Cohomología de Galois y el Problema de Inmersión

Germán Naranjo Sierra

Cohomología de Galois y el Problema de Inmersión

Germán Naranjo Sierra

Memoria presentada como parte de los requisitos para la obtención del título de Máster en Matemáticas por la Universidad de Sevilla.

Tutorizada por

Prof. Sara Arias de Reyna Domínguez

Índice general

English Abstract **1**

Introducción **3**

1. Cohomología de grupos **7**

1.1. G-módulos y H^0 7

1.2. El producto semidirecto y H^1 8

1.3. Extensiones de grupos y H^2 11

1.4. Aplicaciones entre grupos 21

1.4.1. Cambio de coeficientes 21

1.4.2. Cambio de grupo 22

1.4.3. La sucesión exacta larga 25

2. El problema de inmersión **29**

2.1. Planteamiento del problema 29

2.2. Problemas de tipo Brauer 30

2.3. Ejemplos 39

2.3.1. Grupos cíclicos 39

2.3.2. El grupo diedral D_4 42

2.3.3. El grupo de Heisenberg módulo p 45

3. El grupo de Brauer **47**

3.1. Álgebras centrales simples 47

3.1.1. Producto tensorial de álgebras 51

3.1.2. Cuerpos de descomposición 52

3.2. El grupo de Brauer 52

3.2.1. Productos cruzados y conexión con cohomología 53

3.3. Álgebras cíclicas 58

3.4. El problema de inmersión 60

3.5. Ejemplos 61

3.5.1. Grupos cíclicos 61

3.5.2. El grupo diedral D_4 62

3.5.3. El grupo de Heisenberg 62

3.5.4. Extensiones de D_4 63

Bibliografía **69**

English Abstract

This text is the required master thesis that the author needs to present in order to obtain his Master's degree in mathematics. It introduces the Galois embedding problem, focusing in Brauer type embedding problems, which can be studied through the second cohomology group and the relative Brauer group. With that purpose, the cohomology groups H^i for $i = 0, 1, 2$ are introduced as well as the required tools of central simple algebras required to define and understand the Brauer group and deal with the obstructions of the problems.

Introducción

El Problema Inverso de Galois surge al considerar la pregunta de si fijado un cuerpo K y dado un grupo finito G, existe una extensión de K cuyo grupo de Galois sea isomorfo a G. Este se puede dividir en dos partes: dar respuesta a la pregunta y, en caso afirmativo, dar dicha extensión (o el polinomio correspondiente). En la formulación clásica del problema suele tomar $K = \mathbb{Q}$, y en ese caso la pregunta pasa a ser si todo grupo finito es realizable sobre $\mathbb{Q}$.

El Teorema de Fundamental de la Teoría de Galois establece (entre otras cosas) que dada una extensión de Galois L/K con grupo G, si consideramos un cuerpo intermedio $K \subset M \subset L$ la extensión M/K es de Galois si y sólo si $\mathrm{Gal}(L/M)$ es un subgrupo normal de $\mathrm{Gal}(L/K)$, y en ese caso se tiene $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$. Es decir se tiene una sucesión exacta corta

$$1 \to \mathrm{Gal}(L/M) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K) \to 1$$

Con esto se puede considerar el siguiente enfoque al Problema Inverso de Galois: se busca primero una G/N-extensión M/K (con N un subgrupo normal) y se busca extenderla a una G-extensión L/K. Esto se puede formular de la siguiente manera: dada una G-extensión M/K y un epimorfismo $E \to G$, buscamos una extensión L/K isomorfismo $\varphi : \mathrm{Gal}(L/K) \to E$ de tal manera que el diagrama conmute:

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \xrightarrow{\mathrm{res}_M} & \mathrm{Gal}(M/K) \\ {\scriptstyle\varphi}\downarrow & & \| \\ E & \xrightarrow[\pi]{} & G \end{array}$$

Esto es lo que se conoce como el problema de inmersión.

En 1937 Scholz y Richard prueban que todo l-grupo ocurre como grupo de Galois sobre $\mathbb{Q}$, con l un primo impar, resolviendo sucesiones de problemas de inmersión.

Basándose en esto, Shafarevich prueba en 1954 que todo grupo resoluble es realizable sobre cualquier cuerpo de números algebraicos [7, Capítulo 9.6]. Más tarde Ishkhanov prueba que todo problema de inmersión con núcleo nilpotente y extensión trivial tiene solución [3, Capítulo 5.5], con lo que se da otra prueba del resultado de Shafarevich [3, Capítulo 5.6]. Otras aplicaciones del problema de inmersión consisten en la realización de extensiones de grupos simples, para los cuales existen resultados de Matzat y Serre entre otros.

En este trabajo nos centramos en los denominados problemas de inmersión de tipo Brauer, llamados así debido a que fueron considerados por él en su estudio del grupo de Brauer y la clasificación de álgebras centrales simples de dimensión finita. Para dicho tipo de problemas, en los que el núcleo se puede ver como un grupo de raíces p-ésimas de la unidad, puede darse una condición necesaria y suficiente en función de un elemento del segundo grupo de cohomología $H^2(G, M^*)$. Al contrario que Brauer, nosotros utilizaremos la relación entre $H^2(G, M^*)$ y el grupo relativo de Brauer $\mathrm{Br}(M/K)$ para dar con mayor facilidad condiciones para la resolución de los problemas de inmersión.

En el primer capítulo introducimos los grupos de cohomología $H^0(G, A)$, $H^1(G, A)$ y $H^2(G, A)$, así como la relación de H^1 con el producto semidirecto y la de H^2 con las extensiones de grupos, con mayor énfasis en lo segundo. También vemos las aplicaciones inducidas por el cambio de coeficientes, la inclusión de un subgrupo o la proyección a un cociente.

En el segundo introducimos el Problema de Inmersión, demostraremos que la resolubilidad de los problemas de inmersión depende de un elemento de $H^2(G, M^*)$ y veremos varios ejemplos.

En el tercero presentamos el grupo de Brauer, para lo cual primero necesitamos varios conceptos y resultados sobre álgebras centrales simples, muchos de los cuales no probaremos. Si demostraremos el isomorfimo entre $H^2(G, M^*)$ y $\mathrm{Br}(M/K)$ y alguna otra relación, y descompondremos la obstrucción (la imagen en $\mathrm{Br}(M/K)$ del elemento de $H^2(G, M^*)$ del cuál depende la resolubilidad del problema) en producto de álgebras cíclicas y de cuaterniones, lo que hará que sea más fácil de tratar. Por último retomaremos los ejemplos del Capítulo 2 e iremos más allá, llegando a ver condiciones para varios grupos de orden 16.

Durante todo el trabajo seguimos principalmente [5, Capítulos 2-4]. Además, en el Capítulo 1 hemos utilizado [4, Capítulo 6.10] para el desarrollo de H^2, así como [1, Capítulo 4] para algunas interpretaciones y [7, Capítulo 1] para algún detalle sobre

las aplicaciones entre grupos; en el Capítulo 2 se ha consultado la introducción y notación del problema de [3]; y en el Capítulo 3 se ha consultado [4, Capítulos 4 y 8.5] para resultados de álgebras y la relación del grupo de Brauer y $H^2(G, M^*)$, [2, Capítulos 1 y 2.1] para álgebras de cuaterniones y el Teorema de Wedderburn, y [5] para los ejemplos. Para la historia del problema de inmersión se ha consultado [8].

1 Cohomología de grupos

1.1 G-módulos y H^0

Definición 1.1. *Dado un grupo G, un G-módulo es un grupo abeliano A sobre el que tenemos una acción de G, es decir una aplicación $G \times A \to A$, $(\sigma, a) \mapsto \sigma a$, tal que*

$$(\sigma\tau)a = \sigma(\tau(a))$$
$$1_G(a) = a.$$

y además dicha acción sea compatible con la estructura de grupo de A, es decir que cumpla

$$\sigma(a+b) = \sigma a + \sigma b$$

En otras palabra, podemos ver los elementos de G como automorfismos de A.

Normalmente, el grupo A también lo escribiremos con notación multiplicativa.

Definición 1.2. *Dado un G-módulo A, el grupo de cohomología $H^0(G, A)$ es el subgrupo de los elementos fijos por la acción de G,*

$$A^G = \{a \in A : \sigma a = a,\ \forall \sigma \in G\}.$$

Cuando la acción de G sobre A es la trivial, es decir, $A^G = A$, diremos que A es un G-módulo trivial.

Observación 1.1. En el caso de que tengamos un grupo E no abeliano, con G actuando mediante automorfismos, lo denominaremos G-grupo y definimos $H^0(G, E)$ de la misma manera.

Podemos definir la siguiente aplicación $N_G : A \to A^G$, $N_G(a) = \prod_{\sigma \in G} \sigma a$, que llamamos **norma** (si estamos con un grupo aditivo, la llamamos **traza**).

Ejemplo 1.1. Dado un cuerpo K y una extensión de Galois L/K con $G = Gal(L/K)$. Entonces los grupos aditivo L^+ y multiplicativo L^* de L son G-módulos (con la acción del grupo de Galois) con $H^0(G, L^+) = K^+$ y $H^0(G, L^*) = K^*$. Además, en el caso multiplicativo la norma que hemos definido arriba coincide con la norma usual de extensiones de cuerpos, $N_{L/K} : L^* \to K^*$; y en el caso aditivo coincide con la traza.

1.2 El producto semidirecto y H^1

Definición 1.3. *Dados un grupo G y un G-módulo A, se define el producto semidirecto de A y G, que denotaremos $A \rtimes G$, como el grupo dado por el conjunto $A \times G$ y la operación*

$$(a, \sigma)(b, \tau) = (a(\sigma b), \sigma\tau),$$

con elemento neutro $(1_A, 1_G)$ e inverso $(\sigma^{-1}a^{-1}, \sigma^{-1})$.

Observación 1.2.

1. Podemos ver tanto a A como a G como subgrupos de $A \rtimes G$, ya que
$$A \simeq \{(a, 1_G), a \in A\} \quad y \quad G \simeq \{(1_A, \sigma), \sigma \in G\}$$
2. Además A visto como subgrupo de $A \rtimes G$ es un subgrupo normal:
$$(\sigma^{-1}a^{-1}, \sigma^{-1})(b, 1)(a, \sigma) = ((\sigma^{-1}a^{-1})(\sigma^{-1}ba), \sigma^{-1}\sigma) = (\sigma^{-1}(a^{-1}ba), 1) \in A$$
3. Si la acción de G sobre A es la trivial, el producto semidirecto coincide con el producto directo $A \times G$.
4. Dentro de $A \rtimes G$ se cumple también que $A \cap G = \{(1_A, 1_G)\}$ y
$$AG := \{ag : a \in A, g \in G\} = A \rtimes G.$$

Proposición 1.1. Cualquier subgrupo $H \leq A \rtimes G$ que verifique $A \cap H = \{1\}$ y $AH = A \times G$ es isomorfo a G.

Demostración. Tenemos que $HA/A \simeq H/H \cap A = H$ ya que $H \cap A = \{1\}$. Por lo tanto si consideramos la proyección

$$\varphi : A \rtimes G \to G, \ (a, \sigma) \mapsto \sigma,$$

tenemos que

$$G \simeq \frac{A \rtimes G}{\operatorname{Ker} \varphi} \simeq \frac{AH}{A} \simeq H.$$

A un subgrupo $H \leq A \rtimes G$ que cumpla las condiciones de este resultado se le denomina **complemento** de A (esto incluye al propio G).

Sea $\psi : H \to G$ el isomorfismo y consideremos su inversa $\psi^{-1} : G \to H$, que es de la forma $\psi^{-1}(\sigma) = (a_\sigma, \sigma)$, luego da lugar a una aplicación $a_\sigma : G \to A$. Debido a la operación de grupo de $A \rtimes G$, dicha aplicación va a cumplir

$$a_{\sigma\tau} = a_\sigma(\sigma a_\tau).$$

Definición 1.4. *Sean G un grupo y A un G-módulo. Una aplicación $a : G \to A$ satisfaciendo la propiedad de arriba, es decir*

$$a_{\sigma\tau} = a_\sigma(\sigma a_\tau),$$

la denominaremos ***homomorfismo cruzado***[1]*. Si además es de la forma*

$$\sigma \mapsto b(\sigma b^{-1})$$

para $b \in A$, diremos que es ***principal****.*

Obviamente los homomorfismos cruzados principales verifican la condición de homomorfismo cruzado:

$$a_\sigma(\sigma a_\tau) = b(\sigma b^{-1})(\sigma b)(\sigma\tau b^{-1}) = b(\sigma\tau b^{-1}) = a_{\sigma\tau}$$

También destacar que a pesar de su nombre, los homomorfismos cruzados no son homomorfismos (salvo que la acción de G sea la trivial).

Es obvio que dados dos homomorfismos cruzados $a, b : G \to A$, la aplicación $a + b : G \to A$, $\sigma \mapsto a_\sigma + b_\sigma$ también lo es, ya que la acción de G sobre A respeta la suma y A es abeliano. Es fácil comprobar que:

Proposición 1.2. Dados un grupo G y un G-módulo A, el conjunto de todos los homomorfismos cruzados $A \to G$ forman un grupo con la operación de A punto a punto, que denotamos $Z^1(G, A)$, del cual los homomorfismos cruzados principales forman un subgrupo $B^1(G, A)$.

Definición 1.5. *Dados un grupo G y un G-módulo A, definimos el* ***primer grupo de cohomología de G con coeficientes en A*** *como*

$$H^1(G, A) := \frac{Z^1(G, A)}{B^1(G, A)}$$

[1] Del inglés *crossed homomorphism.*

Observación 1.3. Cuando tenemos la acción trivial, $B^1(G, A) = \{1\}$ y por lo tanto $H^1(G, A) = Z^1(G, A) = \mathrm{Hom}(G, A)$.

Proposición 1.3. Dados un grupo G y un G-módulo A, $Z^1(G, A)$ clasifica los complementos de A.

Demostración. Hemos visto que tomando la inversa del isomorfismo $H \simeq G$ todo complemento da lugar a un homomorfismo cruzado.

