de los siguientes diagramas:

$$\begin{array}{ccc} & G_0 & \\ \text{id}_{G_0} \swarrow & \downarrow i & \searrow \text{id}_{G_0} \\ G_0 & G_1 & G_0 \\ \leftarrow s & \xrightarrow{t} & \end{array} \quad \begin{array}{ccccc} & G_1 \times G_0 & \xleftarrow{\text{id}_{G_1} \times s} & G_1 & \xrightarrow{t \times \text{id}_{G_1}} & G_0 \times G_1 \\ \text{id}_{G_1} \times i \downarrow & & & \downarrow \text{id}_{G_1} & & \downarrow i \times \text{id}_{G_1} \\ G_1 \times_{G_0} G_1 & \xrightarrow{\circ} & G_1 & \xleftarrow{\circ} & G_1 \times_{G_0} G_1 & \end{array} \quad (1.4)$$

$$\begin{array}{ccc} G_1 & \xleftarrow{\pi_2} & G_1 \times_{G_0} G_1 & \xrightarrow{\pi_1} & G_1 \\ s \downarrow & & \downarrow \circ & & \downarrow t \\ G_0 & \xleftarrow{s} & G_1 & \xrightarrow{t} & G_0 \end{array} \quad \begin{array}{ccccc} G_1 \times_{G_0} G_1 & \times_{G_0} & G_1 \times_{G_0} G_1 & \xrightarrow{\circ \times \text{id}_{G_1}} & G_1 \times_{G_0} G_1 \\ \text{id}_{G_1} \times \circ \downarrow & & & & \downarrow \circ \\ G_1 \times_{G_0} G_1 & \xrightarrow{\circ} & G_1 & & G_1 \end{array} \quad (1.5)$$

$$\begin{array}{ccccc} G_0 \times_{G_0} G_1 & \xrightarrow{i \times_{G_0} \text{id}_{G_1}} & G_1 \times_{G_0} G_1 & \xleftarrow{\text{id}_{G_1} \times_{G_0} i} & G_1 \times_{G_0} G_0 \\ & \searrow \pi_2 & \downarrow \circ & \swarrow \pi_1 & \\ & & G_1 & & \end{array} \quad (1.6)$$

Por otro lado, dadas dos categorías \mathcal{C} y \mathcal{C}' y un funtor $F: \mathcal{C} \rightarrow \mathcal{C}'$ tal que:

$$F_0: G_0 \rightarrow G'_0 \quad \text{y} \quad F_1: G_1 \rightarrow G'_1,$$

se tiene que dichas aplicaciones son compatibles con las aplicaciones *source*, *target*, *identity* y la aplicación composición como se ha introducido en la Definición 1.21. Esto significa que los siguientes diagramas conmutan:

$$\begin{array}{ccc}
 G_0 & \xleftarrow{s} G_1 & \xrightarrow{t} G_0 \\
 F_0 \downarrow & & \downarrow F_0 \\
 G'_0 & \xleftarrow{s'} G'_1 & \xrightarrow{t'} G'_0
 \end{array}
 \qquad
 \begin{array}{ccc}
 G_0 & \xrightarrow{i} & G_1 \\
 F_0 \downarrow & & \downarrow F_1 \\
 G'_0 & \xrightarrow{i'} & G'_1
 \end{array}
 \qquad
 \begin{array}{ccc}
 G_1 \times_{G_0} G_1 & \xrightarrow{\circ} & G_1 \\
 F_1 \times F_1 \downarrow & & \downarrow F_1 \\
 G'_1 \times_{G'_0} G'_1 & \xrightarrow{\circ'} & G'_1.
 \end{array}
 \tag{1.7}$$

Capítulo 2

Módulos cruzados de grupos

En este capítulo se presentará la definición formal de módulo cruzado, junto con ejemplos que faciliten su comprensión. También, se desarrollarán resultados fundamentales que caracterizan su comportamiento y propiedades, y que permitirán establecer conexiones con otras estructuras algebraicas. El capítulo se basa fundamentalmente en el desarrollo presentado en [14], el cual constituye la referencia principal para la organización y contenido del mismo.

Definición 2.1. Un **módulo cruzado de grupos** es una terna (M, N, μ) donde M y N son grupos, y $\mu: M \rightarrow N$ es un homomorfismo de grupos. Además, se considera una representación de N por automorfismos de M , denotada por φ :

$$\begin{aligned}\varphi: N &\rightarrow \text{Aut}(M) \\ n &\mapsto \varphi(n): M \rightarrow M \\ &\quad m \mapsto \varphi(n)(m) = {}^n m\end{aligned}$$

tal que, para todo $n \in N$ y todo $m, m' \in M$ satisface:

$$\mu({}^n m) = n\mu(m)n^{-1}, \tag{2.1}$$

$$\mu({}^m m') = mm'm^{-1}. \tag{2.2}$$

La propiedad (2.2) es la conocida como Identidad de Peiffer.

Los módulos cruzados de grupos dan lugar a una categoría cuyos morfismos se definen como sigue. Sean (M, N, μ) y (M', N', μ') módulos cruzados de grupos, un **morfismo de módulos cruzados de grupos** es un par

$$(f, g): (M, N, \mu) \rightarrow (M', N', \mu')$$

donde:

(i) $f: M \rightarrow M'$ es un homomorfismo de grupos,

(ii) $g: N \rightarrow N'$ es un homomorfismo de grupos,

verificando las siguientes condiciones:

$$\mu' \circ f = g \circ \mu, \quad (2.3)$$

$$f(nm) = g(n)f(m). \quad (2.4)$$

Equivalentemente, la condición (2.3) se verifica cuando el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} M & \xrightarrow{\mu} & N \\ f \downarrow & & \downarrow g \\ M' & \xrightarrow{\mu'} & N'. \end{array}$$

Sea φ la acción de N sobre M y φ' la acción de N' sobre M' , la condición (2.4) equivale a que el siguiente diagrama sea conmutativo:

$$\begin{array}{ccc} N \times M & \xrightarrow{\varphi} & M \\ g \times f \downarrow & & \downarrow f \\ N' \times M' & \xrightarrow{\varphi'} & M'. \end{array}$$

La categoría de módulos cruzados de grupos se denotará por \mathbf{XMod} .

Definición 2.2. Sea N un grupo y X e Y conjuntos tales que N actúa sobre X a través de una acción φ , y N actúa sobre Y a través de otra acción ψ . Sea $f: X \rightarrow Y$ una aplicación. Se dice que f es N -**equivariante** si el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} N \times X & \xrightarrow{\text{id}_N \times f} & N \times Y \\ \varphi \downarrow & & \downarrow \psi \\ X & \xrightarrow{f} & Y. \end{array}$$

Es decir, $\psi(n, f(x)) = f(\varphi(n, x))$ para todo $n \in N$ y todo $x \in X$.

Observación 2.3. La propiedad (2.1) significa que el homomorfismo μ es equivariante con respecto a la N -acción vía φ de M y la acción por conjugación de N sobre sí mismo que está dada por:

$$\begin{aligned} \text{conj}: N \times N &\rightarrow N \\ (n, h) &\mapsto nhn^{-1}. \end{aligned}$$

Es decir, que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} N \times M & \xrightarrow{\text{id}_N \times \mu} & N \times N \\ \varphi \downarrow & & \downarrow \text{conj} \\ M & \xrightarrow{\mu} & N. \end{array}$$

En efecto, $\mu(\varphi(n, m)) = \mu({}^n m) \stackrel{(2.1)}{=} n\mu(m)n^{-1} = \text{conj}(n, \mu(m))$.

Observación 2.4. Por la propiedad (2.1), $\text{Im}(\mu)$ es un subgrupo normal de N . En efecto, por ser $\mu: M \rightarrow N$ un homomorfismo de grupos $\text{Im}(\mu)$ es un subgrupo de N y además $n\mu(m)n^{-1} = \mu({}^n m) \in \text{Im}(\mu)$ lo que implica que $\text{Im}(\mu)$ es un subgrupo normal de N .

Observación 2.5. Por la propiedad (2.2), $\mu(m)m' = mm'm^{-1}$ y dado un $m \in \ker(\mu)$ es decir que $\mu(m) = 1$ y entonces $m' = mm'm^{-1}$ o $m'm = mm'$ para todo $m' \in M$. Sea $Z(M)$ el centro del grupo M , se tiene entonces que $\ker(\mu) \subseteq Z(M)$ y, consecuentemente, $\ker(\mu)$ es abeliano.

A continuación, se verán ejemplos de módulos cruzados:

Ejemplo 2.6. Sean M y N dos grupos, y sea:

$$\begin{aligned} \mu: M &\rightarrow N \\ m &\mapsto 1_N. \end{aligned}$$

Se tiene que la terna (M, N, μ) es un módulo cruzado si y solo si M es abeliano.

En efecto, de la propiedad (2.2) se deduce que:

$$m' = {}^{1_N} m' = \mu(m)m' \stackrel{(2.2)}{=} mm'm^{-1}.$$

La igualdad previa solo se cumple si M es abeliano.

Ejemplo 2.7. Sean M y N grupos abelianos con $\mu: M \rightarrow N$ y tal que N actúa trivialmente sobre M (mediante la acción φ), es decir que ${}^n m = m$. Se tiene que la terna (M, N, μ) es un módulo cruzado. En efecto,

(i) Se verifica la propiedad (2.1) pues:

$$\mu(m) = \mu(nm) = n\mu(m)n^{-1} = \mu(m),$$

donde en la última igualdad se emplea que N es un grupo abeliano.

(ii) La verificación de (2.2) es también inmediata teniendo en cuenta que M es abeliano.

En efecto,

$$m' = \mu^{(m)}m' = mm'm^{-1} = m'.$$

Ejemplo 2.8. Sea H un subgrupo normal de G ($H \triangleleft G$) y sea $i: H \rightarrow G$ la inclusión. Se considera, por un lado la acción $\varphi: G \times H \rightarrow H$ tal que $\varphi(g, h) := ghg^{-1}$ donde $ghg^{-1} \in H$ por ser subgrupo normal y por otro lado la acción conjugación conj . Se probará a continuación que la terna (H, G, i) es un módulo cruzado:

(i) Se debe probar primero que i es G -equivariante, es decir, que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} G \times H & \xrightarrow{\text{id}_G \times i} & G \times G \\ \downarrow \varphi & & \downarrow \text{conj} \\ H & \xrightarrow{i} & G. \end{array}$$

Por un lado $\varphi(g, h) = ghg^{-1}$ y, por otro lado, $\text{conj}(g, h) = ghg^{-1}$. Es decir $i(\varphi(g, h)) = \text{conj}(g, i(h))$ tal y como queríamos ver.

(ii) Ahora se debe comprobar la identidad de Peiffer. Esta se cumple ya que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} H \times H & \xrightarrow{i \times \text{id}_H} & G \times H \\ & \searrow \text{conj} & \downarrow \varphi \\ & & H. \end{array}$$

Luego como por un lado $(i \times \text{id}_H)(h, h') = (i(h), h')$ y $\varphi(i(h), h') = {}^{i(h)}h' = hh'h^{-1}$ y por otro lado $\text{conj}(h, h') = hh'h^{-1}$, se tiene que el diagrama es conmutativo verificando así que la terna (H, G, i) es un módulo cruzado.

Un caso particular aplicable al anterior ejemplo podría ser considerar como H el grupo de las permutaciones pares de orden 3 (A_3) y como G el grupo de las permutaciones de orden 3 (S_3). Claramente, A_3 es un subgrupo normal de S_3 ($A_3 \triangleleft S_3$).

Ejemplo 2.9. Sean M y N grupos cíclicos de orden 4, $M = \langle m \rangle$ y $N = \langle n \rangle$. Sea el homomorfismo de grupos dado por $\mu: M \rightarrow N$ tal que $\mu(m) = n^2$. Se considera la acción $\varphi: N \times M \rightarrow M$ tal que $\varphi(n, m) = m^{-1} := {}^n m$ y conj la acción conjugación. Veamos que la terna (M, N, μ) es un módulo cruzado:

- (i) Se comprueba primero la condición de N -equivariante probando que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} N \times M & \xrightarrow{\text{id}_N \times \mu} & N \times N \\ \downarrow \varphi & & \downarrow \text{conj} \\ M & \xrightarrow{\mu} & N \end{array}$$

En efecto, se tiene que por un lado $(\text{id}_N \times \mu)(n, m) = (n, \mu(m)) = (n, n^2)$ y $\text{conj}(n, n^2) = nn^2n^{-1} \stackrel{(a)}{=} n^2$ y por otro $\varphi(n, m) = m^{-1} := {}^n m$ y $\mu(m^{-1}) \stackrel{(b)}{=} (\mu(m))^{-1} = (n^2)^{-1} \stackrel{(c)}{=} n^2$.

En (a) se ha empleado la conmutatividad del grupo cíclico N , en (b) se ha empleado el hecho de que μ es un homomorfismo de grupos y en (c) que al ser N un grupo cíclico de orden 4 se tiene que $n^2n^2 = n^4 = 1$ lo que implica que $(n^2)^{-1} = n^2$.

Con todo, se concluye que el diagrama conmuta por lo que se tiene que μ es N -equivariante.

- (ii) Se debe comprobar ahora la Identidad de Peiffer.

$$\begin{array}{ccc} M \times M & \xrightarrow{\mu \times \text{id}_M} & N \times M \\ & \searrow \text{conj} & \downarrow \varphi \\ & & M \end{array}$$

Donde por un lado $(\mu \times \text{id}_M)(m, m) = (\mu(m), m) = (n^2, m)$ y $\varphi(n^2, m) = {}^{n^2} m = {}^{nn} m \stackrel{(1.2)}{=} n({}^n m) = {}^n m^{-1} \stackrel{(a)}{=} ({}^n m)^{-1} = (m^{-1})^{-1} = m$, y por otro $\text{conj}(m, m) \stackrel{(b)}{=} m$.

$mm^{-1}m = m$. En (a) se emplean las propiedades de los automorfismos y en (b) la conmutatividad del grupo cíclico M .

Luego se ha demostrado que el diagrama anterior es conmutativo y por tanto se verifica la Identidad de Peiffer.

Se concluye entonces que la terna (M, N, μ) es un módulo cruzado.

Ejemplo 2.10. Sean $M = \langle m \rangle$ y $N = \langle n \rangle$ grupos cíclicos de orden 4. Sea el homomorfismo de grupos dado por $\mu: M \rightarrow N$ tal que $\mu(m) = n^2$. Se considera la acción $\varphi: N \times M \rightarrow M$ trivial, i.e. $\varphi(n, m) := m$. Entonces el par (μ, φ) es un módulo cruzado.

Ejemplo 2.11. Sea una extensión central

$$E \cong 1 \rightarrow H \xrightarrow{\alpha} N \xrightarrow{\beta} K \rightarrow 1,$$

con $\alpha(H) \subseteq Z(N)$ (véase 1.15). Esta situación define un módulo cruzado con la acción $\alpha^{(h)}h' = hh'h^{-1}$. Se comprobará a continuación que esta acción está bien definida.

Sean $h_1, h, h' \in H$. Se supone que $\alpha(h_1) = \alpha(h)$ y se desea comprobar si $\alpha^{(h)}h' = \alpha^{(h_1)}h'$ es decir, si $hh'h^{-1} = h_1h'h_1^{-1}$. Como $\alpha(h_1) = \alpha(h)$ y α es un homomorfismo de grupos, se tiene que $\alpha(h_1h^{-1}) = 1$ lo que implica que $h_1h^{-1} \in \ker(\alpha)$. Por la observación (2.5), $\ker(\alpha) \subseteq Z(H)$ luego $z := h_1h^{-1} \in Z(H)$ y en particular $h_1 = hz$ con $z \in Z(H)$. Entonces,

$$h_1h'h_1^{-1} = hzh'z^{-1}h^{-1}$$

y como $z \in Z(H)$, se tiene que $zh' = h'z$, por lo que:

$$h_1h'h_1^{-1} = hzh'z^{-1}h^{-1} = hh'zz^{-1}h^{-1} = hh'h^{-1},$$

lo que prueba que la acción está bien definida, es decir, no depende del representante escogido.

Por otro lado, un módulo cruzado simplemente conexo (i.e. α es sobreyectiva) es una extensión central.

En particular, $H \xrightarrow{\text{conj}} \text{Inn}(H)$, $h \mapsto \text{conj}(h)$, con la acción, ${}^{\text{conj}(h)}h' = hh'h^{-1}$, es un módulo cruzado de grupos, donde $\text{Inn}(H)$ denota los automorfismos internos de un grupo H .

Ejemplo 2.12. Para un grupo (G, \cdot) se considera el producto semidirecto $G \rtimes G$ con la multiplicación $(g_1, g_2)(x_1, x_2) = (g_1g_2x_1g_2^{-1}, g_2x_2)$. Entonces $(G, G \rtimes G, \mu)$ es un módulo cruzado, donde $\mu(g) = (g^{-1}, g)$, y la acción de $G \rtimes G$ en G está dada por ${}^g x = xg^{-1}$.

Ejemplo 2.13. Sea el homomorfismo de grupos

$$\begin{aligned} \mu: \mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} &\rightarrow \mathbb{Z}/2\mathbb{Z} = \{0, 1\} \\ \bar{n} &\mapsto \mu(\bar{n}) = 0, \end{aligned}$$

y sea la acción de $\mathbb{Z}/2\mathbb{Z}$ sobre $\mathbb{Z}/4\mathbb{Z}$:

$$\begin{aligned} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} &\rightarrow \mathbb{Z}/4\mathbb{Z} \\ (x, \bar{n}) &\mapsto x\bar{n} = \begin{cases} \bar{n} & \text{si } x = 0, \\ \bar{2n} & \text{si } x = 1. \end{cases} \end{aligned}$$

Se verificará el cumplimiento de las propiedades (2.1) y (2.2) para determinar si $(\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mu)$ se trata de un módulo cruzado.

- (i) Se comenzará probando que se cumple la propiedad (2.1). Dado que $\mathbb{Z}/n\mathbb{Z}$ es un grupo abeliano respecto de la suma, se adoptará en lo sucesivo la notación aditiva.

Se obtiene por un lado que $\mu(x\bar{n}) = 0$ y por otro que, teniendo en cuenta que el grupo es abeliano, $x + \mu(\bar{n}) - x = \mu(\bar{n}) = 0$. Es decir,

$$\mu(x\bar{n}) = x + \mu(\bar{n}) - x.$$

De lo anterior se deduce que la propiedad (2.1) se satisface.

- (ii) A continuación se verificará la propiedad (2.2) (identidad de Peiffer), la cual permitirá concluir que la estructura en cuestión constituye un módulo cruzado.

Por un lado, $\mu(\bar{n})\bar{m} = \bar{0}\bar{m} = \bar{m}$ y por otro lado, por ser el grupo abeliano, $\bar{n} + \bar{m} - \bar{n} = \bar{m}$. Consecuentemente,

$$\mu(\bar{n})\bar{m} = \bar{n} + \bar{m} - \bar{n} = \bar{m}.$$

Esto corresponde, precisamente, a la propiedad (2.2).

Observación 2.14. A cada módulo cruzado de grupos $\mu: M \rightarrow N$ se le puede asociar una sucesión exacta de cuatro términos:

$$0 \rightarrow V \xrightarrow{i} M \xrightarrow{\mu} N \xrightarrow{\pi} G \xrightarrow{p} 1,$$

donde, por ser la sucesión exacta, $\ker(\mu) = \text{Im}(i) = i(V) = V$ y como $\text{Coker}(\mu) = N/\text{Im}(\mu)$ y por ser la sucesión exacta, $\text{Im}(\mu) = \ker(\pi)$ se tiene que $\text{Coker}(\mu) = N/\ker(\pi)$. Ahora, aplicando el Primer Teorema de Isomorfía y teniendo en cuenta que por ser la sucesión exacta $\text{Im}(\pi) = \ker(p) = G$, se tiene que $N/\ker(\pi) = \text{Im}(\pi) = G$. Con todo, $G = \text{Coker}(\mu)$.

Observación 2.15. (i) Considérese $\mu: M \rightarrow N$ un módulo cruzado de grupos y la sucesión exacta asociada:

$$V = \ker(\mu) \xrightarrow{i} M \xrightarrow{\mu} N \xrightarrow{\pi} G = \frac{N}{\text{Im}(\mu)}.$$

Se define a continuación:

$$\begin{aligned} G &\rightarrow \text{Aut}(M) \xrightarrow{p} \text{Out}(M) \\ \bar{n} &\mapsto \varphi(n): M \rightarrow M \\ & m \mapsto \varphi(n)(m) := {}^n m. \end{aligned}$$

Se desea verificar si esta aplicación es un homomorfismo de grupos, ya que eso sería equivalente a comprobar que define una acción de G sobre M .

- (1) En primer lugar, se comprobará si la aplicación anterior está bien definida, es decir, que no depende del representante tomado. Sean $n, n' \in N$ tales que $\bar{n} = \bar{n}'$, se tiene:

$$\begin{aligned} (\varphi(n) \circ (\varphi(n'))^{-1})(m) &\stackrel{(a)}{=} (\varphi(n) \circ \varphi((n')^{-1}))(m) \stackrel{(b)}{=} \varphi(n(n')^{-1})(m) \\ &\stackrel{(c)}{=} \varphi(\mu(m'))(m) \stackrel{(d)}{=} \mu(m')m \stackrel{(e)}{=} m'm(m')^{-1} = \text{conj}_{m'}(m). \end{aligned} \tag{2.5}$$

En (a) y en (b) se ha empleado que φ es un homomorfismo de grupos. En (c) se tiene en cuenta que si $\bar{n} = \bar{n}'$ en G entonces $n(n')^{-1} \in \text{Im}(\mu)$ y esto implica que existe un $m' \in M$ tal que $\mu(m') = n(n')^{-1}$. En (d) se usó que $\varphi(n)(m) := {}^n m$ y en (e) la propiedad (2.2).

Las igualdades establecidas en (2.5) implican que :

$$\varphi(n) \circ (\varphi(n'))^{-1} = \text{conj}'_m \implies \varphi(n) = \text{conj}'_m \circ \varphi(n').$$

De donde, tomando clases módulo $\text{Inn}(M)$, se llega a que:

$$\overline{\varphi(n)} = \overline{\text{conj}'_m} \circ \overline{\varphi(n')} \implies \overline{\varphi(n)} = \overline{\varphi(n')}.$$

- (2) A continuación, se verificará si la aplicación constituye un homomorfismo de grupos. Se quiere comprobar que si dados $\pi(x) = \bar{n}\bar{r}$, $\pi(n) = \bar{n}$ y $\pi(r) = \bar{r}$ con $\bar{n}\bar{r} = \bar{n}\bar{r}$, entonces se cumple que:

$$\begin{aligned} \varphi(x) &= \varphi(n) \circ \varphi(r) \\ &\implies \varphi(n) \circ \varphi(r) \circ (\varphi(x))^{-1} = \text{id}_M \\ &\implies \varphi(n) \circ \varphi(r) \circ \varphi((x)^{-1}) = \text{id}_M \\ &\implies \varphi(nr x^{-1}) = \text{id}_M. \end{aligned}$$

Por un lado,

$$\begin{aligned}\pi(nrx^{-1}) &\stackrel{(a)}{=} \pi(n)\pi(r)\pi(x)^{-1} = \overline{nr(nr)^{-1}} = \overline{1_N} \\ &\implies nrx^{-1} \in \ker(\pi) \stackrel{(b)}{=} \text{Im}(\mu) \implies nrx^{-1} = \mu(m) \text{ para cierto } m \in M.\end{aligned}$$

En el paso (a) se usa el hecho de que π es un homomorfismo de grupos y en el (b) que la sucesión es exacta.