Por el contrario supongamos que tenemos un homomorfismo cruzado $a : G \to A$. Consideremos el conjunto

$$H = \{(a_\sigma, \sigma) \mid \sigma \in G\} \subseteq A \rtimes G,$$

que por la propiedad de los homomorfismos cruzados es un subgrupo de $A \rtimes G$. Como $a_\sigma = a_{\sigma 1} = a_\sigma(\sigma a_1)$, tenemos que $a_1 = 1$ y por tanto $A \cap H = \{1\}$. Por último es obvio que dado que $(a_\sigma, 1) \in A$ para todo $\sigma \in G$, se cumple $AH = A \rtimes G$ y por lo tanto H es un complemento. ∎

Dado un complemento H de A, que ahora sabemos que podemos escribir como $\{(a_\sigma, \sigma) \mid \sigma \in G\}$ para un $a \in Z^1(G, A)$, es fácil observar que para $b \in A$ se tiene que bHb^{-1} es otro complemento ya que $\sigma \mapsto ba_\sigma(\sigma b^{-1})$ es también un homomorfismo cruzado. Tenemos que si a' es el homomorfismo cruzado correspondiente a bHb^{-1}, se tiene la relación $a'_\sigma = a_\sigma b(\sigma b^{-1})$. Es decir, se diferencian en un elemento de $B^1(G, A)$. Por lo tanto $H^1(G, A)$ clasifica las clases de conjugación de los complementos de A.

Ejemplo 1.2 (Teorema 90 de Hilbert). Sean un cuerpo K y una extensión de Galois L/K, con grupo de Galois $Gal(L/K) = G$. Denotemos por L^* y L^+ los grupos multiplicativo y aditivo de L respectivamente, que hemos visto antes que son G-módulos. Entonces:

$$H^1(G, L^*) = 1.$$

$$H^1(G, L^+) = 0.$$

Observación 1.4. Podemos definir de igual manera Z^1, B^1 y H^1 cuando tenemos un G-grupo E (es decir no abeliano), siendo estos conjuntos en vez de grupos. Más concretamente $Z^1(G, E)$ y $H^1(G, E)$ van a ser conjuntos punteados/basados, es decir conjuntos con un elemento destacado (el que correspondería con el elemento neutro en la definicion para G-módulos).

1.3 Extensiones de grupos y H^2

Definición 1.6. *Llamaremos extensión de un grupo G por otro grupo A a una sucesión exacta corta,*

$$1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1,$$

es decir que se cumple que ι es inyectivo, π sobreyectivo y $\operatorname{Ker}\pi = \operatorname{Im}\iota$. Se dice que A es el núcleo de la extensión.

Definición 1.7. *Dadas dos extensiones de G por A,*

$$1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1, \ y \quad 1 \to A \xrightarrow{\iota'} E' \xrightarrow{\pi'} G \to 1,$$

*diremos que son **equivalentes** si existe un homomorfismo $h : E \to E'$ tal que el diagrama*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{\iota} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle h} & & \| & & \\ 1 & \longrightarrow & A & \xrightarrow[\iota']{} & E' & \xrightarrow[\pi']{} & G & \longrightarrow & 1 \end{array}$$

conmuta.

Proposición 1.4. Dicho homomorfismo es en realidad un isomorfismo.

Demostración. Empecemos por la inyectividad. Sea $e \in E$ tal que $h(e) = 1_{E'}$. Entonces por conmutatividad $\pi(e) = \pi'(h(e)) = \pi'(1_{E'}) = 1_G$, luego $e \in \operatorname{Ker}\pi$ y por exactitud existe $a \in A$ tal que $e = \iota(a)$. Tenemos que $1_{E'} = h(e) = h(\iota(a)) = \iota'(a)$ por conmutatividad y como ι' e ι son inyectivos $a = 1_A$ y $e = 1_E$ por lo que $\operatorname{Ker} h = 1_E$.

Veamos ahora la sobreyectividad. Sea $e' \in E'$, entonces como π es sobreyectivo existe $e \in E$ tal que $\pi(e) = \pi'(e') = \pi'(h(e))$. Tenemos que $e' - h(e) \in \operatorname{Ker}\pi'$ luego por exactitud existe $a \in A$ tal que $e' - h(e) = \iota'(a) = h(\iota)(a)$. Por lo tanto $e' = h(e + \iota(a))$ y se cumple $\operatorname{Im} h = E'$. ∎

Observación 1.5. Sin embargo no se da el recíproco. Es decir, si $h : E \to E'$ es un isomorfismo, en general no es una equivalencia de extensiones.

Vamos a trabajar siempre con extensiones con núcleo A abeliano. En este caso, una extensión de G por A induce en A la siguiente estructura de G-módulo: Sean $\sigma \in G$ y $a \in A$ y sea $s \in E$ tal que $\pi(s) = \sigma$. Ahora consideremos $s\iota(a)s^{-1} \in \iota(A)$, ya que $\iota(A) \lhd E$ (por ser el núcleo de $\pi : E \to G$). Como además ι es inyectivo, existe un único elemento $x \in A$ tal que $\iota(x) = s\iota(a)s^{-1}$. Este elemento no depende de la elección

de s, ya que si consideramos $s \neq s' \in E$ tal que $\pi(s') = \sigma$ se cumple que $\pi(s's^{-1}) = 1_G$, luego por exactitud existe $b \in A$ tal que $\iota(b) = s's^{-1}$ y $s' = \iota(b)s$. Finalmente, por ser $\iota(A)$ abeliano tenemos que $s'\iota(a)s'^{-1} = \iota(b)s\iota(a)s^{-1}\iota(b)^{-1} = s\iota(a)s^{-1}$. Por lo tanto $\iota(x) = s\iota(a)s^{-1}$ únicamente depende de a y de σ, por lo que vamos a definir $\sigma a := x$ y de esta forma tenemos nuestra acción de G sobre A, dada por:

$$\iota(\sigma a) = s\iota(a)s^{-1}$$

Como $A \simeq \iota(A)$ esto es una acción de G en A, que dota a A de estructura de G-módulo. Si A tenía ya estructura de G-módulo, y la extensión de G por A induce la misma, diremos que es una **extensión de G con el G-módulo A**. Si la estructura de G-módulo es trivial, diremos que es una extensión **central**, ya que entonces sucede que $\iota(A) \subseteq Z(E)$.

Proposición 1.5. Dos extensiones equivalentes inducen la misma estructura de G-módulo sobre A.

Demostración. Supongamos que tenemos dos extensiones equivalentes, es decir que tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{\iota} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle h} & & \| & & \\ 1 & \longrightarrow & A & \xrightarrow[\iota']{} & E' & \xrightarrow[\pi']{} & G & \longrightarrow & 1 \end{array}$$

Sea $s \in E$ tal que $\pi(s) = \sigma$, entonces la acción de la primera extensión viene dada por $\iota(\sigma a) = s\iota(a)s^{-1}$. Como por conmutatividad se tiene que $\pi'(h(s)) = \pi(s) = \sigma$, la acción de la segunda extensión la podemos escribir como

$$\iota'(\sigma a) = h(s)\iota'(a)h(s)^{-1}$$

con $\pi(s) = \sigma$. Por conmutatividad de nuevo $\iota' = h \circ \iota$ luego la acción es la misma. ∎

Esta Proposición junto a la 1.4 nos verifican que la equivalencia entre extensiones es una equivalencia "buena" (es decir que tiene sentido utilizar dicho término).

Para nuestra acción hemos hecho una elección de elementos $s_\sigma \in E$ tales que $\pi(s_\sigma) = \sigma$, por lo que cada posible elección da lugar a una aplicación $s_\sigma : G \to E$, tal que $\pi \circ s = 1_G$. A una aplicación con estas características la denominaremos **sección** de la extensión.

Dada una sección s, al considerar $s_\sigma s_\tau s_{\sigma\tau}^{-1} \in E$, $\sigma, \tau \in G$ ocurre que $\pi(s_\sigma s_\tau s_{\sigma\tau}^{-1}) = 1_G$, luego por exactitud existe un único $c \in A$ con $\iota(c) = s_\sigma s_\tau s_{\sigma\tau}^{-1}$. Esto da lugar a una aplicación $c_{\sigma,\tau} : G \times G \to A$.

¿Depende la aplicación $c_{\sigma,\tau}$ de la sección escogida? Consideremos otra sección $t : G \to E$, $\pi \circ t = 1_G$. Entonces tenemos

$$\pi(t_\sigma s_\sigma^{-1}) = \pi(t_\sigma)\pi(s_\sigma^{-1}) = \sigma\sigma^{-1} = 1_G.$$

por lo que por exactitud existe un único $a_\sigma \in A$ tal que $t_\sigma s_\sigma^{-1} = \imath(a_\sigma)$ y por lo tanto $t_\sigma = \imath(a_\sigma)s_\sigma$ (podemos considerar una aplicación $a : G \to A$, $a \mapsto a_\sigma$). Si calculamos $c' : G \times G \to A$ la aplicación correspondiente a la sección t tenemos que $t_\sigma t_\tau = \imath(c'_{\sigma,\tau})t_{\sigma\tau}$, luego:

$$\begin{aligned}
\imath(c'_{\sigma,\tau}) &= t_\sigma t_\tau t_{\sigma\tau}^{-1} \\
&= \imath(a_\sigma)s_\sigma\imath(a_\tau)s_\tau s_{\sigma\tau}^{-1}\imath(a_{\sigma\tau})^{-1} \\
&= \imath(a_\sigma)\imath(\sigma a_\tau)s_\sigma s_\tau s_{\sigma\tau}^{-1}\imath(a_{\sigma\tau})^{-1} \\
&= \imath(c_{\sigma,\tau})\imath(a_\sigma a_\tau a_{\sigma\tau}^{-1}),
\end{aligned}$$

donde hemos utilizado que $\imath(\sigma a)s_\sigma = s_\sigma\imath(a)$ (la acción de G en A). Por lo tanto tenemos que las aplicaciones c, c' dadas por dos secciones distintas cumplen

$$c'_{\sigma,\tau} = c_{\sigma,\tau}(a_\sigma \sigma a_\tau a_{\sigma\tau}^{-1})$$

para una aplicación $a : G \to A$.

Observemos también que por la asociatividad , c cumple que para $\sigma, \tau, \rho \in G$:

$$\begin{aligned}
\imath(c_{\rho,\sigma}c_{\rho\sigma,\tau}) &= s_\rho s_\sigma s_{\rho\sigma}^{-1} s_{\rho\sigma} s_\tau s_{\rho\sigma\tau}^{-1} \\
&= s_\rho s_\sigma s_\tau s_{\rho\sigma\tau}^{-1} \\
&= s_\rho s_\sigma s_\tau s_{\sigma\tau}^{-1} s_{\sigma\tau} s_{\rho\sigma\tau}^{-1} \\
&= s_\rho \imath(c_{\sigma,\tau}) s_{\sigma\tau} s_{\rho\sigma\tau}^{-1} \\
&= \imath(\rho c_{\sigma,\tau}) s_\rho s_{\sigma\tau} s_{\rho\sigma\tau}^{-1} \\
&= \imath(\rho c_{\sigma,\tau} c_{\rho,\sigma\tau}).
\end{aligned}$$

Si volvemos a la diferencia entre c y c' y consideramos la aplicación $(\sigma, \tau) \mapsto a_\sigma \sigma a_\tau a_{\sigma\tau}^{-1}$, podemos ver que también verifica la igualdad:

$$\begin{aligned}
a_\rho \rho a_\sigma a_{\rho\sigma}^{-1} a_{\rho\sigma} \rho\sigma a_\tau a_{\rho\sigma\tau}^{-1} &= a_\rho \rho a_\sigma \rho\sigma a_\tau a_{\rho\sigma\tau}^{-1} \\
&= \rho(a_\sigma \sigma a_\tau a_{\sigma\tau}^{-1})\rho a_{\sigma\tau} a_\rho a_{\rho\sigma\tau}^{-1} \\
&= \rho(a_\sigma \sigma a_\tau a_{\sigma\tau}^{-1})(a_\rho \rho a_{\sigma\tau} a_{\rho\sigma\tau}^{-1}).
\end{aligned}$$

Definición 1.8. *Sean G un grupo y A un G-módulo. Una aplicación $c : G\times G \to A$ satisfaciendo la propiedad de arriba, es decir*

$$c_{\rho,\sigma}c_{\rho\sigma,\tau} = (\rho c_{\sigma,\tau})c_{\rho,\sigma\tau}$$

se denomina ***sistema de factores***[2]*. Si además es de la forma*

$$(\sigma,\tau) \mapsto a_\sigma(\sigma a_\tau)a_{\sigma\tau}^{-1}$$

para alguna aplicación $a : G \to A$, lo denominaremos ***sistema de factores escindidos***[3]*.*

De igual manera que ocurría con los homomorfismos cruzados, tenemos:

Proposición 1.6. Los sistemas de factores $c : G \times G \to A$ forman un grupo abeliano con la operación de A punto a punto que denotamos $Z^2(G, A)$. Los sistemas de factores escindidos forman un subgrupo del mismo, que denotamos $B^2(G, A)$.

Definición 1.9. *Dados un grupo G y un G-módulo A, definimos el* ***segundo grupo de cohomología de G con coeficientes en*** *A como el grupo cociente*

$$H^2(G, A) := \frac{Z^2(G, A)}{B^2(G, A)}.$$

Como hemos visto antes, los elementos de $Z^2(G, A)$ correspondientes a dos secciones distintas de una misma extensión se diferencian en un elemento de $B^2(G, A)$, luego pertenecen a la misma clase en $H^2(G, A)$. Con esto tenemos que toda a toda extensión de G con el G-módulo A le corresponde una única clase que no depende de la sección escogida. Más aún, se cumple:

Teorema 1.1. *El grupo de cohomología $H^2(G, A)$ clasifica las extensiones de grupos de G con el G-módulo A salvo equivalencia, es decir:*

1. *Dos extensiones de grupos son equivalentes si y sólo si inducen el mismo G-módulo A y tienen la misma clase de cohomología.*
2. *Para todo $[c] \in H^2(G, A)$ existe una extensión de G con el G-módulo A cuya clase de cohomología es $[c]$.*

Demostración. 1) Por la Proposición 1.5 dos extensiones equivalentes dan lugar a la misma acción de G sobre A. Además, si $s : G \to E$ es una sección de la primera

[2]Del inglés *factor system.*
[3]Del inglés *splitting factor system*

extensión, $h \circ s : G \to E'$ lo es de la segunda. Luego si c es un representante de la clase de cohomología de la primera, dado por una elección de s, es decir $\imath(c_{\sigma,\tau}) = s_\sigma s_\tau s_{\sigma\tau}^{-1}$; entonces es el representante de la clase de cohomología de la segunda extensión viene dado por $\imath'(c') = h(s_\sigma s_\tau s_{\sigma\tau}^{-1})$. Como $\imath' = h \circ \imath$ tenemos que $c = c'$ y por tanto ambas extensiones tienen la misma clase de cohomología.

Veamos ahora el caso contrario y supongamos que tenemos dos extensiones de G con el G-módulo A y la misma clase de cohomología $[c]$. Sean s y s' secciones correspondientes a dichas extensiones. Se cumple que dado $e \in E$ tal que $\pi(e) = \sigma$, $\pi(es_\sigma^{-1}) = 1_G$ luego existe un único $a \in A$ que verifica $\imath(a)s_\sigma = e$. Como π es sobreyectivo, todo elemento $e \in E$ lo podemos expresar de esta manera. Tenemos que

$$\begin{aligned} ef &= \imath(a)s_\sigma \imath(b)s_\tau = \imath(a)s_\sigma \imath(b)s_\sigma^{-1}s_\sigma s_\tau \\ &= \imath(a(\sigma b))s_\sigma s_\tau = \imath(a(\sigma b)c_{\sigma,\tau})s_{\sigma\tau}. \end{aligned}$$

Por lo que podemos expresar la operación en E mediante la acción de G y la clase de cohomología de la extensión. Análogamente para E'. Consideremos ahora la aplicación $h : E \to E'$, $e = \imath(a)s_\sigma \mapsto \imath'(a)s'_\sigma = e'$, que por lo que acabamos de ver es un homomorfismo. Obviamente $h \circ \imath = \imath'$, y $\pi(e) = \pi(\imath(a)s_\sigma) = \sigma = \pi'(\imath'(a)s'_\sigma) = (\pi' \circ h)(e)$. Por lo tanto las extensiones son equivalentes.

2) Supongamos que tenemos un elemento de $Z^2(G, A)$, es decir una aplicación $c : G \times G \to A$ que cumple

$$c_{\rho,\sigma}c_{\rho\sigma,\tau} = (\rho c_{\sigma,\tau})c_{\rho,\sigma\tau}$$

para $\sigma, \tau, \rho \in G$. Vamos a construir una extensión de G por A tal que la acción sea la correspondiente y c sea (un representante de) su clase de cohomología. Consideremos por tanto el grupo E dado por el conjunto $A \times G$ y la operación

$$(a, \sigma)(b, \tau) = (a(\sigma b)c_{\sigma,\tau}, \sigma\tau)$$

La operación es cerrada claramente, y utilizando que c es un sistema de factores po-

demos ver que también es asociativa:

$$\begin{aligned}(c,\rho)[(a,\sigma)(b,\tau)] &= (c,\rho)(a(\sigma b)c_{\sigma,\tau},\sigma\tau)\\ &= (c(\rho(a(\sigma b)c_{\sigma,\tau}))c_{\rho,\sigma\tau},\rho\sigma\tau)\\ &= (c(\rho(a(\sigma b)))c_{\rho,\sigma}c_{\rho\sigma,\tau},\rho\sigma\tau)\\ &= (c(\rho a)c_{\sigma,\rho}(\rho\sigma b)c_{\rho\sigma,\tau},\rho\sigma\tau)\\ &= (c(\rho a)c_{\rho,\sigma},\rho\sigma)(b,\tau)\\ &= [(c,\rho)(a,\sigma)](b,\tau)\end{aligned}$$

Ahora, observamos que tomando primero $\sigma = \rho = 1$ y luego $\rho = \tau, \sigma = \tau = 1$, tenemos las siguientes igualdades:

$$c_{1,1}c_{1,\tau} = c_{1,\tau}c_{1,\tau}; \quad c_{\tau,1}c_{\tau,1} = \tau c_{1,1}c_{\tau,1};$$

luego

$$c_{1,\tau} = c_{1,1} \quad y \quad \tau c_{1,1} = c_{\tau,1} \tag{1.1}$$

y podemos comprobar que el elemento neutro es $(c_{1,1}^{-1}, 1)$. En efecto

$$(c_{1,1}^{-1}, 1)(b,\tau) = (c_{1,1}^{-1}bc_{1,\tau},\tau) = (b,\tau).$$

$$(b,\tau)(c_{1,1}^{-1}, 1) = (b(\tau c_{1,1}^{-1})c_{\tau,1},\tau) = (b,\tau).$$

Finalmente el inverso de (b,τ) será $(c_{1,1}^{-1}c_{\tau^{-1},\tau}^{-1}(\tau^{-1}b^{-1}),\tau^{-1})$:

$$\begin{aligned}(c_{1,1}^{-1}c_{\tau^{-1},\tau}^{-1}(\tau^{-1}b^{-1}),\tau^{-1})(b,\tau) &= (c_{1,1}^{-1}, c_{\tau^{-1},\tau}^{-1}(\tau^{-1}b^{-1})(\tau^{-1}b)c_{\tau^{-1},\tau},\tau^{-1}\tau)\\ &= (c_{1,1}^{-1}, 1).\\ (b.\tau)(c_{1,1}^{-1}c_{\tau^{-1},\tau}^{-1}(\tau^{-1}b^{-1}),\tau^{-1}) &= (c_{1,1}^{-1}(\tau c_{\tau^{-1},\tau}^{-1})c_{\tau,\tau^{-1}}, 1) = (c_{1,1}^{-1}, 1).\end{aligned}$$

Donde además de (1.1) utilizamos que para $\rho = \tau, \sigma = \tau^{-1}$ y $\tau = 1$ se cumple que

$$c_{\tau,\tau^{-1}}c_{1,1} = \tau c_{\tau^{-1},\tau}c_{\tau,1}. \tag{1.2}$$

Tenemos por lo tanto nuestro grupo E, faltan las aplicaciones de la extensión y ver que la extensión verifica lo que queremos.

Consideremos las aplicaciones $\imath : A \to E, \imath(a) = (ac_{1,1}^{-1}, 1)$ y $\pi : E \to G, \pi(a,\sigma) = \sigma$. Claramente π es un homomorfismo sobreyectivo (la proyección sobre la segunda coordenada), mientras que

$$\imath(ab) = (abc_{1,1}^{-1}, 1) = (abc_{1,1}^{-1}, 1)(c_{1,1}^{-1}, 1) = (ac_{1,1}^{-1}, 1)(bc_{1,1}^{-1}, 1) = \imath(a)\imath(b),$$

por lo que ι es también un homomorfismo, que además es inyectivo. También se cumple que $\pi\circ\iota = 1_G$, por lo que $\operatorname{Im}\iota \subseteq \operatorname{Ker}\pi$. La otra igualdad se tiene viendo que los elementos de $\operatorname{Ker}\pi$ son los $(a,1)$ con $a \in A$, luego siempre tenemos $\iota(ac_{1,1}) = (a,1)$. Por lo tanto $\operatorname{Im}\iota = \operatorname{Ker}\pi$ y tenemos una extensión de G por A.

Falta ver que efectivamente la extensión $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ cumple lo que queremos. Empecemos con la estructura de G-módulo. Tomemos $s = (1_A, \sigma)$ que verifica $\pi(s) = \sigma$. Tenemos

$$\begin{aligned} s\iota(a)s^{-1} &= (1,\sigma)(ac_{1,1}^{-1},1)(1,\sigma)^{-1} = (\sigma c_{1,1}^{-1}\sigma a c_{\sigma,1},\sigma)(1,\sigma)^{-1} \\ &= (\sigma a,\sigma)(1,\sigma)^{-1} = (\sigma a,\sigma)(c_{1,1}^{-1}c_{\sigma^{-1},\sigma}^{-1},\sigma^{-1}) \\ &= ((\sigma a)(\sigma c_{1,1}^{-1})(\sigma c_{\sigma^{-1},\sigma}^{-1})c_{\sigma,\sigma^{-1}},1) \\ &= ((\sigma a)c_{1,1}^{-1},1) = \iota(\sigma a), \end{aligned}$$

donde hemos vuelto a usar (1.1) y (1.2). Con esto hemos comprobado que la estructura de G-módulo inducida por la extensión es la que queríamos.

Finalmente solo queda ver que la clase de cohomología tiene como representante a c. Para ello escogemos $s : G \to E$ tal que $\pi\circ s = 1_G$, en este caso $s_\sigma = (1,\sigma)$ y aplicando de nuevo (1.1) y (1.2) vemos que

$$s_\sigma s_\tau = (1,\sigma)(1,\tau) = (c_{\sigma,\tau},\sigma\tau) = (c_{1,1}^{-1}c_{\sigma,\tau},1)(1,\sigma\tau) = \iota(c_{\sigma,\tau})s_{\sigma\tau}.$$

y por lo tanto la clase de cohomología de nuestra extensión es $[c]$ tal y como queríamos. ∎

Tenemos entonces que dado un grupo G y un G-módulo A, los elementos de $H^2(G,A)$ clasifican salvo equivalencia las extensiones de G que inducen dicha estructura de G-módulo en A. Dado que $H^2(G,A)$ es un grupo, lo natural es preguntarse: dadas las clases $[c]$ y $[c']$ de dos extensiones no equivalentes, cuál es la extensión cuya clase es $[c][c']$, así como cuál es la extensión con clase de cohomología 1.

Definición 1.10. *Diremos que una extensión* $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ ***escinde*** *si existe una sección* $s : G \to E$, $\pi\circ s = 1_G$ *que es un homomorfismo.*

Proposición 1.7. Dada una extensión con el G-módulo A son equivalentes:

1. La extensión escinde.
2. La extensión tiene clase de cohomología 1.
3. La extensión es equivalente a la extensión

$$1 \to A \xrightarrow{\iota} A \rtimes G \xrightarrow{\pi} G \to 1$$

donde $\imath(a) = (a, 1_G)$, $\pi(a, \sigma) = \sigma$.

Demostración. (1) $\Rightarrow$ (2) Si la extensión escinde, el representante de la clase de cohomología dado por dicha sección será $\imath(c_{\sigma,\tau}) = s_\sigma s_\tau s_{\sigma\tau}^{-1} = 1_G$, luego $[c] = 1$.

(2) $\Rightarrow$ (3) En la prueba del Teorema 1.1 hemos visto como construir una extensión de G con el G-módulo A que tenga una clase de cohomología $[c]$ dada. Esto es el conjunto $A \times G$ con la operación $(a, \sigma)(b, \tau) = (a(\sigma b)c_{\sigma,\tau}, \sigma\tau)$. Si sustituimos $c = 1$ tenemos el producto semidirecto y las aplicaciones son también las dadas. Entonces la extensión que tenemos con el producto semidirecto es una extensión con el G-módulo A cuya clase de cohomología es 1, luego por la primera parte del Teorema 1.1, es equivalente a nuestra extensión original.

(3) $\Rightarrow$ (1) Consideremos la inclusión de G en $A \rtimes G$ como subgrupo, $s(\sigma) = (1_A, \sigma)$. Dicha aplicación es un homomorfismo y cumple que $\pi(s(\sigma)) = \sigma$, luego es una sección y la extensión con el producto semidirecto escinde. Ahora bien como nuestra extensión es equivalente a esta, componer la sección con el homomorfismo de la equivalencia nos proporciona una sección en nuestra extensión original (como vimos al principio de la prueba del Teorema 1.1), que al ser composición de homomorfismos es un homomorfismo. Por lo tanto la extensión escinde. ∎

Con esto hemos resuelto la cuestión de las extensiones con clase trivial. Como dos extensiones equivalentes tienen el grupo del medio de la sucesión isomorfas, siempre que tengamos una extensión con clase trivial, el grupo del medio de la sucesión será isomorfo al producto semidirecto (con la acción correspondiente). De hecho esto puede considerarse es una caracterización del producto semidirecto salvo isomorfismo.

Pasemos ahora a la pregunta de la suma de clases.

Definición 1.11. *Dadas dos extensiones de G con el G-módulo A,*

$$1 \to A \xrightarrow{\imath} E \xrightarrow{\pi} G \to 1, \ y \quad 1 \to A \xrightarrow{\imath'} E' \xrightarrow{\pi'} G \to 1,$$

y consideremos los subgrupos de $E \times E'$:

$$X := \{(e, e') \in E \times E' : \pi(e) = \pi'(e')\} \quad \textit{(el pull-back de } E \textit{ y } E')$$

$$Y := \{(\imath(a), \imath'(a)^{-1}) : a \in A\} \leq X$$

$$Z := X/Y$$

Se define la ***suma de Baer*** *de dichas extensiones como la extensión*

$$1 \to A \xrightarrow{\alpha} Z \xrightarrow{\beta} G \to 1$$

donde $\alpha(a) = [(\imath(a), 1)]$ *y* $\beta[(e, e')] = \pi(e) = \pi'(e')$.

La mayoría de las comprobaciones de la definición son sencillas: X es un grupo por ser π y π' homomorfismos, Y es subgrupo porque $\pi \circ \imath = \pi' \circ \imath' = 1_G$. Para ver que Y es un subgrupo normal, sea $(\imath(a), \imath'(a)^{-1}) \in Y$ y $(e, e') \in X$. Entonces

$$(e, e')(\imath(a), \imath'(a)^{-1})(e^{-1}, e'^{-1}) = (e\imath(a)e^{-1}, e'\imath'(a)^{-1}e'^{-1})$$

y como $\pi(e) = \pi'(e')$, si lo denotamos por σ y utilizamos la acción de G en A tenemos

$$(e\imath(a)e^{-1}, e'\imath'(a)^{-1}e'^{-1}) = (\imath(\sigma a), \imath'(\sigma a^{-1}) = (\imath(\sigma a), \imath'((\sigma a)^{-1}) \in Y.$$

También es obvio que α y β son homomorfismos inyectivo y sobreyectivo respectivamente, así como que $\operatorname{Ker} \alpha = \operatorname{Im} \beta$.

Proposición 1.8. Dadas dos extensiones de G con el G-módulo A con clases de cohomología $[c]$ y $[c']$ respectivamente. Entonces la suma de Baer de dichas extensiones induce la misma estructura de G-módulo y tiene clase de cohomología $[c][c']$.

Demostración. Por comodidad vamos a omitir el $+Y$, pero cuando tomemos elementos en Z son representantes de su clase.

Empecemos por la acción. Necesitamos un $t \in Z$ tal que $\beta(t) = \sigma$, es decir (t_1, t_2) tal que $\pi(t_1) = \pi'(t_2) = \sigma$. Sean $s \in E$ y $s' \in E'$ tales que $\pi(s) = \pi'(s') = \sigma$ y hagamos $t = (s, s')$. Tenemos entonces que la acción inducida por la extensión viene dada por

$$\alpha(\sigma a) = t\alpha(a)t^{-1} = (s, s')(\imath(a), 1)(s^{-1}, s'^{-1}) = (s\imath(a)s^{-1}, 1)$$

y por lo tanto la acción coincide con la que teníamos.