Por lo tanto,

$$\begin{aligned}\varphi(nrx^{-1})(m') &= \varphi(\mu(m))(m') = \mu^{(m)}m' = mm'm^{-1} \implies \varphi(nrx^{-1}) = \text{conj}_m \\ &\xrightarrow{\text{Tomando clases}} \overline{\varphi(nrx^{-1})} = \overline{\text{conj}_m} = \overline{\text{id}_M}.\end{aligned}$$

Es decir, en general, la aplicación $G \rightarrow \text{Aut}(M)$ no es un homomorfismo de grupos lo que implica que no define una acción de G sobre M , pero sí que lo es cuando se toman clases módulo $\text{Inn}(M)$. Por lo tanto, de acuerdo con la Definición 1.17, φ se trata de una acción externa.

- (ii) Ahora bien, si se realiza el mismo procedimiento que en el apartado anterior pero tomando $V = \ker(\mu)$ en vez de todo M , sí que se obtiene una acción de G sobre V .

$$\begin{aligned}G \times V &\rightarrow V \\ (\bar{n}, m) &\mapsto {}^n m, \text{ con } n \text{ tal que } \pi(n) = \bar{n}.\end{aligned}$$

A continuación, se demostrará que dicha aplicación constituye una acción. Para ello, se verificará que está bien definida y que satisface los axiomas correspondientes a una acción.

- (1) Para demostrar que está bien definida, se deben verificar dos condiciones: en primer lugar, que ${}^n m$ pertenece a V ; y en segundo lugar, que el valor obtenido es independiente del representante escogido.

Por un lado,

$$\mu({}^n m) \stackrel{(2.1)}{=} n\mu(m)n^{-1} \stackrel{(a)}{=} nn^{-1} = 1_N \implies {}^n m \in \ker(\mu) = V.$$

En (a) se ha empleado que $m \in V = \ker(\mu)$ lo que implica que $\mu(m) = 1_N$. Con esto, la primera condición queda demostrada.

Por otro lado,

$$\begin{aligned}\bar{n} = \bar{n}' &\implies n^{-1}n' \in \text{Im}(\mu) \\ &\implies \text{existe } m \in M \mid n^{-1}n' = \mu(m) \implies n' = n\mu(m).\end{aligned}$$

Entonces,

$${}^{n'}m' = {}^{n\mu(m)}m' \stackrel{(1.2)}{=} {}^{n(\mu(m))}m' \stackrel{(2.2)}{=} {}^{n(mm'm^{-1})} \stackrel{(b)}{=} {}^nm'.$$

En (b) se ha empleado que $m' \in V \subset Z(M)$, por ser $V = \ker(\mu)$ un grupo abeliano. Se tiene entonces que la segunda condición también se cumple, concluyendo así que no depende del representante escogido.

- (2) Es claro que la aplicación cumple con los axiomas de acción, dado que ha sido definida como tal.

$$\begin{aligned} (\overline{1_N}, m) &\rightarrow {}^{1_N}m = m, \\ (\overline{nr}, m) &\rightarrow {}^{nr}m = {}^n(rm). \end{aligned}$$

Definición 2.16. Sean $\mu: M \rightarrow N$ (con una acción φ) y $\mu': M' \rightarrow N'$ (con una acción φ') dos módulos cruzados tales que $\ker(\mu) = \ker(\mu') =: V$ y $\text{Coker}(\mu) = \text{Coker}(\mu') =: G$, son **equivalentemente elementales** si $\Phi: M \rightarrow M'$ y $\Psi: N \rightarrow N'$ son homomorfismos de grupos compatibles con las respectivas acciones, esto es,

$$\Phi(\varphi(n)(m)) = \varphi'(\Psi(n))(\Phi(m)),$$

para todo $n \in N$ y todo $m \in M$, y tal que el siguiente diagrama es conmutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V & \xrightarrow{i} & M & \xrightarrow{\mu} & N & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \text{id}_V \parallel & & \downarrow \Phi & & \downarrow \Psi & & \text{id}_G \parallel & & \\ 0 & \longrightarrow & V & \xrightarrow{i'} & M' & \xrightarrow{\mu'} & N' & \xrightarrow{\pi'} & G & \longrightarrow & 1. \end{array}$$

Notar que la relación de equivalencia elemental es reflexiva y transitiva. En efecto,

- (i) **Propiedad reflexiva.** Tomando $\Phi = \text{id}_M$ y $\Psi = \text{id}_N$:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V & \xrightarrow{i} & M & \xrightarrow{\mu} & N & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \text{id}_V \parallel & & \text{id}_M \parallel & & \text{id}_N \parallel & & \text{id}_G \parallel & & \\ 0 & \longrightarrow & V & \xrightarrow{i} & M & \xrightarrow{\mu} & N & \xrightarrow{\pi} & G & \longrightarrow & 1. \end{array}$$

Se tiene que $\text{id}_N \circ \mu = \mu = \mu \circ \text{id}_M$.

(ii) **Propiedad transitiva.**

$$\begin{array}{ccccccccc}
 0 & \longrightarrow & V & \xrightarrow{i} & M & \xrightarrow{\mu} & N & \xrightarrow{\pi} & G & \longrightarrow & 1 \\
 & & \parallel & & \downarrow \Phi_1 & & \downarrow \Psi_1 & & \parallel & & \\
 & & \text{id}_V & & & & & & \text{id}_G & & \\
 0 & \longrightarrow & V & \xrightarrow{i'} & M' & \xrightarrow{\mu'} & N' & \xrightarrow{\pi'} & G & \longrightarrow & 1 \\
 & & \parallel & & \downarrow \Phi_2 & & \downarrow \Psi_2 & & \parallel & & \\
 & & \text{id}_V & & & & & & \text{id}_G & & \\
 0 & \longrightarrow & V & \xrightarrow{i''} & M'' & \xrightarrow{\mu''} & N'' & \xrightarrow{\pi''} & G & \longrightarrow & 1.
 \end{array}$$

El primer diagrama conmuta (por ser μ y μ' equivalentemente elementales):

$$\Psi_1 \circ \mu = \mu' \circ \Phi_1.$$

Y el segundo diagrama también conmuta (por ser μ' y μ'' equivalentemente elementales):

$$\Psi_2 \circ \mu' = \mu'' \circ \Phi_2.$$

Componiendo a ambos lados, se obtiene:

$$(\Psi_2 \circ \Psi_1) \circ \mu = \Psi_2 \circ (\Psi_1 \circ \mu) = \Psi_2 \circ (\mu' \circ \Phi_1) = (\Psi_2 \circ \mu') \circ \Phi_1 = (\mu'' \circ \Phi_2) \circ \Phi_1 = \mu'' \circ (\Phi_2 \circ \Phi_1).$$

Esto demuestra que el diagrama total, compuesto por los dos anteriores, también conmuta. Es decir, se cumple la propiedad transitiva.

La relación de equivalencia anterior es reflexiva y transitiva como se ha visto pero **no es simétrica** en general, ya que los homomorfismos Φ y Ψ no tienen por qué ser invertibles.

Se llama **equivalencia de módulos cruzados** a la relación de equivalencia generada por la equivalencia elemental. Es decir, dos módulos cruzados son equivalentes si existe un zigzag de equivalencias elementales que va de uno al otro (donde las flechas no van necesariamente en la misma dirección), lo que garantiza el cumplimiento de la propiedad simétrica. El siguiente diagrama ilustra esta situación:

$$\begin{array}{ccccccccc}
 0 & \longrightarrow & V & \xrightarrow{i'} & M' & \xrightarrow{\mu} & N' & \xrightarrow{\pi'} & G & \longrightarrow & 1 \\
 & & \parallel & & \uparrow & & \uparrow & & \parallel & & \\
 & & & & & & & & & & \\
 0 & \longrightarrow & V & \xrightarrow{i} & M & \xrightarrow{\mu'} & N & \xrightarrow{\pi} & G & \longrightarrow & 1 \\
 & & \parallel & & \downarrow & & \downarrow & & \parallel & & \\
 & & & & & & & & & & \\
 0 & \longrightarrow & V & \xrightarrow{i''} & M'' & \xrightarrow{\mu''} & N'' & \xrightarrow{\pi''} & G & \longrightarrow & 1.
 \end{array}$$

Se denota por $\text{crmod}(G, V)$ al conjunto de clases de equivalencia de módulos cruzados con núcleo fijo V y con conúcleo fijo G .

Se consideran ahora los dos módulos cruzados $\mu: M \rightarrow N$ y $\mu': M' \rightarrow N'$ con el mismo núcleo V y el mismo conúcleo G y sus correspondientes sucesiones exactas de cuatro términos:

$$0 \rightarrow V \xrightarrow{i} M \xrightarrow{\mu} N \xrightarrow{\pi} G \rightarrow 1$$

y

$$0 \rightarrow V \xrightarrow{i'} M' \xrightarrow{\mu'} N' \xrightarrow{\pi'} G \rightarrow 1.$$

Se denota por $K := \{(v, -v) \mid v \in V\}$ al núcleo de la aplicación adición:

$$\begin{aligned} V \oplus V &\rightarrow V \\ (v, v') &\mapsto v + v'. \end{aligned}$$

Notar que la diagonal $\Delta_V: V \rightarrow V \oplus V, v \rightarrow (v, v)$, seguida de la aplicación cociente $V \oplus V \rightarrow (V \oplus V)/K$ identifica V con el cociente $(V \oplus V)/K$.

La identificación se hace de la siguiente manera:

$$V \xrightarrow{\Delta_V} V \oplus V \rightarrow (V \oplus V)/K, \quad v \mapsto (v, v) \mapsto \overline{(v, v)}.$$

Nótese, que esta correspondencia, es claramente inyectiva, ya que si $\overline{(v, v)} = \overline{(0, 0)}$, entonces $(v, v) \in K$, y por lo tanto $v = -v$, y así $v = 0$.

Además, es sobreyectiva, ya que $\overline{(v_1, v_2)} = \overline{(\frac{v_1+v_2}{2}, \frac{v_1+v_2}{2})}$, pues $(v_1, v_2) = (\frac{v_1+v_2}{2}, \frac{v_1+v_2}{2}) + (\frac{v_1-v_2}{2}, -\frac{v_1-v_2}{2})$.

El conjunto K puede ser considerado como un subespacio en $M \times M'$ mediante $i \times i'$. Como V es central en M y M' , entonces K es un subgrupo normal de $M \times M'$.