Nuestras dos extensiones tenían como representantes de sus clases de cohomología c y c' respectivamente. Consideremos s y s' las secciones correspondientes. Entonces como acabamos de ver la aplicación $t : G \to Z$, $t = (s, s')$ es una sección de la suma de Baer. Se cumple que

$$\begin{aligned}
t_\sigma t_\tau &= (s_\sigma, s'_\sigma)(s_\tau, s'_\tau) \\
&= (s_\sigma s_\tau, s'_\sigma s'_\tau) \\
&= (\imath(c_{\sigma\tau})s_{\sigma\tau}, \imath'(c'_{\sigma\tau})s'_{\sigma\tau}) \\
&= (\imath(c'_{\sigma\tau})\imath(c_{\sigma\tau})s_{\sigma\tau}, \imath'(c'_{\sigma\tau})^{-1}\imath'(c'_{\sigma\tau})s'_{\sigma\tau}) \\
&= (\imath(c_{\sigma\tau}c'_{\sigma\tau}, 1)(s_{\sigma\tau}, s'_{\sigma\tau}) \\
&= \alpha(c_{\sigma\tau}c'_{\sigma\tau})t_{\sigma\tau}
\end{aligned}$$

y por lo tanto la clase de la suma de Baer es el producto de las clases de las extensiones originales tal y como queríamos.

Observación 1.6.

- Podríamos haber obtenido un representante de la extensión con clase el producto de dos clases utilizando la construcción que se da en el Teorema 1.1, sin embargo la suma de Baer nos da la extensión a partir de las otras dos extensiones, sin necesidad de conocer las clases de cohomología. (ambas maneras dan lugar a extensiones equivalentes por el Teorema 1.1)
- Mediante la suma de Baer, se puede dotar al conjunto de clases de equivalencia de extensiones de G con el G-módulo A de una estructura de grupo, haciendo que la biyección del Teorema 1.1 sea en realidad un isomorfismo.

Las extensiones que escinden (o sea que tienen clase de cohomología trivial) nos dan otra forma de ver la caracterización de $H^1(G, A)$. Dada una extensión de G con el G-módulo A con clase de cohomología trivial, consideremos el representante canónico de dicha clase:

$$1 \longrightarrow A \xrightarrow{\iota} A \rtimes G \underset{s}{\overset{\pi}{\rightleftarrows}} G \longrightarrow 1$$

Vimos anteriormente que esta extensión escindía mendiante la inclusión de G en $A \rtimes G$. Sin embargo ahora queremos ver qué debe cumplir una sección cualquiera $s : G \to A \rtimes G$ para que sea un homomorfismo. Como s es una sección, se debe cumplir que $s(\sigma) = (a_\sigma, \sigma)$, y como ha de ser un homomorfismo ha de cumplir $s(\sigma\tau) = (a_{\sigma\tau}, \sigma\tau) = (a_\sigma, \sigma)(a_\tau, \tau)$, luego por la operación de grupo vamos a tener que s_σ ha de ser de la forma (a_σ, σ) donde a_σ es un homomorfismo cruzado. Por lo tanto $Z^1(G, A)$ clasifica las escisiones de la clase de extensiones con el G-módulo A con clase 1. Otra forma de ver esto sería ver que una sección s que sea un homomorfismo ha de ser inyectiva (ya que si $s(\sigma) = 1$ no se cumple que $\pi(s(\sigma)) = 1 \neq \sigma$), y por lo tanto tenemos un subgrupo $s(G) \leq A \rtimes G$ isomorfo a G que verifica $A \cap s(G) = \{1\}$ (de nuevo por ser s una sección), y $As(G) = A \rtimes G$, luego $s(G)$ es un complemento de A.

Por lo tanto otra interpretación de $H^1(G, A)$ es que clasifica las clases de conjugación de las escisiones de la clase de extensiones con el G-módulo A con clase 1 (las clases de conjugación por A de $s(G)$).

Observación 1.7. A diferencia de la construcción de $H^0(G, A)$ y $H^1(G, A)$, el hecho de que A sea abeliano ha sido necesario, por lo que no es posible realizarlo para un G-grupo E. Sin embargo si que existe el problema de clasificar extensiones con núcleo no abeliano (ver por ejemplo [1, Capítulo 4.6]).

1.4 Aplicaciones entre grupos

Una vez tenemos nuestros grupos $H^0(G,A)$, $H^1(G,A)$ y $H^2(G,A)$, otra pregunta natural es si modificaciones "clásicas" de los grupos G y/o A se ven reflejadas de manera correspondiente en ellos.

1.4.1 Cambio de coeficientes

Definición 1.12. *Dados un grupo G y dos G-módulos A y B, diremos que un homomorfismo $\varphi : A \to B$ es un G-**homomorfismo** si respeta la acción de G, es decir*

$$\varphi(\sigma a) = \sigma\varphi(a)$$

para $\sigma \in G$, $a \in A$.

En el caso de $H^0(G,A)$ es obvio que cualquier G-homomorfismo $\varphi : A \to B$ induce un homomorfismo $H^0(G,A) \to H^0(G,B)$ ya que por la propiedad de respetar la acción de G si $a \in A$ es un elemento fijo, $\varphi(a) \in B$ también. El homomorfismo inducido en este caso no es más que la restricción de φ a A^G.

En el caso de $H^1(G,A)$ tenemos que observar que sucede con los homomorfismos cruzados. Se cumple que si $f : G \to A$ es un homomorfismo cruzado, es decir que cumple $f(\sigma\tau) = f(\sigma)(\sigma f(\tau))$ entonces $\varphi \circ f$ cumple

$$\varphi(f(\sigma\tau)) = \varphi(f(\sigma)(\sigma f(\tau))) = \varphi(f(\sigma))\varphi(\sigma f(\tau)) = \varphi(f(\sigma))\sigma\varphi(f(\tau))$$

y por lo tanto es un homomorfismo cruzado $G \to B$. Obtenemos de nuevo un homomorfismo inducido $Z^1(G,A) \to Z^1(G,B)$. Observemos ahora, que si $f \in B^1(G,A)$, es decir es de la forma $f(\sigma) = a(\sigma a^{-1})$ para un $a \in A$, entonces como φ es un G-homomorfismo se cumple $\varphi(f(\sigma)) = \varphi(a)(\sigma\varphi(a)^{-1})$. Por lo tanto el homomorfismo inducido lleva $B^1(G,A)$ en $B^1(G,B)$, luego podemos tomar cocientes para obtener un homomorfismo $\varphi^1 : H^1(G,A) \to H^1(G,B)$.

Finalmente para $H^2(G,A)$ procedemos de igual manera con los sistemas de factores. Dado uno de ellos $c : G \times G \to A$ vemos que

$$\varphi(c_{\rho,\sigma})\varphi(c_{\rho\sigma,\tau}) = \varphi(c_{\rho,\sigma}c_{\rho\sigma,\tau}) = \varphi((\rho c_{\sigma,\tau})c_{\rho,\sigma\tau}) = \varphi((\rho c_{\sigma,\tau}))\varphi(c_{\rho,\sigma\tau})) = \rho\varphi(c_{\sigma,\tau})\varphi(c_{\rho,\sigma\tau}))$$

luego $\varphi \circ c$ es un elemento de $Z^2(G,B)$. Por lo tanto tenemos un homomorfismo $Z^2(G,A) \to Z^2(G,B)$ que, al igual que en el caso anterior, va a llevar $B^2(G,A)$ en

$B^2(G,B)$, luego tomando cocientes obtenemos el homomorfismo $\varphi^2 : H^2(G,A) \to H^2(G,B)$.

En los 3 casos la aplicación φ^i inducida es un homomorfismo debido a que la estructura de grupo viene dada por la operación de A punto a punto y $\varphi : A \to B$ es un homomorfismo.

El caso $\varphi^2 : H^2(G,A) \to H^2(G,B)$ se puede expresar mediante extensiones de la siguiente manera: dada una extensión $1 \to A \to E \to G \to 1$ y un G-homomorfismo $A \to B$, entonces existe una única extensión (salvo equivalencia) que hace el siguiente diagrama conmutativo:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{\iota} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow & & \| & & \\ 1 & \longrightarrow & B & \xrightarrow{\iota'} & F & \xrightarrow{\pi'} & G & \longrightarrow & 1 \end{array}$$

Esto se puede probar tomando representantes de las extensiones en función de $[c]$ y $[\varphi(c)]$ como en el Teorema 1.1 (el homomorfismo $E' \to F'$ sería $(\varphi, 1_G)$).

1.4.2 Cambio de grupo

Vamos ahora a ver que sucede al cambiar nuestro grupo G, en concreto por un subgrupo o el cociente por un subgrupo normal.

Empecemos por el más sencillo. Consideremos un subgrupo H de G. Claramente cualquier G-módulo A es a su vez un H-módulo y además:

Proposición 1.9. La inclusión $i : H \hookrightarrow G$ induce homomorfismos $\mathrm{res}^i_{G\to H} : H^i(G,A) \to H^i(H,A)$, $i = 0,1,2$.

Demostración. Empecemos por $i = 0$. En este caso es obvio que el homomorfismo inducido es la inclusión de A^G en A^H (los elementos fijos por G son fijos por cualquier subgrupo de G).

Para $i = 1$ consideremos un elemento $f \in Z^1(G,A)$, que no es más que una aplicación $f : G \to A$ que cumple $f(\sigma\tau) = f(\sigma)(\sigma f(\tau))$. Obviamente $f \circ i$ no es más que f restringido a H, por lo que obtendremos un elemento de $Z^1(H,A)$. En particular si $f(\sigma) = a_\sigma(\sigma a^{-1})$ para cierto $a \in A$ y $\sigma \in G$, se mantiene para $\sigma \in H$ luego la aplicación manda $B^1(G,A)$ en $B^1(H,A)$ y no hay problema al tomar cociente.

Tenemos entonces

$$\begin{aligned} \mathrm{res}^1_{G\to H} : H^1(G,A) &\to H^1(H,A) \\ [f] &\mapsto [f\circ i] \end{aligned}$$

Por último para $i=2$ ocurre igual. Los elementos de $Z^2(G,A)$ son aplicaciones $G\times G\to A$ que verifican una propiedad respecto de los elementos de G y la acción sobre A, que se mantiene al restringirnos a $H\times H$ obteniendo un elemento de $Z^2(H,A)$, y de igual forma los elementos de $B^2(G,A)$ son de una forma específica que se mantiene al restringirnos a H, por lo que podemos cocientar y obtener

$$\begin{aligned} \mathrm{res}^2_{G\to H} : H^2(G,A) &\to H^2(H,A) \\ [c] &\mapsto [c\circ(i,i)] \end{aligned}$$

con $(i,i) : H\times H\to G\times G$

En los tres casos al mantener A igual, la estructura de grupo correspondiente (la operación de A punto a punto) se mantiene, por lo que tenemos homomorfismos.

Para $i=2$ que es el caso que más nos interesa, veamos cómo actúa la restricción en términos de extensiones.

Si tenemos una extensión con el G-módulo A:

$$1\to A\to E\xrightarrow{\pi} G\to 1$$

cuya clase de cohomología es $[c]\in H^2(G,A)$. Entonces la extensión

$$1\to A\to \pi^{-1}(H)\to H\to 1$$

es una extensión con el H-módulo A cuya clase de cohomología es $\mathrm{res}^2_{G\to H}[c]\in H^2(H,A)$.

Ahora veamos la inflación. Sea N un subgrupo normal de G, y A un G-módulo, entonces A^N es a su vez un G/N-módulo (la acción de N sobre A^N es la trivial por lo que al pasar al cociente no hay problema).

Proposición 1.10. La proyección canónica $\kappa : G\to G/N$ induce homomorfismos $\inf^i_{G/N\to G} : H^i(G/N,A^N)\to H^i(G,A)$, $i=0,1,2$.

Demostración. Para $i=0$, $\inf^0_{G/N\to G} : (A^N)^{G/N}\to A^G$ es la inclusión, ya que $\sigma a=\sigma Na$ (porque $a\in A^N$) y $\sigma Na=a$ (porque $a\in (A^N)^{G/N}$).

Para $i = 1$, tenemos un homomorfismo $Z^1(G/N, A^N) \to Z^1(G, A)$ donde la composición de κ con un homomorfismo cruzado $f : G/N \to A^N$ da lugar a un homomorfismo cruzado $G \to A$. (en realidad $G \to A^N$ pero A^N es un subgrupo de A) ya que como κ es un homomorfismo,

$$f(\kappa(\sigma\tau)) = f(\kappa(\sigma)\kappa(\tau)) = f(\kappa(\sigma))(\kappa(\sigma)f(\kappa(\tau))$$

y por tanto $f \circ \kappa \in Z^1(G, A)$. Además, si $f \in B^1(G/N, A^N)$, entonces es de la forma $f(\sigma N) = a(\sigma N a^{-1}) = a(\sigma a^{-1})$ (ya que $a \in A^N$) para cierto $a \in A^N$, luego tiene la misma forma para $\sigma N \in G/N$ y para $\sigma \in G$, y entonces la aplicación lleva $B^1(G/N, A^N)$ en $B^1(G, A)$. Por lo tanto, tomando cocientes tenemos el homomorfismo inducido

$$\begin{aligned} \inf^1_{G/N \to G} : H^1(G/N, A^N) &\to H^1(G, A) \\ [f] &\mapsto [f \circ \kappa] \end{aligned}$$

Para $i = 2$, de igual manera tomando un elemento $c \in Z^2(G/N, A^N)$ y componer con κ obtenemos elemento de $Z^2(G, A)$ ya que nuevamente al ser κ un homomorfismo se cumple que

$$c_{\kappa(\rho),\kappa(\sigma)} c_{\kappa(\rho\sigma),\kappa(\tau)} = c_{\kappa(\rho),\kappa(\sigma)} c_{\kappa(\rho)\kappa(\sigma),\kappa(\tau)} = \kappa(\rho) c_{\kappa(\sigma),\kappa(\tau)} c_{\kappa(\rho),\kappa(\sigma\tau)}$$

Además, como en el caso anterior, la aplicación lleva $B^2(G/N, A^N)$ en $B^2(G, A)$ y por tanto tomando cocientes tenemos el homomorfismo

$$\begin{aligned} \inf^2_{G/N \to G} : H^2(G/N, A^N) &\to H^2(G, A) \\ [c] &\mapsto [c \circ (\kappa, \kappa)] \end{aligned}$$

con $(\kappa, \kappa) : G \times G \to G/N \times G/N$.

Al igual que con la restricción, que las aplicaciones sean homomorfismos se tiene por ser la operación siempre la de A punto a punto.

Cuando está claro el contexto, se suele utilizar simplemente "res" e "inf" para referirse a la restricción e inflación. Además, ambos homomorfismos están relacionados de la siguiente manera:

Proposición 1.11. Dados un grupo G, un G-módulo A y un subgrupo normal $N \lhd G$ se tiene la siguiente sucesión exacta:

$$1 \to H^1(G/N, A^N) \xrightarrow{inf} H^1(G, A) \xrightarrow{res} H^1(N, A)$$

Demostración. Empecemos viendo que $\inf : H^1(G/N, A^N) \to H^1(G, A)$ es inyectiva. Sea $f : G/N \to A^N$ un elemento de $Z^1(G/N, A^N)$ tal que $(\inf f)(\sigma) = f(\kappa(\sigma)) = a(\sigma a^{-1})$ para $a \in A$, donde $\kappa : G \to G/N$ es la proyección canónica. Como para $n \in N$ ocurre que

$$(\inf f)(\sigma n) = a(\sigma n a^{-1}) = f(\kappa(\sigma n)) = f(\kappa(\sigma)) = a(\sigma a^{-1})$$

se cumple que $a \in A^N$ y $f(\sigma N) = a(\sigma a^{-1})$, por lo que $[f] = 1$.

Veamos ahora que $\operatorname{Ker} \inf = \operatorname{Im} \operatorname{res}$. Dado $f \in Z^1(G/N, A^N)$ tenemos que

$$(\operatorname{res}(\inf f))(\sigma) = \operatorname{res}(f(\kappa(\sigma)) = 1.$$

luego $\operatorname{Im} \inf \subseteq \operatorname{Ker} \operatorname{res}$. Para la desigualdad contraria consideremos $g : G \to A$ un elemento de $Z^1(G, A)$ tal que $(\operatorname{res} g)(\sigma) = a(na^{-1})$ para un $a \in A$. Consideremos ahora $g' \in Z^1(G, A)$ definido como

$$g'(\sigma) = g(\sigma)a(\sigma a^{-1})$$

para el mismo elemento $a \in A$. Entonces g y g' pertenecen a la misma clase en $H^1(G, A)$ (se diferencian en un elemento de $B^1(G, A)$) y se verifica que $g'(n) = 1$ para $n \in N$. Ahora definimos $f : G/N \to A$, $f(\sigma N) = g'(\sigma)$. Se cumple que para $n \in N$,

$$g'(\sigma n) = g'(\sigma)(\sigma g'(n)) = g'(\sigma)$$

luego f está bien definido, y

$$f(\sigma N) = f(n\sigma N) = g'(n\sigma) = g'(n)(ng'(\sigma)) = ng'(\sigma) = nf(\sigma N)$$

luego $f(\sigma N) \in A^N$. Tenemos por lo tanto $f \in Z^1(G/N, A^N)$ con $[\inf f] = [g'] = [g]$, por lo que $\operatorname{Ker} \inf \subseteq \operatorname{Im} \operatorname{res}$. Por doble inclusión tenemos la igualdad y la exactitud. ∎

1.4.3 La sucesión exacta larga

Consideremos una sucesión exacta corta

$$1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} D \to 1$$

donde A, B y D son G-módulos y α y β son G-homomorfismos. Entonces ya hemos visto que tenemos homomorfismos inducidos entre los H^i para el mismo índice ($i = 0, 1, 2$).

Para pasar de $i = 0$ a $i = 1$ consideremos la aplicación $\delta^0 : H^0(G, D) \to H^1(G, A)$ definida como sigue: tomemos un elemento $d \in D^G \subset D$ y tomemos $b \in B$ tal que $\beta(b) = d$, que existe por la sobreyectividad de β. Por lo tanto como β respeta la acción de G y $d \in D^G$, tenemos que

$$1 = dd^{-1} = d(\sigma d^{-1}) = \beta(b)(\sigma\beta(b^{-1})) = \beta(b(\sigma b^{-1}))$$

y $b(\sigma b^{-1}) \in \operatorname{Ker}\beta = \operatorname{Im}\alpha$. Existe entonces $a_\sigma \in A$ tal que $b(\sigma b^{-1}) = \alpha(a_\sigma)$. Esto podemos hacerlo para cualquier $\sigma \in G$ y tenemos entonces una aplicación $a : G \to A$. Podemos observar que

$$\alpha(a_{\sigma\tau}) = b(\sigma\tau b^{-1}) = b(\sigma b^{-1})(\sigma b)(\sigma\tau b^{-1}) = \alpha(a_\sigma)(\sigma\alpha(a_\tau)).$$

y por tanto, como α es inyectiva, $a_{\sigma\tau} = a_\sigma(\sigma a_\tau)$ y $a : G \to A$ es un homomorfismo cruzado. Por lo tanto definimos $\delta^0(d) = [a]$. Si tomamos otra preimagen b' de d, entonces $b'b^{-1} \in \operatorname{Ker}\beta$ y $b' = \alpha(a')b$ para un $a' \in A$. Por lo tanto el homomorfismo cruzado correspondiente vendría dado por

$$\alpha(a'_\sigma) = b'(\sigma b'^{-1}) = \alpha(a')b(\sigma b^{-1}\alpha(a'^{-1})) = \alpha(a' a_\sigma(\sigma a'^{-1})),$$

luego sería $a'_\sigma = a' a_\sigma(\sigma a'^{-1}_\tau)$ y tiene la misma clase que a_σ, luego la aplicación está bien definida. Por último es un homomorfismo (al ser $H^1(G, A)$ abeliano, el homomorfismo cruzado correspondiente a dd' sería $bb'(\sigma b'^{-1}b^{-1}) = b(\sigma b^{-1})b'(\sigma b'^{-1})$).

Para pasar de $i = 1$ a $i = 2$ definimos la aplicación $\delta^1 : H^1(G, D) \to H^2(G, A)$ de la siguiente manera: tomamos $d_\sigma \in Z^1(G, D)$ y definimos $b_\sigma : G \to B$ tal que $\beta(b_\sigma) = d_\sigma$ (que funciona porque β es sobreyectivo), lo que se llama un levantamiento. Se tiene que $b_\sigma(\sigma b_\tau)b_{\sigma\tau}^{-1} \in \operatorname{Ker}\beta$ luego por exactitud existe $c_{\sigma,\tau}$ tal que $\alpha(c_{\sigma,\tau}) = b_\sigma(\sigma b_\tau)b_{\sigma\tau}^{-1}$. Se cumple que

$$\begin{aligned}
\alpha(c_{\rho,\sigma}c_{\rho\sigma,\tau}) &= b_\rho(\rho b_\sigma)b_{\rho\sigma}^{-1}b_{\rho\sigma}(\rho\sigma b_\tau)b_{\rho\sigma\tau}^{-1} \\
&= b_\rho(\rho b_\sigma(\sigma b_\tau))b_{\rho\sigma\tau}^{-1} \\
&= b_\rho(\rho b_\sigma(\sigma b_\tau))(\rho b_{\sigma\tau}^{-1}b_{\sigma\tau}))b_{\rho\sigma\tau}^{-1} \\
&= b_\rho\alpha(\rho c_{\sigma\tau})(\rho b_{\sigma\tau})b_{\rho\sigma\tau}^{-1} \\
&= \alpha(\rho c_{\sigma,\tau}c_{\rho,\sigma\tau}),
\end{aligned}$$

luego $c_{\sigma,\tau} \in Z^2(G, A)$. Si tomamos un $b'_\sigma : G \to B$ con $\beta(b'_\sigma) = d_\sigma$ distinto, análogamente al caso de δ^0 se tiene que $b'_\sigma = \alpha(a_\sigma)b_\sigma$ para cierta aplicación $a_\sigma : G \to A$. Por tanto tenemos

$$\alpha(c_{\sigma,\tau}) = b'_\sigma(\sigma b'_\tau)b'^{-1}_{\sigma\tau} = \alpha(a_\sigma)b_\sigma(\sigma\alpha(a_\tau)b_\tau)b_{\sigma\tau}^{-1}\alpha(a_{\sigma\tau}^{-1}) = \alpha(a_\sigma(\sigma a_\tau)a_{\sigma\tau}^{-1}c_{\sigma,\tau}),$$

que está en la misma clase en $H^2(G,A)$ por lo que la aplicación está bien definida. Por último, si b_σ y b'_σ son los levantamientos respectivos de d_σ y d'_σ, entonces $b_\sigma b'_\sigma$ es un levantamiento de $d_\sigma d'_\sigma$ y por ser A, B y D abelianos se verifica que δ^1 es un homomorfismo.

Proposición 1.12. Dada una sucesión exacta corta de G-módulos

$$1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} D \to 1$$

se tiene la siguiente sucesión exacta:

$$\begin{aligned} 1 \to H^0(G,A) \xrightarrow{\alpha^0} H^0(G,B) \xrightarrow{\beta^0} H^0(G,D) \xrightarrow{\delta^0} H^1(G,A) \xrightarrow{\alpha^1} H^1(G,B) \\ \xrightarrow{\beta^1} H^1(G,D) \xrightarrow{\delta^1} H^2(G,A) \xrightarrow{\alpha^2} H^2(G,B) \xrightarrow{\beta^2} H^2(G,D). \end{aligned}$$

Demostración. Empecemos por el tramo de los H^0. En este caso α^0 y β^0 no son más que la restricción de α y β a los subgrupos fijos correspondientes, y por lo tanto se tiene inmediatamente que α^0 es inyectivo e $\operatorname{Im}\alpha^0 \subseteq \operatorname{Ker}\beta^0$. La otra inclusión se tiene viendo que si $b \in B^G$ con $\beta^0(b) = 1$ por la exactitud de β se tiene que $b = \alpha(a)$ y al ser α inyectivo, $\alpha(\sigma a) = \alpha(a)$ implica $\sigma a = a$ y por tanto $a \in A^G$.

El paso de H^0 a H^1 depende de δ^0. Sea $b \in H^0(G,B)$, entonces $\delta^0(\beta^0(b)) = a_\sigma$ tal que $\alpha(a_\sigma) = b(\sigma b^{-1}) = bb^{-1} = 1$ ya que $b \in B^G$. Por lo tanto $\operatorname{Im}\beta^0 \subseteq \operatorname{Ker}\delta^0$. Para la inclusión contraria, si $\delta^0(d) = [1]$ entonces existe $b \in B$ con $\beta(b) = d$ tal que $b(\sigma b^{-1}) = \alpha(a_\sigma)$ y $a_\sigma = a_0(\sigma a_0^{-1})$ para un cierto $a_0 \in A$. Por lo tanto

$$b(\sigma b^{-1}) = \alpha(a_\sigma) = \alpha(a_0)(\sigma\alpha(a_0)^{-1}),$$

luego $\alpha(a_0^{-1})b = (\sigma\alpha(a_0^{-1})b)$ y entonces $\alpha(a_0^{-1})b \in B^G$ y $\beta(\alpha(a_0^{-1})b) = \beta(b) = d$. Por lo tanto $d \in \operatorname{Im}\beta^0$.

Ahora para el siguiente tramo se tiene $\operatorname{Im}\delta^0 \subset \operatorname{Ker}\alpha^1$ por definición ($\delta^0(d) = a_\sigma$ tal que $\alpha(a_\sigma) = \alpha^1(a_\sigma) = b(\sigma b^{-1}) \in B^1(G,B)$). Para la inclusión contraria basta observar que si $a_\sigma \in H^1(G,A)$ con $\alpha^1(a_\sigma) = b(\sigma b^{-1})$ para un $b \in B$, entonces $\beta(b(\sigma b^{-1})) = \beta(\alpha^1(a_\sigma)) = 1$ y por lo tanto $\beta(b) \in D^G$ y $a_\sigma \in \operatorname{Im}\delta^0$.

En el tramo de los H^1 se tiene $\operatorname{Im}\alpha^1 \subseteq \operatorname{Ker}\beta^1$ por la exactitud de la sucesión original ($\beta\circ\alpha = 1$). Para la inclusión contraria sea $b \in Z^1(G,B)$, $b : G \to B$ tal que $\beta^1(b_\sigma) = d(\sigma d^{-1})$ para un $d \in D$. Como $\beta : B \to D$ es sobreyectiva existe $b_0 \in B$ tal que $\beta(b_0) = d$. Consideremos ahora $b' : G \to B$, $b'_\sigma = b_\sigma b_0^{-1}(\sigma b_0)$, que pertenece a la misma clase en $H^1(G,B)$ que b. Se cumple

$$\beta(b'_\sigma) = \beta(b_\sigma)\beta(b_0^{-1}(\sigma b_0)) = \beta(b_\sigma)(d(\sigma d^{-1})^{-1} = 1,$$

luego por la exactitud de la sucesión original, para todo $\sigma \in G$ existe $a_\sigma \in A$ tal que $\alpha(a_\sigma) = b'_\sigma$. Además, como $\alpha(a_{\sigma\tau}) = b'_{\sigma\tau}$ y $\alpha : A \to B$ es inyectiva, la aplicación $a : G \to A$, $\sigma \mapsto a_\sigma$ es un homomorfismo cruzado. Por tanto $[b] = [b'] = [\alpha^1(a)]$ y $[b] \in \operatorname{Im}\beta^1$.

El paso de H^1 a H^2 depende de δ^1. Primero veamos que $\operatorname{Im}\beta^1 = \operatorname{Ker}\delta^1$. La primera inclusión de tiene viendo que $\delta^1(\beta^1(b_\sigma)) = c_{\sigma,\tau}$ tal que $\alpha(c_{\sigma\tau}) = b_\sigma(\sigma b_\tau)b_{\sigma\tau}^{-1}$ (el levantamiento es el propio b_σ) y por la propiedad de los homomorfismos cruzados $b_\sigma(\sigma b_\tau)b_{\sigma\tau}^{-1} = b_{\sigma\tau}b_{\sigma\tau}^{-1} = 1$. Para inclusión contraria si $\delta^1(d) = [1]$ entonces existe $c \in Z^2(G, A)$ tal que

$$b_\sigma(\sigma b_\tau)b_{\sigma\tau}^{-1} = \alpha(c_{\sigma\tau}) = \alpha(a_\sigma)(\sigma\alpha(a_\tau))\alpha(a_{\sigma\tau}^{-1})$$

con $\beta(b_\sigma) = d_\sigma$. Por lo tanto $b_\sigma\tau\alpha(a_\sigma\tau) = b_\sigma\alpha(a_\sigma^{-1})(\sigma b_\tau\alpha(a_\tau^{-1}))$ y tenemos un homomorfismo cruzado $G \to B$, $\sigma \mapsto b_\sigma\alpha(a_\sigma^{-1})$ tal que $\beta^1(b_\sigma\alpha(a_\sigma^{-1}) = \beta^1(b_\sigma) = d_\sigma$. Por lo tanto $d_\sigma \in \operatorname{Im}\beta^1$.