La restricción de $\pi \times \pi'$ a $N \times_G N'$ toma valores en la diagonal:

$$\Delta_G := \{(g, g) \mid g \in G\},$$

que es isomorfa a G mediante (la restricción de) la aplicación diagonal $\Delta_G: G \rightarrow \Delta_G \subset G \times G$. Teniendo en cuenta los preliminares anteriores, se obtiene la siguiente definición:

Definición 2.17. La **suma de dos módulos cruzados** $\mu: M \rightarrow N$ y $\mu': M' \rightarrow N'$ tales que $\ker(\mu) = \ker(\mu') = V$ y $\text{Coker}(\mu) = \text{Coker}(\mu') = G$ es por definición el módulo cruzado:

$$0 \rightarrow V \xrightarrow{(i \oplus i') \circ \Delta_V} (M \times M')/K \xrightarrow{\mu \times \mu'} N \times_G N' \xrightarrow{(\Delta_G)^{-1} \circ (\pi \times \pi')} G \rightarrow 1.$$

La acción de $N \times_G N'$ en $(M \times M')/K$ está inducida por el producto de las acciones de los dos factores. Las propiedades (2.1) y (2.2) se verifican en el producto directo, y por lo tanto, en la suma del módulo cruzado. En efecto:

- (i) En primer lugar se quiere probar que se verifica la propiedad (2.1). Es decir, que para $[(m, m')] \in (M, M')/K$ y $(n, n') \in N \times_G N'$,

$$(\mu \times \mu')^{(n, n')}(m, m') = (n, n')(\mu(m), \mu'(m'))(n, n')^{-1}.$$

La acción de (n, n') sobre (m, m') es por componentes:

$${}^{(n, n')} (m, m') = ({}^n m, {}^{n'} m'),$$

aplicando $\mu \times \mu'$, se obtiene:

$$(\mu \times \mu')^{(n, n')}(m, m') = (\mu({}^n m), \mu'({}^{n'} m')).$$

Dado que μ y μ' son módulos cruzados que cumplen (2.1):

$$(\mu({}^n m), \mu'({}^{n'} m')) \stackrel{(2.1)}{=} (n\mu(m)n^{-1}, n'\mu'(m')n'^{-1}) = (n, n')(\mu(m), \mu'(m'))(n, n')^{-1}.$$

Probando así que efectivamente se verifica la propiedad (2.1).

- (ii) En segundo lugar, se quiere demostrar la propiedad (2.2),

$$(\mu^{(m)}, \mu'^{(m')})(m_\star, m'_\star) = (m, m')(m_\star, m'_\star)(m, m')^{-1}.$$

Como la acción es componente a componente, y μ y μ' satisfacen (2.2):

$$\begin{aligned} (\mu^{(m)}, \mu'^{(m')})(m_\star, m'_\star) &= (\mu^{(m)} m_\star, \mu'^{(m')} m'_\star) = \\ &\stackrel{(2.2)}{=} (m m_\star m^{-1}, m' m'_\star m'^{-1}) \\ &= (m, m')(m_\star, m'_\star)(m, m')^{-1}. \end{aligned}$$

Como se quería demostrar.

Lema 2.18. *La suma de módulos cruzados define una estructura de grupo abeliano en el conjunto de clases de equivalencia de módulos cruzados $\text{crmod}(G, V)$ con núcleo fijo V y conúcleo fijo G .*

Demostración. Se debe probar que la suma de módulos cruzados define una estructura de grupo abeliano en el conjunto de clases de equivalencia, es decir, que cumple la propiedad asociativa, tiene elemento neutro, inverso y además cumple la propiedad conmutativa (abeliano).

Es claro que la suma de módulos cruzados es asociativa y conmutativa (hasta equivalencia, es decir, que estas propiedades se cumplen para las clases de equivalencia), ya que está inducida por el producto directo. En efecto, sean A, B y C grupos, el producto directo cumple:

(i) Asociatividad:

$$(A \times B) \times C \cong A \times (B \times C)$$

(ii) Conmutatividad:

$$A \times B \cong B \times A$$

Entonces, si la suma de módulos cruzados se define mediante el producto directo (con ciertas condiciones adicionales, como que el núcleo sea V y el conúcleo sea G), esas propiedades se heredan naturalmente, aunque sólo hasta equivalencia.

Igualmente, es evidente que la suma es compatible con la relación de equivalencia, ya que podemos tomar el producto de los morfismos que inducen las equivalencias. Esto significa que si dos módulos cruzados $\mu: M \rightarrow N$ y $\mu': M' \rightarrow N'$ son equivalentes a otros dos $\mu_\star: M_\star \rightarrow N_\star$ y $\mu'_\star: M'_\star \rightarrow N'_\star$, entonces los productos $(M \times M')/K$ y $(M_\star \times M'_\star)/K_\star$ serán también equivalentes. Esto es así pues, la siguiente operación sobre las clases de equivalencia está bien definida:

$$[\mu] + [\mu'] := [\mu \oplus \mu']$$

Es decir, la suma respeta las clases de equivalencia.

Ahora falta por demostrar que existe un elemento neutro y un inverso para cada módulo cruzado. Definimos el módulo cruzado cero, con núcleo V y conúcleo G como:

$$0 \rightarrow V \xrightarrow{\text{id}_V} V \xrightarrow{1} G \xrightarrow{\text{id}_G} G \rightarrow 1,$$

donde la aplicación $1: V \rightarrow G$ lleva los elementos de V a la unidad $1 \in G$. Sea $[\mu]$ un módulo cruzado en el conjunto de clases de equivalencia tal que $\mu: M \rightarrow N$ y tal que hay acciones sobre M y N . Al sumar este módulo cruzado con el módulo cruzado cero es evidente que la acción del módulo cruzado cero no modifica los elementos de M ni de N pues:

- (i) Acción sobre M : La acción de id_V sobre V no cambia los elementos de V , y la aplicación 1 lleva los elementos de V a $1 \in G$ lo que no afecta a la estructura de los elementos de M .
- (ii) Acción sobre N : Análogamente, la acción de N de la aplicación id_G no cambia los elementos de N .

De tal forma que:

$$[\mu] + [0] = [\mu] = [0] + [\mu].$$

Concluyendo así que el módulo cero es el elemento neutro.

Por otro lado, el inverso de un módulo cruzado

$$0 \rightarrow V \xrightarrow{i} M \xrightarrow{\mu} N \xrightarrow{\pi} G \rightarrow 1,$$

está definido por

$$0 \rightarrow V \xrightarrow{-i} M \xrightarrow{\mu} N \xrightarrow{\pi} G \rightarrow 1,$$

La demostración de que dicho módulo cruzado es inverso al dado se puede ver en [14]. \square

Capítulo 3

Definiciones equivalentes de módulos cruzados

El concepto de módulo cruzado admite múltiples formulaciones equivalentes que surgen de manera natural en distintos marcos algebraicos y categóricos.

En la primera sección se analiza la equivalencia entre los Cat^1 -grupos y los módulos cruzados, estableciendo correspondencias estructurales precisas entre estas dos nociones. Para el desarrollo de esta parte se emplean como referencias principales [3], [5] y [6]. Se dedica la segunda sección a los 2-grupos estrictos, presentando su interpretación como una forma categórica de los módulos cruzados; para ello se siguen los enfoques propuestos en [11] y [14]. Finalmente, la tercera sección está dedicada al análisis de los grupos categóricos estrictos, cuya interpretación y relación con los módulos cruzados se apoya en los resultados y técnicas desarrolladas en [13].

3.1. Cat^1 -grupos y módulos cruzados

Definición 3.1. Un Cat^1 -grupo (G, P, i, s, t) consiste en dos grupos G y P , una inclusión $i: P \rightarrow G$ y dos homomorfismos sobreyectivos $s, t: G \rightarrow P$ satisfaciendo:

$$s \circ i = t \circ i = \text{id}_P, \quad (3.1)$$

$$[\ker(s), \ker(t)] = \{1_G\}. \quad (3.2)$$

Los Cat^1 -grupos dan lugar a una categoría cuyos morfismos se definen como sigue. Sean (G, P, i, s, t) y (G', P', i', s', t') Cat^1 -grupos, un **morfismo de Cat^1 -grupos** es un par

$$(x, y): (G, P, i, s, t) \rightarrow (G', P', i', s', t')$$

donde

(i) $x: G \rightarrow G'$ es un homomorfismo de grupos,

(ii) $y: P \rightarrow P'$ es un homomorfismo de grupos,

verificando las siguientes condiciones:

$$y \circ s = s' \circ x, \quad (3.3)$$

$$y \circ t = t' \circ x, \quad (3.4)$$

$$x \circ i = i' \circ y. \quad (3.5)$$

Equivalentemente, las condiciones (3.3), (3.4) y (3.5) se verifican cuando el siguiente diagrama es conmutativo:

$$\begin{array}{ccc}
 G & \begin{array}{c} \xrightarrow{s} \\ \xleftarrow{t} \end{array} & P \\
 \downarrow x & \begin{array}{c} \curvearrowright \\ i \end{array} & \downarrow y \\
 G' & \begin{array}{c} \xrightarrow{s'} \\ \xleftarrow{t'} \end{array} & P' \\
 & \begin{array}{c} \curvearrowleft \\ i' \end{array} &
 \end{array}$$

La categoría de Cat^1 -grupos se denotará por Cat^1 .

Observación 3.2. La propiedad (3.1) es equivalente a que $s|_P = \text{id}_P$ y $t|_P = \text{id}_P$.

Lema 3.3. *Para un Cat^1 -grupo (G, P, i, s, t) ,*

$$G \cong \ker(s) \rtimes P.$$

Demostración. Sea $\phi: G \rightarrow \ker(s) \rtimes P$ con $\phi(g) := (gi(s(g^{-1})), s(g)) = (gs(g^{-1}), s(g))$ y $\psi: \ker(s) \rtimes P \rightarrow G$ con $\psi(c, p) := ci(p) = cp$, donde se está identificando $i(a) = a$ para todo $a \in P$. Se comprobará que ϕ y ψ son homomorfismos y que $\psi = \phi^{-1}$. En efecto,

(i) Se quiere ver que $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$. Por un lado,

$$\phi(g_1g_2) = (g_1g_2s((g_1g_2)^{-1}), s(g_1g_2))$$

por otro lado,

$$\phi(g_1) = (g_1s(g_1^{-1}), s(g_1)) \quad \text{y} \quad \phi(g_2) = (g_2s(g_2^{-1}), s(g_2)).$$

Ahora bien, teniendo en cuenta que:

$$\begin{aligned}
 \varphi: P \times \ker(s) &\rightarrow \ker(s) \\
 (p, a) &\mapsto pa := i(p)a = i(p)ai(p)^{-1} = pap^{-1},
 \end{aligned}$$

y empleando el producto semidirecto construido a partir de la acción φ , dicho producto viene dado por:

$$(a_1, p_1)(a_2, p_2) = (a_1^{p_1} a_2, p_1 p_2) = (a_1 p_1 a_2 p_1^{-1}, p_1 p_2).$$

A partir de lo anterior,

$$\begin{aligned} \phi(g_1)\phi(g_2) &= (g_1 s(g_1^{-1}), s(g_1))(g_2 s(g_2^{-1}), s(g_2)) \\ &= (g_1 s(g_1^{-1})^{s(g_1)}(g_2 s(g_2^{-1})), s(g_1)s(g_2)) \\ &= (g_1 s(g_1^{-1}) s(g_1) g_2 s(g_2^{-1}) (s(g_1))^{-1}, s(g_1)s(g_2)) \\ &= (g_1 g_2 s(g_2^{-1}) s(g_1^{-1}), s(g_1)s(g_2)), \end{aligned}$$

donde se ha empleado que s es un homomorfismo de grupos, y entonces $s(g_1^{-1}) = s(g_1)^{-1}$.