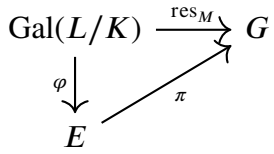
Ahora veamos que $\operatorname{Im}\delta^1 = \operatorname{Ker}\alpha^2$. La inclusión $\operatorname{Im}\delta^1 \subseteq \operatorname{Ker}\alpha^2$ se tiene por definición, $c_{\sigma\tau} \in \operatorname{Im}\delta^1$ si $\alpha(c_{\sigma\tau}) \in B^2(G, B)$. Para la otra inclusión consideremos $c_{\sigma\tau} \in Z^2(G, A)$ tal que $\alpha(c_{\sigma\tau)} \in B^2(G, B)$, es decir existe $b_\sigma : G \to B$ tal que $\alpha(c_{\sigma\tau}) = b_\sigma(\sigma b_\tau)b_{\sigma\tau}^{-1}$. Como $\beta\circ\alpha = 1$ entonces $\beta(b_{\sigma\tau}) = \beta(b_\sigma)(\sigma\beta(b_\tau))$ y por lo tanto $d_\sigma = \beta(b_\sigma)$ es un elemento de $Z^1(G, D)$ tal que $\delta^1(d_\sigma) = c_{\sigma\tau}$.

Por último en el tramo de los H^2 se procede igual que en de los H^1. ∎

2 El problema de inmersión

2.1 Planteamiento del problema

Dados un cuerpo K, una extensión de Galois M/K con $\mathrm{Gal}(M/K) = G$ y $\pi : E \to G$ un epimorfismo de un grupo finito E en G, el problema de inmersión consiste en encontrar una extensión L/K con $M \subseteq L$ y un isomorfismo $\varphi : \mathrm{Gal}(L/K) \to E$ tal que el siguiente diagrama conmute:



es decir, $\pi \circ \varphi = \mathrm{res}_M$ donde $\mathrm{res}_M : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ es la restricción canónica.

Si denotamos por N el núcleo de π, podemos ver el epimorfismo $\pi : E \to G$ como una extensión de grupos

$$1 \to N \to E \xrightarrow{\pi} G \to 1,$$

y por tanto tiene asociada una clase de cohomología $\gamma \in H^2(G, N)$. Denotaremos a dicho problema de inmersión por $(M/K, E, \pi)$ o $(M/K, E, \pi, N)$ y llamaremos **solución** del problema al par (L, φ) satisfaciendo lo exigido.

Dado un problema de inmersión $(M/K, E, \pi)$, si relajamos las condiciones de φ, en particular la de que φ sea un isomorfismo, tenemos dos casos a destacar:

1. Si tenemos una extensión L/K y un homomorfismo inyectivo $\varphi : \mathrm{Gal}(L/K) \to E$ tal que $\pi \circ \varphi = \mathrm{res}_M$, diremos que (L, φ) es una **solución débil**. De por sí

no tienen mayor utilidad que en los casos en los que una solución débil es una solución.

2. Si tenemos una extensión L/K y un homomorfismo sobreyectivo $\varphi : E \to \mathrm{Gal}(L/K)$ tal que $\mathrm{res}_M \circ \varphi = \pi$, podemos plantear un nuevo problema de inmersión $(L/K, E, \varphi)$.

2.2 Problemas de tipo Brauer

Vamos a ver un caso concreto del problema de inmersión. Entre otras cosas vamos a trabajar con núcleo cíclico, por lo que vamos a necesitar varios resultados auxiliares sobre extensiones de Galois cíclicas.

Observación 2.1. En el anterior capítulo hemos dicho que un homomorfismo cruzado $f : G \to A$ era principal si existía $a \in A$ tal que $f(\sigma) = a(\sigma a^{-1})$ para todo $\sigma \in G$. Es obvio, tomando $b = a^{-1}$ y dado que A es abeliano, que esto es equivalente a decir que existe $b \in A$ tal que $f(\sigma) = (\sigma b)b^{-1}$ para todo $\sigma \in G$. En este capítulo utilizaremos normalmente la notación de $\sigma b/b$ para los homomorfismos cruzados principales, más natural al trabajar con cuerpos y el Teorema 90 de Hilbert.

Lema 2.1.

1. Sea M/K una extensión cíclica de grado n y σ un generador de $G = \mathrm{Gal}(M/K)$. Entonces $a \in M^*$ tiene norma 1 si y sólo si $a = \sigma x/x$ para un $x \in M^*$.
2. Sea K un cuerpo y $n \in \mathbb{N}$ tal que la característica de K no divide a n y $\mu_n \subseteq K^*$. Entonces cualquier extensión cíclica M/K de grado n es de la forma $M = K(\sqrt[n]{a})$ para un $a \in K^*$, y si $\zeta \in \mu_n \subseteq K^*$ es primitiva, un generador de $\mathrm{Gal}(M/K)$ es aquel que manda $\sqrt[n]{a}$ en $\zeta\sqrt[n]{a}$. Recíprocamente, $K(\sqrt[n]{a})/K, a \in K$ es una extensión cíclica de grado un divisor de n.

Demostración. 1) Supongamos que $a = \sigma x/x$ para un $x \in M^*$. Entonces como G es cíclico de grado n y σ es un generador,

$$N_G\left(\frac{\sigma x}{x}\right) = \prod_{i=1}^{n} \sigma^i\left(\frac{\sigma x}{x}\right) = \prod_{i=1}^{n} \frac{\sigma^{i+1}x}{\sigma^i x} = 1.$$

Recíprocamente sea $a \in M^*$ con norma 1. Entonces la aplicación $f : G \to M^*$, $f(\sigma^i) = a(\sigma a)\cdots(\sigma^{i-1}a)$ está bien definida $f(\sigma^{kn+i}) = f(\sigma^i)$ por tener a norma 1) y

verifica que

$$\begin{aligned} f(\sigma^i\sigma^j) &= a(\sigma a)\cdots(\sigma^{i-1}a)(\sigma^i a)\cdots(\sigma^{i+j-1}a) \\ &= a(\sigma a)\cdots(\sigma^{i-1}a)(\sigma^i(a(\sigma a)\cdots(\sigma^{j-1}a))) \\ &= f(\sigma^i)(\sigma^i f(\sigma^j)). \end{aligned}$$

luego es un homomorfismo cruzado y por el Teorema 90 de Hilbert es principal, luego $f(\sigma^i) = \sigma^i x/x$ para algún $x \in M^*$. En particular $a = f(\sigma) = \sigma x/x$.

2) Sea $\sigma \in \mathrm{Gal}(M/K)$ un generador y $\zeta \in \mu_n$ primitiva. Entonces como $\zeta \in \mu_n$ tiene norma 1 ($\sigma(\zeta) = \zeta$, luego $N_G(\zeta) = \zeta^n = 1$), por el apartado anterior existe $\theta \in M^*$ tal que $\zeta = \sigma\theta/\theta$ y por lo tanto $\sigma(\theta) = \zeta\theta$. Además $(\sigma(\theta)/\theta)^n = \zeta^n = 1$, luego $\sigma(\theta^n) = \theta^n$ y $\theta^n \in K$, luego podemos escribir $\theta = \sqrt[n]{a}$, $a \in K$, y $\sigma(\sqrt[n]{a}) = \zeta\sqrt[n]{a}$. Si consideramos el polinomio $f(x) = x^n - a$, tiene como raíces a $\{\theta, \zeta\theta, \dots, \zeta^{n-1}\theta\} = \{\theta, \sigma(\theta)\dots, \sigma^{n-1}(\theta)\}$ que son todas distintas. Consideremos la extensión $K(\theta)$ y supongamos que $K(\theta) \neq M$, entonces la extensión $M/K(\theta)$ es no trivial y existe un $j \in \{1, \dots, n-1\}$ tal que $\sigma^j \in \mathrm{Gal}(M/K(\theta))$. Pero entonces $\sigma^j(\theta) = \theta$, una contradicción (tendríamos dos raíces iguales de f). Por lo tanto $K(\theta) = M$.

Recíprocamente consideremos la extensión $K(\sqrt[n]{a})/K$, $a \in K$. Como $\mu_n \subseteq K$, y las raíces de $f(x) = x^n - a$ son de la forma $\zeta\sqrt[n]{a}$, $\zeta \in \mu_n$, y su cuerpo de descomposición es $K(\sqrt[n]{a})$ luego la extensión $K(\sqrt[n]{a})/K$ es de Galois. Consideremos el homomorfismo $\mathrm{Gal}(K(\sqrt[n]{a})/K) \to \mu_n$, $\tau \mapsto \tau(\sqrt[n]{a})/\sqrt[n]{a}$. Dicho homomorfismo es inyectivo y por lo tanto tenemos que $\mathrm{Gal}(K(\sqrt[n]{a})/K)$ es isomorfo a un subgrupo de μ_n, luego es cíclico de grado un divisor de n. ∎

Lema 2.2. Sea K un cuerpo, $n \in \mathbb{N}$ tal que la característica de K no lo divide y $\mu_n \subseteq K^*$ (donde μ denota el grupo de las raíces n-ésimas de la unidad). Supongamos que M/K con $M = K(\sqrt[n]{a})$ para un $a \in K^*$ es una extensión cíclica de grado n. Entonces los únicos $\theta \in M$ con $\theta^n \in K$ son aquellos de la forma $\theta = x(\sqrt[n]{a})^j$ con $x \in K$ y $j \in \{0, 1 \dots, n-1\}$.

Demostración. Únicamente tenemos que probar una dirección. Sea $\alpha = \sqrt[n]{a}$ y consideremos el polinomio $m_\alpha(x) = x^n - a$, que al ser mónico, de grado n y anularse en α es su polinomio mínimo. Entonces $\{1, \alpha, \dots, \alpha^{n-1}\}$ es una base de $K(\alpha)/K$ y dado $\theta \in K(\alpha)$ podemos escribir $\theta = \lambda_0 + \lambda_1\alpha + \cdots + \lambda_{n-1}\alpha^{n-1}$ para $\lambda_0, \dots, \lambda_{n-1} \in K$.

Como $G = \mathrm{Gal}(M/K)$ es cíclico podemos tomar un generador σ de G. Se tiene que $\sigma(\alpha)$ es otra raíz de $m_\alpha(x)$, que es de la forma $\sigma(\alpha) = \zeta\alpha$ con $\zeta \in \mu_n$ y además es primitiva por ser σ generador.

Sea ahora $b = \theta^n$ y supongamos que $b \in K$. Entonces θ es raíz del polinomio $f(x) = x^n - b \in K[x]$, y $\sigma(\theta)$ es otra raíz de la forma $\sigma(\theta) = \zeta^j\theta$ con $j \in \{0, 1 \dots, n-1\}$. Se cumple la siguiente igualdad

$$\sigma(\theta) = \sum_{i=0}^{n-1} \lambda_i \sigma(\alpha)^i = \sum_{i=0}^{n-1} \lambda_i \zeta^i \alpha^i = \zeta^j \theta = \zeta^j \sum_{i=0}^{n-1} \lambda_i \alpha^i = \sum_{i=0}^{n-1} \lambda_i \zeta^j \alpha^i.$$

Tenemos entonces

$$\sum_{i=0}^{n-1} (\zeta^i - \zeta^j)\lambda_i \alpha^i = 0$$

y como $\{1, \alpha, \dots, \alpha^{n-1}\}$ es una base de M como K-espacio vectorial, $\zeta^i \lambda_i = \zeta^j \lambda_i$ para todo $i = 0, \dots, n-1$ y $\lambda_i = 0$ si $i \neq j$. Por lo tanto $\theta = \lambda_j \alpha^j$, con $j \in \{0, 1 \dots, n-1\}$ y $\lambda_j \in K$.

Lema 2.3. Sea M/K una extensión de Galois, $G = \mathrm{Gal}(M/K)$ y $n \in \mathbb{N}$ tal que la característica de K no divide a n y $\mu_n \subseteq M^*$. Sea $a \in M^*$. Entonces $M(\sqrt[n]{a})/K$ es una extensión de Galois si y sólo si para cada $\sigma \in G$ existe i_σ coprimo con n tal que $\sigma(a)/a^{i_\sigma}$ es una n-ésima potencia en M.

Demostración. Supongamos primero que $M(\sqrt[n]{a})/K$ es de Galois, entonces $M(\sqrt[n]{a})/M$ también lo es. Tomemos $\sigma \in G$, y sea $\tilde{\sigma} \in \mathrm{Gal}(M(\sqrt[n]{a})/K)$ tal que $\tilde{\sigma}|_G = \sigma$. Sea $\alpha := \sqrt[n]{a}$, entonces $\sigma(a) = \sigma(\alpha^n) = \tilde{\sigma}(\alpha^n) = \tilde{\sigma}(\alpha)^n$. Entonces $\tilde{\sigma}(\alpha) \in M(\alpha)$ y $(\tilde{\sigma}(\alpha))^n \in M$ y podemos aplicar el lema anterior para obtener $\tilde{\sigma}(\alpha) = x\sqrt[n]{a}^j$ con $x \in M$ y $j \in \{0, \dots, n-1\}$. Por lo tanto $\sigma(a) = \tilde{\sigma}(\alpha)^n = x^n a^j$ tal y como queríamos. Faltaría por ver que j y n son coprimos. Supongamos que no, y sea $n = jk$, $k \geq 2$. Entonces el polinomio mínimo de α^j es $m_{\alpha^j}(x) = x^k - a$, de grado $k < n$, mientras que el de α es $m_\alpha(x) = x^n - \alpha$ como hemos visto anteriormente. Sin embargo $M(\alpha^j) = M(\alpha)$ pero $[M(\alpha) : M] = n$ y $[M(\alpha^j) : M] = k < n$ lo cual es una contradicción.