Ahora bien, se obtuvo que

$$\phi(g_1 g_2) = (g_1 g_2 s((g_1 g_2)^{-1}), s(g_1 g_2)),$$

teniendo en cuenta que s es un homomorfismo de grupos y por tanto $s(g_1 g_2) = s(g_1)s(g_2)$ y que $s((g_1 g_2)^{-1}) = s(g_2^{-1} g_1^{-1}) = s(g_2^{-1})s(g_1^{-1})$ se tiene el resultado, concluyendo que ϕ es un homomorfismo de grupos.

(ii) Se demostrará a continuación que $\psi((c_1, p_1)(c_2, p_2)) = \psi(c_1, p_1)\psi(c_2, p_2)$.

Empleando el producto semidirecto,

$$(c_1, p_1)(c_2, p_2) = (c_1^{p_1} c_2, p_1 p_2) = (c_1 p_1 c_2 p_1^{-1}, p_1 p_2)$$

entonces

$$\psi((c_1, p_1)(c_2, p_2)) = \psi(c_1 p_1 c_2 p_1^{-1}, p_1 p_2) = c_1 p_1 c_2 p_1^{-1} p_1 p_2 = c_1 p_1 c_2 p_2$$

y

$$\psi(c_1, p_1)\psi(c_2, p_2) = c_1 p_1 c_2 p_2.$$

Con lo cual, queda demostrado que ψ es un homomorfismo de grupos.

(iii) Por último, falta comprobar que $\psi = \phi^{-1}$.

Por un lado, se demostrará que $\psi(\phi(g)) = g$. En efecto,

$$\begin{aligned} \psi(\phi(g)) &= \psi(g s(g^{-1}), s(g)) \\ &= g s(g^{-1}) s(g) \\ &= g s(g)^{-1} s(g) \\ &= g. \end{aligned}$$

Por otro lado, hace falta ver que $\phi(\psi(c, p)) = (c, p)$.

$$\begin{aligned}\phi(\psi(c, p)) &= \phi(cp) = (cps((cp)^{-1}), s(cp)) \\ &= (cps(p^{-1}c^{-1}), s(cp)) = (cps(p^{-1})s(c^{-1}), s(c)s(p)).\end{aligned}$$

Teniendo en cuenta que $s(p^{-1}) = s(p)^{-1} = p^{-1}$ y $s(p) = p$ debido a (3.1), entonces:

$$(cps(p^{-1})s(c^{-1}), s(c)s(p)) = (cpp^{-1}s(c^{-1}), s(c)p) = (cs(c^{-1}), s(c)p).$$

Ahora bien como $c \in \ker(s)$ entonces $s(c) = 1$ y $s(c^{-1}) = s(c)^{-1} = 1^{-1} = 1$ luego,

$$(cs(c^{-1}), s(c)p) = (c, p).$$

De este modo, se obtiene el resultado deseado y, por lo tanto, $\psi = \phi^{-1}$.

□

Los módulos cruzados y los Cat^1 -grupos son dos formalizaciones algebraicas que, aunque definidas de manera diferente, representan esencialmente la misma estructura, es decir, existe una equivalencia de categorías entre ellas. En lo que sigue, presentaremos de manera detallada la correspondencia categórica que establece la equivalencia entre los módulos cruzados y los Cat^1 -grupos.

Proposición 3.4. *Existe un funtor*

$$F: \text{XMod} \longrightarrow \text{Cat}^1$$

actuando como sigue en objetos y morfismos:

$$\begin{array}{ll} F: \text{Ob}(\text{XMod}) \rightarrow \text{Ob}(\text{Cat}^1) & F: \text{Mor}(\text{XMod}) \rightarrow \text{Mor}(\text{Cat}^1) \\ (M, N, \mu) \mapsto (M \rtimes N, N, i, s, t), & (f, g) \mapsto (f \times g, g), \end{array}$$

donde $i: N \rightarrow M \rtimes N$; $i(n) = (1, n)$, $s: M \rtimes N \rightarrow N$; $s(m, n) = n$ y $t: M \rtimes N \rightarrow N$; $t(m, n) = \mu(m)n$.

Demostración. Dado un módulo cruzado (M, N, μ) se comprobará que $(M \rtimes N, N, i, s, t)$ es un Cat^1 -grupo. Se procederá, por tanto, a la verificación de las propiedades (3.1) y (3.2).

- (i) Se tiene que: $s(i(n)) = s(1, n) = n = \text{id}_N$ y $t(i(n)) = t(1, n) = \mu(1)n = n = \text{id}_N$ con lo cual, (3.1) se cumple.

(ii) Se probará a continuación que $[\ker(s), \ker(t)] = \{1_{M \times N}\}$. Se tiene que $\ker(s) = \{(m, 1) \mid m \in M\}$ y $\ker(t) = \{(m, n) \mid \mu(m)n = 1\} = \{(m, n) \mid n = \mu(m)^{-1}\} = \{(m, \mu(m)^{-1}) \mid m \in M\}$. Entonces,

$$\begin{aligned} [\ker(s), \ker(t)] &= [(m_1, 1), (m_2, \mu(m_2)^{-1})] \\ &= (m_1, 1)(m_2, \mu(m_2)^{-1})(m_1, 1)^{-1}(m_2, \mu(m_2)^{-1})^{-1}. \end{aligned}$$

Ahora bien, tenemos que por (1.3), $(m_1, 1)^{-1} = (\varphi(1, m_1^{-1}), 1) = (m^{-1}, 1)$ y que $(m_2, \mu(m_2)^{-1})^{-1} = (\varphi(\mu(m_2), m_2^{-1}), \mu(m_2)) = (\mu(m_2)m_2^{-1}, \mu(m_2))$. Luego,

$$[\ker(s), \ker(t)] = (m_1, 1)(m_2, \mu(m_2)^{-1})(m_1^{-1}, 1)(\mu(m_2)m_2^{-1}, \mu(m_2)).$$

A continuación, se procederá a realizar las operaciones paso a paso empleando el producto semidirecto y teniendo en cuenta que $\varphi(n, m) = {}^n m$.

$$(m_1, 1)(m_2, \mu(m_2)^{-1}) = (m_1 m_2, \mu(m_2)^{-1}) = (m_1 m_2, \mu(m_2)^{-1}),$$

$$(m_1 m_2, \mu(m_2)^{-1})(m_1^{-1}, 1) = (m_1 m_2 \mu(m_2)^{-1} m_1^{-1}, \mu(m_2)^{-1}),$$

y por último

$$\begin{aligned} & (m_1 m_2 \mu(m_2)^{-1} m_1^{-1}, \mu(m_2)^{-1})(\mu(m_2)m_2^{-1}, \mu(m_2)) \\ &= (m_1 m_2 \mu(m_2)^{-1} m_1^{-1} \mu(m_2)^{-1} (\mu(m_2)m_2^{-1}), \mu(m_2)^{-1} \mu(m_2)). \end{aligned}$$

Ahora bien, teniendo en cuenta que por ser μ homomorfismo, $\mu(m_2)^{-1} m_1^{-1} = \mu(m_2^{-1}) m_1^{-1}$ y por la propiedad (2.2), $\mu(m_2^{-1}) m_1^{-1} = m_2^{-1} m_1^{-1} m_2$ se tiene que:

$$\begin{aligned} & (m_1 m_2 \mu(m_2)^{-1} m_1^{-1} \mu(m_2)^{-1} (\mu(m_2)m_2^{-1}), \mu(m_2)^{-1} \mu(m_2)) = \\ & (m_1 m_2 m_2^{-1} m_1^{-1} m_2 m_2^{-1}, 1) = (1, 1) = \{1_{M \times N}\}, \end{aligned}$$

de donde se concluye que $(M \times N, N, i, s, t)$ es un Cat^1 -grupo.

Por lo tanto, se ha demostrado que el funtor F está bien definido en objetos. Se verá que dicho funtor también está bien definido en morfismos. Dado el morfismo $(f, g): (M, N, \mu) \rightarrow (M', N', \mu')$ en \mathbf{XMod} , se verá que $(f \times g, g): (M \times N, N, i, s, t) \rightarrow (M' \times N', N', i', s', t')$ es un morfismo en Cat^1 .

En primer lugar, se debe comprobar que tanto $f \times g$ como g son homomorfismos de grupos. Nótese que g ya es homomorfismo de grupos debido a como están definidos los morfismos en \mathbf{XMod} . Se probará entonces que $f \times g$ también es homomorfismo de grupos,

es decir si $(f \times g)((m_1, n_1)(m_2, n_2)) = (f \times g)(m_1, n_1)(f \times g)(m_2, n_2)$. En efecto,

$$\begin{aligned} (f \times g)((m_1, n_1), (m_2, n_2)) &= (f \times g)(m_1^{n_1} m_2, n_1 n_2) \\ &= (f(m_1^{n_1} m_2), g(n_1 n_2)) \\ &= (f(m_1) f^{(n_1)} m_2, g(n_1) g(n_2)) \\ &\stackrel{(2.4)}{=} (f(m_1) g^{(n_1)} f(m_2), g(n_1) g(n_2)) \\ &= (f(m_1), g(n_1))(f(m_2), g(n_2)) = (f \times g)(m_1, n_1)(f \times g)(m_2, n_2). \end{aligned}$$

Se debe demostrar ahora que el par $(f \times g, g)$ verifica las propiedades (3.3), (3.4) y (3.5).

(i) Para comprobar (3.3), se debe verificar si $g \circ s = s' \circ (f \times g)$. Por un lado,

$$(g \circ s)(m, n) = g(s(m, n)) = g(n),$$

y por otro lado,

$$(s' \circ (f \times g))(m, n) = s'(f(m), g(n)) = g(n),$$

con lo que se obtiene la igualdad.

(ii) En el caso de (3.4) se debe comprobar si $g \circ t = t' \circ (f \times g)$. Por un lado,

$$(g \circ t)(m, n) = g(t(m, n)) = g(\mu(m)n) = g(\mu(m))g(n),$$

y por otro lado,

$$(t' \circ (f \times g))(m, n) = t'(f(m), g(n)) = \mu'(f(m))g(n),$$

teniendo en cuenta que $(f, g): (M, N, \mu) \rightarrow (M', N', \mu')$ es un morfismo de módulos cruzados se tiene por la propiedad (2.3) que $\mu' \circ f = g \circ \mu$, luego $g(\mu(m)) = \mu'(f(m))$, concluyendo así la prueba de la igualdad (3.4).

(iii) Para la propiedad (3.5) se debe probar que $(f \times g) \circ i = i' \circ g$. En efecto,

$$((f \times g) \circ i)(n) = (f \times g)(i(n)) = (f \times g)(1, n) = (f(1), g(n)),$$

$$(i' \circ g)(n) = i'(g(n)) = (1, g(n)),$$

y, como f es un homomorfismo de grupos, $f(1) = 1$, luego se obtiene la igualdad.

Se ha probado que, dado el morfismo (f, g) en \mathbf{XMod} , el morfismo $(f \times g, g)$ es de \mathbf{Cat}^1 -grupos, concluyendo así la demostración. \square

Por otro lado se construirá ahora un funtor en el otro sentido, de la categoría de Cat^1 -grupos en la categoría de módulos cruzados.

Proposición 3.5. *Existe un funtor*

$$G: \text{Cat}^1 \longrightarrow \text{XMod}$$

actuando como sigue en objetos y morfismos:

$$\begin{aligned} G: \text{Ob}(\text{Cat}^1) &\rightarrow \text{Ob}(\text{XMod}) & G: \text{Mor}(\text{Cat}^1) &\rightarrow \text{Mor}(\text{XMod}) \\ (G, P, i, s, t) &\mapsto (\ker(s), P, t|_{\ker(s)}), & (x, y) &\mapsto (x|_{\ker(s)}, y), \end{aligned}$$

donde la acción de P sobre $\ker(s)$ se define por ${}^p a := {}^{i(p)} a = i(p)ai(p)^{-1}$, para todo $a \in \ker(s)$ y para todo $p \in P$.

Demostración. Dado un Cat^1 -grupo (G, P, i, s, t) se comprobará que la terna $(\ker(s), P, t|_{\ker(s)})$ es un módulo cruzado, donde P actúa sobre $\ker(s)$ a través de la acción ${}^p a := i(p)ai(p)^{-1}$, i.e., por conjugación.

Que la aplicación $t|_{\ker(s)}$ es un homomorfismo de grupos es obvio puesto que se trata de la restricción de un homomorfismo de grupos, t , a un subgrupo del dominio, $\ker(s) < G$.

Se probará a continuación que se verifican las dos propiedades de módulo cruzado.

(i) En primer lugar, se debe comprobar si $t({}^p a) = pt(a)p^{-1}$. En efecto:

$$t({}^p a) = t(i(p)ai(p)^{-1}) \stackrel{(a)}{=} t(i(p))t(a)t(i(p)^{-1}) \stackrel{(3.1)}{=} pt(a)p^{-1}, \text{ para todo } p \in P, a \in \ker(s).$$

En (a) se emplea que t es un homomorfismo de grupos. Por tanto, la igualdad (2.1) se verifica.

(ii) Se comprobará ahora la propiedad (2.2), es decir, ${}^{t(a)} b = aba^{-1}$.

Sean $a, b \in \ker(s)$. Por un lado, por la propiedad 3.1, $t \circ i = \text{id}_P$ y por otro lado se tiene que $i(t(a^{-1}))a \in \ker(t)$, ya que $t(i(t(a^{-1}))a) \stackrel{t \text{ hom.}}{=} t(i(t(a^{-1})))t(a) = t(a^{-1})t(a) = 1$.

Por la propiedad (3.2), $[\ker(s), \ker(t)] = \{1_G\}$, entonces se tiene que:

$$bi(t(a^{-1}))a = i(t(a^{-1}))ab,$$

y por lo tanto

$${}^{t(a)} ba = i(t(a))bi(t(a^{-1}))a = i(t(a))i(t(a^{-1}))ab = ab.$$

Así, tenemos

$${}^{t(a)} b = aba^{-1}, \text{ para todo } a, b \in \ker(s).$$

Se concluye que la propiedad (2.2) también se cumple y por tanto, queda demostrado que $(\ker(s), P, t|_{\ker(s)})$ es un módulo cruzado.

Se ha demostrado que el funtor está bien definido en objetos. Se verá que también está bien definido en morfismos. Dado el morfismo $(x, y): (G, P, i, s, t) \rightarrow (G', P', i', s', t')$ en Cat^1 , se verá que $(x|_{\ker(s)}, y): (\ker(s), P, t|_{\ker(s)}) \rightarrow (\ker(s'), P', t'|_{\ker(s)})$ es un morfismo en XMod .

En primer lugar, se debe comprobar que tanto $x|_{\ker(s)}$ como y son homomorfismos de grupos. Por definición, y es un homomorfismo de grupos. Como $\ker(s)$ es un subgrupo de G y x es un homomorfismo de grupos, se tiene que $x|_{\ker(s)}$ es claramente un homomorfismo de grupos.

A continuación se probará que $\text{Im}(x|_{\ker(s)}) \subseteq \ker(s')$. Sea $a \in \ker(s)$, se tiene que:

$$s'(x(a)) \stackrel{(3.3)}{=} y(s(a)) \stackrel{(a)}{=} y(1) \stackrel{(b)}{=} 1 \implies x(a) \in \ker(s').$$

En (a) se ha empleado el hecho de que $a \in \ker(s)$ y en (b) que y es un homomorfismo de grupos.

Ahora se debe comprobar si se verifican las propiedades de morfismo de módulos cruzados de grupos, las igualdades (2.3) y (2.4).

- (i) Para ver que se verifica (2.3), se debe comprobar si $t'|_{\ker(s')} \circ x|_{\ker(s)} = y \circ t|_{\ker(s)}$. Por un lado,

$$t'|_{\ker(s')} \circ x|_{\ker(s)}(a) = t'|_{\ker(s')}(x|_{\ker(s)}(a))$$

por otro,

$$y \circ t|_{\ker(s)}(a) = y(t|_{\ker(s)}(a)).$$

Como $(x, y): (G, P, i, s, t) \rightarrow (G', P', i', s', t')$ es un morfismo de Cat^1 -grupos, se verifica la propiedad (3.4) donde $y \circ t = t' \circ x$ y teniendo en cuenta que $\ker(s)$ es un subgrupo de G se llega al resultado.

- (ii) Se debe comprobar a continuación la verificación de la propiedad (2.4), es decir si $x|_{\ker(s)}(pa) = y^{(p)}x|_{\ker(s)}(a)$. Por un lado,

$$x|_{\ker(s)}(pa) = x|_{\ker(s)}(i(p)ai(p)^{-1}) \stackrel{(x \text{ hom. de grupos})}{=} x|_{\ker(s)}(i(p))x|_{\ker(s)}(a)x|_{\ker(s)}(i(p))^{-1},$$

y por otro lado,

$$y^{(p)}x|_{\ker(s)}(a) = i'(y(p))x|_{\ker(s)}(a)i'(y(p))^{-1},$$

ahora como $(x, y): (G, P, i, s, t) \rightarrow (G', P', i', s', t')$ es un morfismo de Cat^1 -grupos, se cumple la propiedad (3.5), es decir que $x \circ i = i' \circ y$ lo cual permite obtener el resultado deseado.

□

Teorema 3.6. *Los funtores F y G inducen una equivalencia entre las categorías \mathbf{XMod} y Cat^1 .*

Demostración. Sean los funtores

$$G: \text{Cat}^1 \rightarrow \mathbf{XMod}, \quad (G, P, i, s, t) \rightarrow (\ker(s), P, t|_{\ker(s)})$$

y

$$F: \mathbf{XMod} \rightarrow \text{Cat}^1, \quad (M, N, \mu) \rightarrow (M \rtimes N, N, i, s, t)$$

donde $i: N \rightarrow M \rtimes N$ con $i(n) = (1, n)$, $s: M \rtimes N \rightarrow N$ con $s(m, n) = n$, y $t: M \rtimes N \rightarrow N$ con $t(m, n) = \mu(m)n$.

Se comienza calculando la composición $G \circ F$. Para un objeto $(M, N, \mu) \in \mathbf{XMod}$, se tiene:

$$(G \circ F)(M, N, \mu) = G(M \rtimes N, N, i, s, t) = (\ker(s), N, t|_{\ker(s)}),$$

donde el núcleo de s viene dado por:

$$\begin{aligned} \ker(s) &= \{(m, n) \in M \rtimes N \mid s(m, n) = 1_N\} = \{(m, n) \in M \rtimes N \mid n = 1_N\} \\ &= \{(m, 1_N) \mid m \in M\} = M \times \{1_N\} \cong M. \end{aligned}$$

Además, la restricción de t a $\ker(s)$ satisface:

$$t|_{\ker(s)}(m, 1_N) = \mu(m)1_N = \mu(m).$$

Por tanto, se concluye que

$$G \circ F = \text{id}_{\mathbf{XMod}}.$$

Se considera ahora la otra composición, $F \circ G$. Dado un objeto $(G, P, i, s, t) \in \text{Cat}^1$, se tiene:

$$(F \circ G)(G, P, i, s, t) = F(\ker(s), P, t|_{\ker(s)}) = (\ker(s) \rtimes P, P, i', s', t').$$

En virtud del isomorfismo establecido en el Lema 3.3, se dispone de una aplicación

$$\phi: G \rightarrow \ker(s) \rtimes P, \quad \phi(g) = (gi(s(g^{-1})), s(g)),$$

la cual induce el morfismo de Cat^1 -grupos $(\phi, \text{id}_P): (G, P, i, s, t) \rightarrow (\ker(s) \rtimes P, P, i', s', t')$.

Para concluir que (ϕ, id_P) es un morfismo de Cat^1 -grupos se debe comprobar que se verifican las propiedades correspondientes (3.3), (3.4) y (3.5).

- (i) Se debe comprobar que $\text{id}_P \circ s = s' \circ \phi$, donde $s': \ker(s) \rtimes P \rightarrow P$ está definida por $s'(a, p) = p$. En efecto,

$$(\text{id}_P \circ s)(g) = \text{id}_P(s(g)) = s(g),$$

$$(s' \circ \phi)(g) = s'(\phi(g)) = s'((gi(s(g^{-1})), s(g))) = s(g),$$

por lo que ambas expresiones coinciden.

- (ii) Para demostrar la propiedad (3.4), se debe comprobar que $\text{id}_P \circ t = t' \circ \phi$, donde $t': \ker(s) \times P \rightarrow P$ está dada por $t'(a, p) = t|_{\ker(s)}(a)p$. Por un lado,

$$(\text{id}_P \circ t)(g) = \text{id}_P(t(g)) = t(g)$$

y por otro lado,

$$\begin{aligned} (t' \circ \phi)(g) &= t'(\phi(g)) = t'(gi(s(g^{-1})), s(g)) \\ &= t|_{\ker(s)}(gi(s(g^{-1})))s(g) \stackrel{(a)}{=} t(gi(s(g^{-1})))s(g) \\ &\stackrel{(b)}{=} t(g)t(i(s(g^{-1})))s(g) \stackrel{(c)}{=} t(g)s(g^{-1})s(g) = t(g), \end{aligned}$$

donde en (a) se ha empleado que $gis(g^{-1}) \in \ker(s)$. Esto se tiene ya que, por un lado, s es un homomorfismo de grupos y por otro, al tratarse de un Cat^1 -grupo se verifica la propiedad (3.1), es decir, $s \circ i = \text{id}_P$. De lo anterior, se obtiene que $s(gi(s(g^{-1}))) = s(g)s(g^{-1}) = 1$ y por tanto $gis(g^{-1}) \in \ker(s)$.

En (b) se usa que t es un homomorfismo de grupos y en (c) la propiedad (3.1) es decir que $t \circ i = \text{id}_P$ por tanto $t(i(s(g^{-1}))) = \text{id}(s(g^{-1})) = s(g^{-1})$.

- (iii) Por último, se debe comprobar que $\phi \circ i = i' \circ \text{id}_P$, donde $i': P \rightarrow \ker(s) \times P$ está dada por $i'(p) = (1, p)$. En efecto,

$$(\phi \circ i)(p) = \phi(i(p)) = (i(p)i(s(i(p)^{-1})), s(i(p)))$$

empleando que i es un homomorfismo de grupos y que se cumple la propiedad (3.1) es decir que, $s \circ i = \text{id}_P$, se tiene que:

$$(i(p)i(s(i(p)^{-1})), s(i(p))) = (i(p)i(p^{-1}), p) = (1, p).$$

Por último,

$$i' \circ \text{id}_P(p) = i'(p) = (1, p).$$

Es decir, se llega a que efectivamente (ϕ, id_P) es un isomorfismo de Cat^1 -grupos y por tanto se concluye la demostración. \square

3.2. 2-grupos estrictos y módulos cruzados

Definición 3.7. Dada una categoría \mathcal{C} con pullbacks, se dice que la tupla de objetos y morfismos en \mathcal{C} , $\mathcal{G} = (G_0, G_1, s, t, i, \circ)$ es una **categoría interna** en \mathcal{C} si los diagramas en (1.4) y (1.5) conmutan.