Recíprocamente, supongamos que para todo $\sigma \in G$ existe un i_σ coprimo con n tal que $\sigma(a)/a^{i_\sigma}$ es una potencia n-ésima en M. De nuevo sea $\alpha = \sqrt[n]{a}$; nuestro objetivo es probar que $M(\alpha)/K$ es de Galois. Sea $m_\alpha(x) \in K[x]$ el polinomio mínimo de α, $\tilde{M}$ el cuerpo de descomposición de $m_\alpha(x)$ y β otra raíz del mismo. Nuestro objetivo es probar que $\tilde{M} = M(\alpha)$ (y por lo tanto $M(\alpha)/K$ es de Galois). Como α y β son raíces de $m_\alpha(x)$, existe $\tilde{\sigma} \in \mathrm{Gal}(\tilde{M}/K)$ tal que $\tilde{\sigma}(\alpha) = \beta$.

Sea ahora $\sigma = \tilde{\sigma}|_M \in \mathrm{Gal}(M/K)$. Se cumple que $\alpha^n - a = 0$ luego

$$0 = \tilde{\sigma}(\alpha)^n - \tilde{\sigma}(a) = \beta^n - \sigma(a).$$

Por hipótesis existe i_σ comprimo con n tal que $\sigma(a)/a^{i_\sigma} = x^n$ para un $x \in M$. Entonces

$$(\beta/\alpha^{i_\sigma})^n = \sigma(a)/a^{i_\sigma} = x^n$$

y tenemos que para un $\zeta \in \mu_n$, $\beta = \zeta x \alpha^{i_\sigma} \in M(\alpha)$. Por lo tanto $\tilde{M} = M(\alpha)$ y $M(\alpha)/K$ es de Galois.

Con estos resultados podemos introducir las extensiones de tipo Brauer, que son las de la forma del teorema a continuación.

Teorema 2.1. *Sea K un cuerpo y M/K una extensión de Galois con grupo de Galois $G = \mathrm{Gal}(M/K)$. Sea $m \in \mathbb{N}$ tal que la característica de K no divide a m y $\mu_m \subseteq M^*$. Entonces μ_n es un G-módulo mediante la acción de G como grupo de Galois. Consideremos la extensión de G con el G-módulo μ_m dada por*

$$1 \to \mu_m \to E \xrightarrow{\pi} G \to 1,$$

con clase de cohomología $\gamma \in H^2(G, \mu_m)$. Entonces el problema de inmersión $(M/K, G, \pi, \mu_m)$ es débilmente resoluble si y sólo si $i^*(\gamma) = 1$, donde $i^* : H^2(G, \mu_m) \to H^2(G, M^*)$ es el homomorfismo inducido por la inclusión $\mu_m \subseteq M^*$. Además, si $M(\sqrt[m]{\omega})/K$, $\omega \in M^*$ es una solución débil, entonces todas las soluciones débiles son de la forma $M(\sqrt[m]{r\omega})/K$, $r \in K^*$.

Demostración. Empecemos suponiendo $i^*(\gamma) = 1$. Sea $c \in Z^2(G, \mu_m)$ un representante de γ. Entonces

$$i^*(c_{\sigma,\tau}) = a_\sigma(\sigma a_\tau)a_{\sigma\tau}^{-1}$$

para cierta aplicación $a : G \to M^*$. Como $c : G \times G \to \mu_m$, se tiene que $c_{\sigma,\tau}^m = 1$, luego $i^*(c_{\sigma,\tau})^m = 1$ y la aplicación $\sigma \mapsto a_\sigma^m$ es un homomorfismo cruzado $G \to M^*$. Por el Teorema 90 de Hilbert existe $\omega \in M^*$ tal que $\sigma(\omega)/\omega = a_\sigma^m$ para todo $\sigma \in G$. Por lo tanto estamos en las condiciones de aplicar el Lema 2.3 y tenemos que $M(\sqrt[m]{\omega})/K$ es de Galois. Nuestro objetivo va a ser probar que $M(\sqrt[m]{\omega})/K$ es una solución débil.

Como $M(\sqrt[m]{\omega})/K$ es de Galois, dado $\sigma \in G$ podemos extenderlo a $\tilde{\sigma} \in \mathrm{Gal}(M(\sqrt[m]{\omega})/K)$ mediante

$$\tilde{\sigma}(\sqrt[m]{\omega}) = \zeta_\sigma a_\sigma \sqrt[m]{\omega}$$

donde $\zeta_\sigma \in \mu_m$. Se cumple $\tilde{\sigma}(\sqrt[m]{\omega})^m = \zeta_\sigma^m a_\sigma^m (\sqrt[m]{\omega})^m = \sigma(\omega)$ y está bien definido. Sea $b_\sigma = \zeta_\sigma a_\sigma$ y $\kappa \in Gal(M(\sqrt[m]{\omega})/M)$ (y por tanto también en $\mathrm{Gal}(M(\sqrt[m]{\omega})/K)$). Se cumple que $\kappa(\sqrt[m]{\omega}) = \zeta \sqrt[n]{\omega}$ para $\zeta \in \mu_m$, luego

$$\tilde{\sigma}\kappa(\sqrt[m]{\omega}) = \tilde{\sigma}(\zeta \sqrt[m]{\omega}) = \zeta^{e_\sigma} b_\sigma \sqrt[m]{\omega} = \kappa^{e_\sigma}(b_\sigma \sqrt[m]{\omega}) = \kappa^{e_\sigma}\tilde{\sigma}(\sqrt[m]{\omega}).$$

Donde $\zeta^{e_\sigma} = \tilde{\sigma}(\zeta) = \sigma(\zeta)$. Entonces, como por el Lema 2.1 (2), $M(\sqrt[m]{\omega})/M$ es una extensión cíclica de grado d divisor de m es isomorfa a μ_d, y además como G-módulo. Tenemos por tanto la siguiente extensión

$$1 \to \mu_d \xrightarrow{\zeta \mapsto \kappa} \mathrm{Gal}(M(\sqrt[m]{\omega})/K) \xrightarrow{res_M} G \to 1$$

de G con el G-módulo μ_d. Calculemos su clase de cohomología, para lo cual tomemos $\tilde{\sigma}, \tilde{\tau} \in \mathrm{Gal}(M(\sqrt[m]{\omega})/K)$ tales que $\tilde{\sigma}|_M = \sigma$ y $\tilde{\tau}|_M = \tau$. Entonces:

$$\begin{aligned}
\tilde{\sigma}\tilde{\tau}(\sqrt[m]{\omega}) &= \tilde{\sigma}(b_\tau \sqrt[m]{\omega}) = \tilde{\sigma}(b_\tau) b_\sigma \sqrt[m]{\omega} = b_\sigma(\sigma b_\tau)\sqrt[m]{\omega} \\
&= \zeta_\sigma a_\sigma(\sigma\zeta_\tau a_\tau)\sqrt[m]{\omega} = \zeta_\sigma(\sigma\zeta_\tau)a_\sigma(\sigma a_\tau)a_{\sigma\tau}^{-1}a_{\sigma\tau}\sqrt[m]{\omega} \\
&= \zeta_\sigma\zeta_\tau c_{\sigma,\tau}a_{\sigma\tau}\sqrt[m]{\omega} = \zeta_\sigma(\sigma\zeta_\tau)\zeta_{\sigma\tau}^{-1}c_{\sigma,\tau}b_{\sigma\tau}\sqrt[m]{\omega} \\
&= (\zeta_\sigma(\sigma\zeta_\tau)\zeta_{\sigma\tau}^{-1})c_{\sigma,\tau}\widetilde{\sigma\tau}(\sqrt[m]{\omega}).
\end{aligned}$$

y por lo tanto la clase de cohomología de la extensión viene tiene como representante al sistema de factores $c' \in Z^2(G, \mu_d)$,

$$c'_{\sigma,\tau} = (\zeta_\sigma(\sigma\zeta_\tau)\zeta_{\sigma\tau}^{-1})c_{\sigma,\tau}.$$

Si consideramos dicho sistema de factores en $Z^2(G, \mu_m)$ (mediante la inclusión $\mu_d \subseteq \mu_m$), es equivalente a $c_{\sigma,\tau}$, el representante que elegimos de γ. Entonces tenemos el siguiente diagrama tativo,

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_d & \longrightarrow & \mathrm{Gal}(M(\sqrt[m]{\omega})/K) & \xrightarrow{\mathrm{res}_M} & G & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle f} & & \| & & \\
1 & \longrightarrow & \mu_m & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \\
 & & \| & & \downarrow{\scriptstyle h} & & \| & & \\
1 & \longrightarrow & \mu_m & \longrightarrow & E & \xrightarrow{\pi} & G & \longrightarrow & 1
\end{array}$$

donde la primera fila viene dada por el homomorfismo $H^2(G, \mu_d) \to H^2(G, \mu_m)$ inducido por la inclusión $\mu_d \hookrightarrow \mu_m$ (como vimos en la sección 1.4.1) y la segunda, por la equivalencia de extensiones con misma clase de cohomología. Por conmutatividad de la primera fila, f es inyectivo, y por equivalencia de extensiones h es un isomorfismo, luego $\varphi : \mathrm{Gal}(M(\sqrt[m]{\omega}/K) \to E$ dada por $\varphi = h \circ f$ es inyectiva y verifica que $\pi \circ \varphi = \mathrm{res}_M$. Por lo tanto tenemos que $(M(\sqrt[m]{\omega}), \varphi)$ es una solución débil.

Recíprocamente supongamos que tenemos una solución débil $(L/K, \varphi)$. Entonces tenemos el siguiente diagrama conmutativo

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(L/M) & \longrightarrow & \mathrm{Gal}(L/K) & \xrightarrow{\mathrm{res}_M} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \varphi} & & \| & & \\ 1 & \longrightarrow & \mu_m & \longrightarrow & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \end{array}$$

donde f ha de ser inyectiva por conmutatividad. Entonces $\mathrm{Gal}(L/M)$ es cíclico de grado $d|n$ y por el Lema 2.1 (con $n = d$) $L = M(\sqrt[d]{\theta})$, $\theta \in M^*$. Ahora como d es un divisor de m, $m = dk$ para un cierto k y podemos escribir $\sqrt[d]{\theta}$ como $\sqrt[m]{\omega}$ con $\omega = \theta^k \in M^*$. Por lo tanto $L = M(\sqrt[m]{\omega})$, $\omega \in M^*$. Identificando entonces $\mathrm{Gal}(M\sqrt[m]{\omega})/M)$ con μ_d como antes, tenemos de nuevo un diagrama conmutativo,

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_d & \xrightarrow{\alpha} & \mathrm{Gal}(M(\sqrt[m]{\omega})/K) & \xrightarrow{\mathrm{res}_M} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle \varphi} & & \| & & \\ 1 & \longrightarrow & \mu_m & \xrightarrow{\beta} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \end{array}$$

donde $\alpha(\zeta) = \tilde{\sigma}$, $\tilde{\sigma}(\sqrt[m]{\omega}) = \zeta\sqrt[m]{\omega}$ y $\tilde{\sigma}|_M = \mathrm{id}_M$, y $g(\zeta) = \zeta^h$, $h \in \mathbb{Z}$ coprimo con m por inyectividad (si no, $\zeta^h = 1$).

Primero de todo, como $M(\sqrt[m]{\omega})/K$ es Galois podemos aplicar el Lema 2.3 y por tanto $\sigma\omega/\omega^{i_\sigma} = x^m$ para cierto $x \in M^*$ e i_σ coprimo con m. Más aún, veamos que $i_\sigma = 1$. Sea j_σ el inverso módulo m, $\sigma \in G$, $\tilde{\sigma} \in \mathrm{Gal}(M(\sqrt[m]{\omega})/K)$ tal que $\tilde{\sigma}|_M = \sigma$, que podemos tomar como $\tilde{\sigma}(\sqrt[m]{\omega}) = \eta x\sqrt[m]{\omega}^{i_\sigma}$, $\eta \in \mu_m$; $\zeta \in \mu_d$ y $\tau \in \mathrm{Gal}(M(\sqrt[m]{\omega})/K)$ la imagen de ζ por α. Para calcular la acción de G tenemos que calcular $(\tilde{\sigma}\circ\tau\circ\tilde{\sigma}^{-1})(\sqrt[m]{\omega})$. Para ello primero veamos la forma de $\tilde{\sigma}^{-1}$. Tenemos que

$$\tilde{\sigma}(\sqrt[m]{\omega}) = \eta x\sqrt[m]{\omega}^{i_\sigma}$$

luego

$$\sqrt[m]{\omega} = \tilde{\sigma}^{-1}(\eta x\sqrt[m]{\omega}^{i_\sigma}); \quad \tilde{\sigma}^{-1}(\sqrt[m]{\omega}) = \tilde{\sigma}^{-1}(\eta x)^{-j_\sigma}\sqrt[m]{\omega}^{j_\sigma}.$$

Finalmente podemos hacer el cálculo explícito:

$$\begin{aligned} (\tilde{\sigma}\circ\tau\circ\tilde{\sigma}^{-1})(\sqrt[m]{\omega}) &= (\tilde{\sigma}\circ\tau)(\tilde{\sigma}^{-1}(\eta x)^{-j_\sigma}\sqrt[m]{\omega}^{j_\sigma}) \\ &= \tilde{\sigma}(\tilde{\sigma}^{-1}(\eta x)^{-j_\sigma}\zeta^{j_\sigma}\sqrt[m]{\omega}^{j_\sigma}) \\ &= (\eta x)^{-j_\sigma}\tilde{\sigma}(\zeta\sqrt[m]{\omega})^{j_\sigma} \\ &= (\eta x)^{-j_\sigma}(\eta x)^{j_\sigma}\tilde{\sigma}(\zeta)^{j_\sigma}(\sqrt[m]{\omega}^{i_\sigma})^{j_\sigma} \\ &= \sigma(\zeta)^{j_\sigma}\sqrt[m]{\omega}. \end{aligned}$$

Es decir la acción inducida por la extensión es $\alpha(\sigma\zeta) = \rho$, donde $\rho \in \mathrm{Gal}(M(\sqrt[m]{\omega})/K)$ tal que $\rho(\sqrt[m]{\omega}) = \sigma(\zeta)^{j_\sigma}\sqrt[m]{\omega}$ y la identidad en M, luego $\sigma\zeta = \sigma(\zeta)^{j_\sigma}$ Sin embargo, dicha acción sabemos que debe coincidir con la natural, $\sigma\zeta = \sigma(\zeta)$, luego $j_\sigma \equiv i_\sigma \equiv 1$ (mód m) e $i_\sigma = 1$ (recordemos que i_σ y m eran coprimos). Con esto tenemos que existe un $a_\sigma \in M^*$ tal que $\sigma\omega/\omega = a_\sigma^m$. Además podemos suponer que $\tilde{\sigma}(\sqrt[m]{\omega})/\sqrt[m]{\omega} = a_\sigma$ y tenemos definida una aplicación $a : G \to M^*$.