Definición 3.8. Un **functor interno** en \mathcal{C} entre dos categorías internas \mathcal{G} y \mathcal{G}' consiste en un par de morfismos en \mathcal{C} , $(F_0: G_0 \rightarrow G'_0, F_1: G_1 \rightarrow G'_1)$, tal los diagramas (1.7) conmutan.

Definición 3.9. Un **2-grupo estricto** es una categoría interna en la categoría de grupos.

Ejemplo 3.10. Todo grupo (G, \cdot) da lugar a un 2-grupo estricto dado por la tupla $(G, G, \text{id}_G, \text{id}_G, \text{id}_G, \cdot)$.

Ejemplo 3.11. Para un grupo dado G , se puede construir un 2-grupo cuya estructura es la siguiente:

$$G_0 = \text{Aut}(G), \quad G_1 = G \rtimes \text{Aut}(G), \quad s(g, F) = F$$

$$t(g, F) = \text{conj}_g \circ F, \quad i(g) = (1, g),$$

donde $\text{conj}_g(h) = ghg^{-1}$ y $(g', F') \circ (g, F) = (g'g, F)$. Esta estructura se conoce como el 2-grupo de automorfismos de G .

Definición 3.12. Un **morfismo de 2-grupos estrictos** es un functor interno en la categoría de grupos.

Con los elementos anteriores, 2-grupos estrictos constituye una categoría que se denotará por 2-Grp.

Proposición 3.13. *Existe un functor*

$$T: \text{XMod} \longrightarrow 2\text{-Grp}$$

actuando como sigue en objetos y morfismos:

$$T: \text{Ob}(\text{XMod}) \rightarrow \text{Ob}(2\text{-Grp}) \qquad T: \text{Mor}(\text{XMod}) \rightarrow \text{Mor}(2\text{-Grp})$$

$$(M, N, \mu) \mapsto (N, M \rtimes N, s, t, i, \circ), \qquad (f, g) \mapsto (g, f \times g),$$

donde $s: M \rtimes N \rightarrow N$ tal que $s(m, n) = n$, $t: M \rtimes N \rightarrow N$ con $t(m, n) = \mu(m)n$ e $i: N \rightarrow M \rtimes N$ tal que $i(n) = (1, n)$. Además, la composición se define como $(m', n') \circ (m, n) = (m'm, n)$.

Demostración. La demostración de este resultado es análoga a la demostración de la Proposición 3.4 puesto que las construcciones son idénticas. \square

Observación 3.14. En el contexto anterior, la composición \circ definida en $M \rtimes N$ por $(m', n') \circ (m, n) = (m'm, n)$ está bien definida si y sólo si se cumple que el *target* del primer morfismo coincide con la *source* del segundo, es decir, $t(m, n) = s(m', n')$, luego la composición solo es posible si $\mu(m)n = n'$. Suponiendo que dicha condición se cumple, se verificará que la composición respeta las funciones *source* y *target*.

- (i) $s(m'm, n) = n = s(m, n)$.
- (ii) $t(m'm, n) = \mu(m'm)n \stackrel{(a)}{=} \mu(m')\mu(m)n \stackrel{(b)}{=} \mu(m')n' = t(m', n')$, donde en (a) se usa que μ es un homomorfismo de grupos y en (b) que $\mu(m)n = n'$.

Proposición 3.15. *Existe un funtor*

$$S: 2\text{-Grp} \longrightarrow \mathbf{XMod}$$

actuando como sigue en objetos y morfismos:

$$\begin{aligned} S: \text{Ob}(2\text{-Grp}) &\rightarrow \text{Ob}(\mathbf{XMod}) & S: \text{Mor}(2\text{-Grp}) &\rightarrow \text{Mor}(\mathbf{XMod}) \\ (G_0, G_1, s, t, i, \circ) &\mapsto (\ker(s), G_0, t|_{\ker(s)}), & (x, y) &\mapsto (y|_{\ker(s)}, x), \end{aligned}$$

donde la acción de G_0 sobre $\ker(s)$ se define por ${}^g a := i(g)ai(g)^{-1}$, para todo $a \in \ker(s)$ y para todo $g \in G_0$.

Demostración. La demostración de este resultado es análoga a la demostración de la Proposición 3.5 puesto que las construcciones son idénticas. \square

Teorema 3.16. *Los funtores S y T inducen una equivalencia entre las categorías \mathbf{XMod} y 2-Grp .*

Demostración. Sean los funtores S y T construidos en las proposiciones anteriores (3.13 y 3.15):

$$S: 2\text{-Grp} \rightarrow \mathbf{XMod}, \quad (G_0, G_1, s, t, i, \circ) \rightarrow (\ker(s), G_0, t|_{\ker(s)}),$$

$$T: \mathbf{XMod} \rightarrow 2\text{-Grp}, \quad (M, N, \mu) \rightarrow (N, M \rtimes N, s, t, i),$$

donde $i: N \rightarrow M \rtimes N$ con $i(n) = (1, n)$, $s: M \rtimes N \rightarrow N$ con $s(m, n) = n$ y $t: M \rtimes N \rightarrow N$ con $t(m, n) = \mu(m)n$.

Se comienza considerando la composición $S \circ T$. Para un objeto $(M, N, \mu) \in \mathbf{XMod}$, se tiene:

$$(S \circ T)(M, N, \mu) = S(N, M \rtimes N, s, t, i) = (\ker(s), N, t|_{\ker}).$$

Dado que $s(m, n) = n$, el núcleo de s viene dado por:

$$\begin{aligned} \ker(s) &= \{(m, n) \in M \rtimes N \mid s(m, n) = 1_N\} = \{(m, n) \in M \rtimes N \mid n = 1_N\} \\ &= \{(m, 1_N) \mid m \in M\} = M \times \{1_N\} \cong M. \end{aligned}$$

Además, la restricción de t a $\ker(s)$ satisface:

$$t|_{\ker(s)}(m, 1_N) = \mu(m)1_N = \mu(m).$$

Por tanto, se concluye que

$$S \circ T = \text{id}_{\mathcal{X}\text{Mod}}.$$

Se considera ahora la otra composición $T \circ S$. Dado un objeto $(G_0, G_1, s, t, i, \circ) \in 2\text{-Grp}$, se tiene:

$$(T \circ S)(G_0, G_1, s, t, i, \circ) = T(\ker(s), G_0, t|_{\ker(s)}) = (G_0, \ker(s) \rtimes G_0, s', t', i').$$

Este objeto no coincide estrictamente con el objeto original, pero se puede construir un isomorfismo natural:

$$(\text{id}_{G_0}, \phi^{-1}),$$

donde ϕ está definida por:

$$\phi: G_1 \rightarrow \ker(s) \rtimes G_0, \quad \phi(a) = (ai(s(a))^{-1}, s(a)),$$

es un isomorfismo de grupos. En efecto,

- (i) Es homomorfismo de grupos. Para ello se debe comprobar que $\phi(ab) = \phi(a)\phi(b)$ para todo $a, b \in G_1$,

$$\phi(ab) = (abi(s(ab))^{-1}, s(ab))$$

pero como s es homomorfismo de grupos $s(ab) = s(a)s(b)$, luego

$$\phi(ab) = (abi(s(a)s(b))^{-1}, s(a)s(b)).$$

Ahora bien, aplicando el producto semidirecto:

$$\begin{aligned} \phi(a)\phi(b) &= (ai(s(a))^{-1}, s(a))(bi(s(b))^{-1}, s(b)) \\ &= (ai((s(a))^{-1})^{s(a)}(bi(s(b))^{-1}), s(a)s(b)) \end{aligned}$$

donde

$${}^{s(a)}(bi(s(b))^{-1}) = i(s(a))(bi(s(b))^{-1})i(s(a))^{-1},$$

entonces

$$\begin{aligned} \phi(a)\phi(b) &= (ai((s(a))^{-1})i(s(a))(bi(s(b))^{-1})i(s(a))^{-1}, s(a)s(b)) \\ &= (abi(s(b))^{-1}i(s(a))^{-1}, s(a)s(b)), \end{aligned}$$

por ser i un homomorfismo entonces $i(s(b))^{-1}i(s(a))^{-1} = i(s(a)s(b))^{-1}$ y por tanto se obtiene el resultado.

(ii) Es biyectiva.

Sea $\phi : G_1 \rightarrow \ker(s) \rtimes G_0$ definida como $\phi(a) = (ai(s(a))^{-1}, s(a))$ se debe comprobar que

$$\phi^{-1}(h, g) = hi(g)$$

es su inversa. En efecto,

$$\phi(\phi^{-1}(h, g)) = \phi(hi(g)) = (hi(g)i(s(hi(g)))^{-1}, s(hi(g)))$$

como $s(h) = 1$ pues $h \in \ker(s)$ y $s(i(g)) = g$, se tiene que:

$$\phi(hi(g)) = (hi(g)i(g)^{-1}, g) = (h, g).$$

$$\phi^{-1}(\phi(a)) = \phi^{-1}((ai(s(a))^{-1}, s(a))) = ai(s(a))^{-1}i(s(a)) = a.$$

Luego, ϕ es un isomorfismo.

A continuación, se comprobará que $(\text{id}_{G_0}, \phi^{-1})$ es un morfismo en 2-Grp. En efecto,

(i) **Compatibilidad con el morfismo *source*:**

Se tiene que $s : G_1 \rightarrow G_0$ y se quiere comprobar que $s(hi(g)) = g$.

Dado que $h \in \ker(s)$, entonces $s(h) = 1$, y además $s(i(g)) = g$. Así que,

$$s(hi(g)) = s(h)s(i(g)) = g.$$

(ii) **Compatibilidad con el morfismo *target*:**

Se tiene que $t : G_1 \rightarrow G_0$ y se quiere comprobar que $t(hi(g)) = t(h)g$.

Como t es un homomorfismo de grupos y $t(i(g)) = g$, se tiene que:

$$t(hi(g)) = t(h)t(i(g)) = t(h)g.$$

(iii) **Compatibilidad con el morfismo *identity*:**

Se tiene que $i : G_0 \rightarrow G_1$ y se quiere ver que $\phi(i(g)) = (1, g)$.

$$\phi(i(g)) = \phi(i(g)i(s(i(g)))^{-1}, s(i(g))) = \phi(i(g)i(g)^{-1}, g) = (1, g).$$

Por tanto, $(\text{id}_{G_0}, \phi^{-1})$ es un isomorfismo en 2-Grp lo que concluye la prueba del teorema. □

3.3. Grupos categóricos estrictos y módulos cruzados

La noción de categoría es una categorificación de la noción de conjunto. De igual manera, la noción de categoría monoidal es una categorificación de la noción de monoide. Se recuerda que un monoide es una estructura más débil que la de un grupo ya que la existencia de un inverso no es requerida. Un monoide M es un conjunto con una operación de multiplicación $(x, y) \rightarrow x \cdot y$, asociativa $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ con un elemento 1 tal que $1 \cdot 1 = 1$ y las aplicaciones $1 \cdot, \cdot 1: M \rightarrow M$ son biyecciones. Es fácil probar que la última condición es equivalente al axioma unitario habitual $1 \cdot x = x \cdot 1 = x$. Véase [1].

Ejemplo 3.17.

- (i) Los números naturales $\mathbb{N} - \{0\}$ con el producto y el 1 es un monoide.
- (ii) Los números naturales \mathbb{N} con la suma y el 0 es un monoide.

Como es habitual en teoría de categorías, para categorificar la definición de un monoide, se deberán substituir las igualdades en la definición de un monoide (la asociatividad $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ y la ecuación $1 \cdot 1 = 1$) por isomorfismos que satisfagan algunas propiedades de consistencia, y la palabra “biyección” por la palabra “equivalencia” (de categorías). Esto nos conduce a la siguiente definición.

Definición 3.18. Una **categoría monoidal (o tensorial)** es una 6-tupla $\mathcal{C} = (\mathcal{C}, \otimes, a, I, l, r)$ donde \mathcal{C} es una categoría, $\otimes: \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$ es un functor, $a_{X,Y,Z}: (X \otimes Y) \otimes Z \rightarrow X \otimes (Y \otimes Z)$ es un isomorfismo natural llamado el asociator, que satisface un diagrama de coherencia asociativo (axioma del pentágono):

$$\begin{array}{ccc}
 & ((X \otimes Y) \otimes Z) \otimes W & \\
 & \swarrow^{a_{X,Y,Z} \otimes \text{id}_W} \quad \searrow^{a_{X \otimes Y, Z, W}} & \\
 (X \otimes (Y \otimes Z)) \otimes W & & (X \otimes Y) \otimes (Z \otimes W) \\
 & \swarrow^{a_{X, Y \otimes Z, W}} \quad \searrow^{a_{X, Y, Z \otimes W}} & \\
 X \otimes ((Y \otimes Z) \otimes W) & \xrightarrow{\text{id}_X \otimes a_{Y, Z, W}} & X \otimes (Y \otimes (Z \otimes W))
 \end{array}$$

$I \in \text{Ob}(\mathcal{C})$ (objeto unidad), y $l: I \otimes X \rightarrow X$, $r: X \otimes I \rightarrow X$ son isomorfismos naturales (llamadas las unidades izquierda y derecha, respectivamente), que también satisfacen para todo $X, Y \in \text{Ob}(\mathcal{C})$ los diagramas de coherencia de la unidad (ecuación del triángulo).

$$\begin{array}{ccc}
 (X \otimes I) \otimes Y & \xrightarrow{a_{X,I,Y}} & X \otimes (I \otimes Y) \\
 \searrow r_X \otimes \text{id}_Y & & \swarrow \text{id}_X \otimes l_Y \\
 & X \otimes Y &
 \end{array}$$

Una categoría monoidal es llamada **estricta** si los isomorfismos a , l y r son los morfismos identidad. En este caso tenemos que $(X \otimes Y) \otimes Z = X \otimes (Y \otimes Z)$, $X \otimes I = X = I \otimes X$.

Ejemplo 3.19.

- (i) Sea la categoría $\mathcal{C} = \mathbf{Set}$ de conjuntos. Para cualesquiera dos objetos X, Y en \mathbf{Set} , el producto tensor $X \otimes Y := X \times Y$, es el producto cartesiano.

El isomorfismo $a_{X,Y,Z}$ es la biyección $(X \times Y) \times Z \rightarrow X \times (Y \times Z)$, $((x, y), z) \mapsto (x, (y, z))$, el objeto unidad es $I = \{*\}$ el conjunto con un elemento, que es único salvo una biyección. La unidad izquierda $l: I \times X \rightarrow X$ es la biyección $(*, x) \mapsto x$ y la unidad derecha $r: X \times I \rightarrow X$ es la biyección $(x, *) \mapsto x$.

Así, $(\mathbf{Set}, \times, a, \{*\}, l, r)$ es una categoría monoidal.

- (ii) Sea la categoría $\mathcal{C} = \mathbf{Vect}_K$ de espacios vectoriales. Para cualesquiera dos espacios vectoriales V, W en \mathbf{Vect}_K , el producto tensor $V \otimes W := V \otimes_K W$, es el producto tensor de espacios vectoriales.

El isomorfismo $a_{V,W,Z}$ es $(V \otimes W) \otimes Z \rightarrow V \otimes (W \otimes Z)$, $(v \otimes w) \otimes z \mapsto v \otimes (w \otimes z)$, el objeto unidad es $I = K$ el cuerpo. La unidad izquierda $l: K \otimes V \rightarrow V$ es el isomorfismo $\lambda \otimes v \mapsto \lambda v$ y la unidad derecha $r: V \otimes K \rightarrow V$ es el isomorfismo $v \otimes \lambda \mapsto \lambda v$.

Así, $(\mathbf{Vect}_K, \otimes, a, K, l, r)$ es una categoría monoidal.

Definición 3.20. Un **grupo categórico** \mathcal{C} es una categoría monoidal en la que todo morfismo es invertible y, para cada objeto X existe un objeto X^* con un isomorfismo $\varepsilon_X: X \otimes X^* \rightarrow I$, i.e. todo objeto tiene inverso.

Un grupo categórico es **estricto** cuando es estricto como una categoría monoidal, y ε_X puede ser elegido como la identidad, i.e. los isomorfismos naturales son identidades.

Grupos categóricos estrictos son grupos internos en la categoría de categorías pequeñas (categorías donde los objetos forman un conjunto).

Así, en un grupo categórico estricto \mathcal{C} , tenemos las igualdades:

$$\begin{aligned}
 (g_1 \otimes g_2) \otimes g_3 &= g_1 \otimes (g_2 \otimes g_3), \\
 I \otimes g &= g = g \otimes I,
 \end{aligned}$$

y para todo objeto g existe un objeto g^* tal que $g \otimes g^* = I = g^* \otimes g$.

Un morfismo entre dos grupos categóricos estrictos $F: \mathcal{C} \rightarrow \mathcal{C}'$ es un funtor monoidal $F = (F, F_2, F_I): \mathcal{C} \rightarrow \mathcal{C}'$ con

$$F_2^{X,Y}: FX \otimes FY \rightarrow F(X \otimes Y), \quad F_I: I \rightarrow FI,$$

entre las categorías monoidales \mathcal{C} y \mathcal{C}' . Así, tenemos la categoría de grupos categóricos estrictos, que denotaremos \mathbf{Gcs} .

Teorema 3.21 (Brown-Spencer [2]). *Existe una equivalencia de categorías entre grupos categóricos estrictos y módulos cruzados.*

La prueba del teorema puede verse en [2] y con más detalle en [13]. Aquí, solo daremos la construcción de los funtores:

$$T: \mathbf{Gcs} \longrightarrow \mathbf{XMod}, \quad S: \mathbf{XMod} \longrightarrow \mathbf{Gcs}$$

que proporcionan la equivalencia de categorías.

- Construcción del funtor T .

Sea \mathcal{C} un grupo categórico estricto. Construimos el módulo cruzado (M, G, μ) , con φ la acción de G sobre M de la siguiente manera:

- Sea G el conjunto de objetos de \mathcal{C} , con estructura de grupo por el producto tensor.
- Sea M el conjunto de morfismos $X \xrightarrow{f} I$, de objetos arbitrarios de $X \in \mathcal{C}$ en el objeto unidad $I \in \mathcal{C}$, μ es la función *source* $f \mapsto X$, con estructura de grupo por el producto tensor,

$$(X \xrightarrow{f} I) \cdot (Y \xrightarrow{g} I) := X \otimes Y \xrightarrow{f \otimes g} I \otimes I = I.$$

- Sea $\mu: M \rightarrow G$ la aplicación que lleva cualquier morfismo $f: X \rightarrow I$ a su *source* $X \in G$, i.e. $\mu(f) = X$.
- $\varphi^{(X)} f = \text{id}_X \otimes f \otimes \text{id}_{X^{-1}}$.

- Construcción del funtor S .

Sea el módulo cruzado (M, G, μ) , con φ la acción de G sobre M .

- \mathcal{C} es la categoría cuyos objetos son los elementos de G .
- El producto tensor de dos objetos de \mathcal{C} es la multiplicación en G .

- Un morfismo $g \xrightarrow{m} g'$ es un elemento $m \in M$ con $g = \mu(m)g'$, la composición es la multiplicación en M , el tensor producto tensor está dado por:

$$g \otimes g' := gg' \quad \text{y} \quad (g_1 \xrightarrow{m_1} g'_1) \otimes (g_2 \xrightarrow{m_2} g'_2) := g_1 g_2 \xrightarrow{m_1 g'_1 m_2} g'_1 g'_2,$$

Otra manera de ver los morfismos y su composición es la siguiente:

- El conjunto de morfismos de \mathcal{C} es el producto semidirecto $M \rtimes G$, con la multiplicación dada por:

$$(m, g) \otimes (m', g') := (m, g)(m', g') = (m {}^g m', gg').$$

El producto tensor de morfismos es la multiplicación en el producto semidirecto.

- Consideramos el par (m, g) como un morfismo $\mu(m)g \xrightarrow{(m, g)} g$, $g, \mu(m)g \in \mathcal{C}$, y definimos la composición de morfismos:

$$\left(\mu(m)g \xrightarrow{(m, g)} g \right) \circ \left(\mu(m')g' \xrightarrow{(m', g')} g' \right) := \mu(m)g \xrightarrow{(mm', g')} g'.$$

Bibliografía

- [1] J. C. Baez, *Hoàng Xuân Sính's thesis: categorifying group theory*, Thang Long J. Sci. Math. Math. Sci. **2**(8) (2023) 1–35.
- [2] R. Brown, C. B. Spencer, *G-groupoids, crossed modules and the fundamental groupoid of a topological group*, Indag. Math. **38**(4) (1976) 296–302.
- [3] R. Fernández Casado, *Relations between crossed modules of different algebras*, 2015. <http://hdl.handle.net/10347/13839>
- [4] A. Fernández-Fariña, *Braided Crossed Modules and Loday-Pirashvili category*, 2021. <http://hdl.handle.net/10347/26581>
- [5] M. Forrester-Barker, *Group Objects and Internal Categories*, 2002, arXiv:0212065. <https://arxiv.org/pdf/math/0212065>
- [6] M. Forrester-Barker, *Representations of Crossed Modules and Cat^1 -Groups*, 2003. https://pure.bangor.ac.uk/ws/portalfiles/portal/60895782/M_FORRESTER_BARKER_PhD_2004_OCR.pdf
- [7] R. Lal, *Algebra 1—groups, rings, fields and arithmetic*, Infosys Science Foundation Series Infosys Science Foundation Series in Mathematical Sciences, Springer, Singapore, 2017.
- [8] R. Lal, *Algebra 2—linear algebra, Galois theory, representation theory, group extensions and Schur multiplier*, Infosys Science Foundation Series Infosys Science Foundation Series in Mathematical Sciences, Springer, Singapore, 2017.
- [9] J.-L. Loday, *Spaces with finitely many nontrivial homotopy groups*, J. Pure Appl. Algebra **24**(2) (1982) 179–202.
- [10] S. Mac Lane, J. H. C. Whitehead, *On the 3-type of a complex*, Proc. Nat. Acad. Sci. U.S.A. **36** (1950) 41–48.

- [11] S-S. Porst, *Strict 2-Groups are Crossed Modules*, 2008, arXiv:0812.1464. <https://arxiv.org/pdf/0812.1464>
- [12] E. Riehl, *Category theory in context*, Aurora Dover Modern Math Originals, Dover, Mineola, NY, 2016.
- [13] S. Thomas, *(Co)homology of Crossed Modules*, 2017. https://pnp.mathematik.uni-stuttgart.de/lexmath/kuenzer/diploma_thomas.pdf
- [14] F. Wagemann, *Crossed Modules*, De Gruyter Studies in Mathematics 82, De Gruyter, Berlin, 2021.
- [15] J. H. C. Whitehead, *On adding relations to homotopy groups*, Ann. of Math. **42**(2) (1941) 409–428.
- [16] J. H. C. Whitehead, *Combinatorial homotopy II*, Bull. Am. Math. Soc. **55** (1949) 453–496.