Sea ahora $s : G \to E$ una sección tal que $\mathrm{Im}\, s \subseteq \mathrm{Im}\, \varphi$, que da lugar a una sección $s' : G \to \mathrm{Gal}(M(\sqrt[m]{\omega})/K)$, $s'(\sigma) = \varphi^{-1}(s(\sigma))$. Por conmutatividad, la imagen por g de $c' \in Z^2(G, \mu_d)$ dada por s' coincide con el representante de $\gamma \in H^2(G, \mu_m)$ dado por la sección s, luego es a su vez un representante de γ. Vamos a calcular dicho representante explícitamente.

Necesitamos tomar $\tilde{\sigma}, \tilde{\tau} \in \mathrm{Gal}(M(\sqrt[m]{\omega})/K)$ tales que $\tilde{\sigma}|_M = \sigma$ y $\tilde{\tau}|_M = \tau$, y queremos calcular $(\tilde{\sigma}\circ\tilde{\tau}\circ\widetilde{\sigma\tau}^{-1})(\sqrt[m]{\omega})$ Igual que antes primero veamos que forma tiene $\widetilde{\sigma\tau}^{-1}$. Sabemos que $\widetilde{\sigma\tau}(\sqrt[m]{\omega}) = a_{\sigma\tau}\sqrt[m]{\omega}$, luego

$$\widetilde{\sigma\tau}^{-1}(\sqrt[m]{\omega}) = \widetilde{\sigma\tau}^{-1}(a_{\sigma\tau}^{-1})\sqrt[m]{\omega}$$

Con esto podemos continuar y:

$$\begin{aligned}
(\tilde{\sigma}\circ\tilde{\tau}\circ\widetilde{\sigma\tau}^{-1})(\sqrt[m]{\omega}) &= (\tilde{\sigma}\circ\tilde{\tau})(\widetilde{\sigma\tau}^{-1}(a_{\sigma\tau}^{-1})\sqrt[m]{\omega}) \\
&= (\tilde{\sigma}\circ\tilde{\tau})((\tilde{\tau}^{-1}\circ\tilde{\sigma}^{-1})(a_{\sigma\tau}^{-1})\sqrt[m]{\omega}) \\
&= \tilde{\sigma}(\tilde{\sigma}^{-1}(a_{\sigma\tau}^{-1})\tilde{\tau}(\sqrt[m]{\omega})) \\
&= \tilde{\sigma}(\tilde{\sigma}^{-1}(a_{\sigma\tau}^{-1})a_\tau\sqrt[m]{\omega}) \\
&= a_{\sigma\tau}^{-1}\tilde{\sigma}(a_\tau)a_\sigma\sqrt[m]{\omega}) \\
&= a_\sigma(\sigma a_\tau)a_{\sigma\tau}^{-1}\sqrt[m]{\omega}.
\end{aligned}$$

Tenemos que $c'_{\sigma\tau} = \zeta'$ con $\alpha(\zeta') = \rho$ siendo $\rho|_M = \mathrm{id}_M$ y $\rho(\sqrt[m]{\omega}) = a_\sigma(\sigma a_\tau)a_{\sigma\tau}^{-1}\sqrt[m]{\omega}$. Como hemos comentado antes, $\zeta \in \mu_m$ tal que $\beta(\zeta) = \varphi(\alpha(\rho))$ es un representante de γ, que por conmutatividad es $\zeta = g(\zeta') = (a_\sigma(\sigma a_\tau)a_{\sigma\tau}^{-1})^h$. Esto visto en M^* es un elemento de $B^2(G, M^*)$ y por lo tanto $i^*(\gamma) = 1$ tal como queríamos.

Finalmente demostremos la última parte del teorema. Sea $M(\sqrt[m]{\lambda})/K$, $\lambda \in M^*$ otra solución débil (hemos visto que toda solución débil L/K tiene que ser de esta forma). Repitiendo los argumentos anteriores $\sigma\lambda/\lambda = b_\sigma^p$ y

$$c''_{\sigma\tau} = (b_\sigma(\sigma b_\tau)b_{\sigma\tau}^{-1})^k$$

es un representante de γ. Tanto $c'_{\sigma\tau}$ como $c''_{\sigma\tau}$ pertenecen a μ_m luego multiplicando a_σ y b_σ por los elementos de μ_m adecuados podemos suponer $c' = c''$. Entonces $\sigma \mapsto b_\sigma^k / a_\sigma^h$ verifica que

$$b_{\sigma\tau}^k a_{\sigma\tau}^{-h} = (b_\sigma(\sigma b_\tau))^k (a_\sigma(\sigma a_\tau))^h = b_\sigma^k a_\sigma^h (\sigma b_\tau^k a_\tau^h)$$

y por tanto es un homomorfismo cruzado $G \to M^*$. Por el Teorema 90 de Hilbert, existe $x \in M^*$ tal que $\sigma x / x = b_\sigma^k / a_\sigma^h$ para todo $\sigma \in G$. Por lo tanto

$$\frac{\sigma\lambda^k}{\lambda^k} = b_\sigma^{mk} = \frac{\sigma x^m}{x^m} a_\sigma^m h = \frac{\sigma(x^m \omega^h)}{x^m \omega^h}$$

y por lo tanto $\lambda^k = s x^m \omega^h$ para algún $s \in K^*$. Por lo tanto (recordemos que k y h son coprimos con m):

$$M(\sqrt[m]{\lambda}) = M(\sqrt[m]{\lambda^k}) = M(\sqrt[m]{s x^m \omega^h}) = M(\sqrt[m]{s\omega^h}) = M(\sqrt[m]{r\omega}$$

donde $r = s^j$ siendo j el inverso de h módulo m. Por lo tanto todas las soluciones son de la forma $M(\sqrt[m]{r\omega})/K$ para cierto $r \in K^*$.

Este teorema (y las soluciones débiles) nos son útiles en los casos en los que a la fuerza una solución débil ha de ser una solución. En particular reforzando las hipótesis del teorema obtenemos el siguiente resultado:

Corolario 2.1. Sea M/K una extensión de Galois con grupo de Galois $G = \mathrm{Gal}(M/K)$, y p un primo distinto de la característica de K y tal que $\mu_p \subseteq K^*$. Sea

$$1 \to \mu_p \to E \xrightarrow{\pi} G \to 1$$

una extensión central con clase de cohomología no trivial $\gamma \in H^2(G, \mu_p)$ (es decir que no escinde). Entonces el problema de inmersión $(M/K, E, \pi, \mu_p)$ es resoluble si y sólo si $i^*(\gamma) = 1$, donde $i^* : H^2(G, \mu_p) \to H^2(G, M^*)$ es el homomorfismo inducido por la inclusión $\mu_p \subseteq K^* \subseteq M^*$. Más aún, si $M(\sqrt[p]{\omega})/K$, $\omega \in M^*$ es una solución, todas las soluciones son de la forma $M(\sqrt[m]{r\omega})/K$, $r \in K^*$.

Demostración. Si $M(\sqrt[m]{\omega})/K, \omega \in M^*$ es una solución, en particular es una solución débil y por tanto por el teorema anterior $i^*(\gamma) = 1$.

Supongamos ahora que $i^*(\gamma) = 1$. Observando la prueba del teorema, identificábamos $\mathrm{Gal}(M(\sqrt[m]{\omega})/M)$ con μ_d, d dividiendo a m. Ahora $m = p$ es primo luego $d = 1$ o $d = p$. Si d fuese 1 la extensión sería trivial y nuestro homomorfismo $\varphi : \mathrm{Gal}(M/K) \to E$ sería una sección, luego la extensión escindiría (contradicción). Entonces $d = p$ y el homomorfismo inyectivo φ de la solución débil es una equivalencia de extensiones, y por tanto un isomorfismo.

Bajo las mismas hipótesis, podemos reformular este resultado de la siguiente manera: el problema de inmersión es resoluble si y sólo si podemos embeber E en $M^* \rtimes G$ de tal manera que el siguiente diagrama conmute

$$\begin{array}{ccc} E & \xrightarrow{\pi} & G \\ {\scriptstyle\psi}\downarrow & & \| \\ M^* \rtimes G & \xrightarrow[(x,\sigma)\mapsto\sigma]{} & G \end{array}$$

Esto es por lo siguiente. Supongamos primero que el problema es resoluble, entonces $i^*(\gamma) = 1$ y podemos hacer la construcción

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_p & \longrightarrow & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & {\scriptstyle i}\downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & M^* & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & {\scriptstyle h}\downarrow & & \| & & \\ 1 & \longrightarrow & M^* & \longrightarrow & M^* \rtimes G & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

donde la primea parte viene inducida por la imclusión $i : \mu_p \to M^*$ y la segunda por equivalencia de extensiones. Por otro lado, si tenemos el cuadrado conmutativo tenemos lo siguiente:

$$\begin{array}{ccccccccc} & & \mu_p & & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & {\scriptstyle i}\downarrow & & {\scriptstyle\psi}\downarrow & & \| & & \\ 1 & \longrightarrow & M^* & \xrightarrow{\alpha} & M^* \rtimes G & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

y al ser i, α y ψ inyectivas tenemos una aplicación inyectiva $\mu_p \to E$ que hace que el diagrama conmute. Por lo tanto tenemos una extensión

$$1 \to \mu_p \to E \to G \to 1$$

con $i^*(\gamma) = 1$, luego por el corolario el problema de inmersión es resoluble.

Para conseguir embeber E en $M^* \rtimes G$ haciendo el diagrama conmutativo procedemos de la siguiente manera. Buscamos generadores σ en G, tomamos sus preimagenes (a_σ, σ) en $M^* \rtimes G$, y vemos que sus respectivas preimagenes en E han de verificar las propiedades de los mismos (por la inyectividad). Además, los a_σ nos darán ω como hemos visto en la prueba del Teorema 2.1.

2.3 Ejemplos

2.3.1 Grupos cíclicos

Empecemos viendo una forma de representar los elementos de $H^2(C, A)$, con C un grupo cíclico de orden n. Sea $\sigma \in C$ un generador, y consideremos una extensión

$$1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} C \to 1.$$

Sea $s \in E$ tal que $\pi(s) = \sigma$, entonces la aplicación $C \to E$, $\sigma^i \mapsto s^i$ $(i = 0, \dots, n-1)$ es una sección (efectivamente $\pi(s^i) = \pi(s)^i = \sigma^i$) y se verifica $s^n = 1$, luego existe $a \in A$ tal que $\iota(a) = s^n$. El sistema de factores dado por esta sección sería

$$\iota(c_{\sigma^i,\sigma^j}) = s^i s^j (s^{i+j})^{-1}$$

es decir, por la inyectividad de ι:

$$c_{\sigma^i,\sigma^j} = \begin{cases} 1 & \text{si } i + j < n \\ a & \text{si } i + j \geq n \end{cases}$$

para $i, j = 0, \dots, n-1$. Además, la acción de C en $a \in A$ es

$$\iota(\sigma^i a) = s^i \iota(a) s^{-i} = s^i s^n s^{-i} = s^n = \iota(a),$$

luego $a \in A^C$. También es fácil comprobar que si consideramos una aplicación $c : G \times G \to A$ como la anterior, verifica las condiciones de un sistema de factores. Por lo tanto, dado un generador $\sigma \in C$ tenemos el isomorfismo $A^C \simeq Z^2(C, A)$ dado por $\sigma \mapsto c$.

Ahora supongamos que $c \in B^2(C, A)$, entonces $c_{\sigma^i,\sigma^j} = a_{\sigma^i}(\sigma^i a_{\sigma^j}) a^{-1}_{\sigma^{i+j}}$ para cierta aplicación $a : C \to A$. Como tiene que seguir verificando las condiciones de sistema de factores, se tiene que $a_{\sigma^{i+j}} = a_{\sigma^i}(\sigma^i a_{\sigma^j})$ para $i + j < n$. Por lo tanto, $a_1 = 1$ y si $a_\sigma = x$, $x \in A$ entonces

$$\begin{aligned} a_{\sigma^2} &= a_\sigma(\sigma a_\sigma) = x(\sigma x) \\ a_{\sigma^3} &= a_\sigma(\sigma a_{\sigma^2}) = x(\sigma(x(\sigma x)) = x(\sigma x)(\sigma^2 x) \\ &\cdots \\ a_{\sigma^{n-1}} &= x(\sigma x) \cdots (\sigma^{n-2} x). \end{aligned}$$

La condición $c_{\sigma^i,\sigma^j} = a$ si $i + j \geq n$ hace que $aa_{\sigma^{i+j}} = a_{\sigma^i}(\sigma^i a_{\sigma^j})$ luego

$$a = aa_1 = aa_{\sigma^n} = a_{\sigma^{n-1}}(\sigma^{n-1}a_\sigma) = x(\sigma x)\cdots(\sigma^{n-1}x)$$

luego se tiene que cumplir que $N_C(x) = a$. Por lo tanto dado un $c \in Z^2(C, A)$, este pertenece a $B^2(C, A)$ si y sólo si podemos encontrar un $x \in A$ con $N_C(x) = a$ (siendo $a \in A^C$ el elemento que "define" a c). Por lo tanto, mediante el isomorfismo de antes tenemos

$$H^2(C, A) \simeq A^C / N_C(A).$$

Visto esto sea K un cuerpo con característica distinta de p primo y conteniendo una raíz p-ésima primitiva de la unidad, $\zeta \in \mu_p$. Sea M/K una extensión cíclica de grado p^n, $n \in \mathbb{N}$ y sea σ un generador de $C_{p^n} = \mathrm{Gal}(M/K)$. Consideremos el siguiente problema de inmersión $(M/K, C_{p^{n+1}}, \pi, \mu_p)$ con la extensión

$$1 \to \mu_p \xrightarrow{\zeta \mapsto \tilde{\sigma}^{p^n}} C_{p^{n+1}} \xrightarrow{\tilde{\sigma} \mapsto \sigma} C_{p^n} \to 1$$

Como acabamos de ver, podemos tomar como representante de la clase de la extensión a $c \in Z^2(C_{p^n}, \mu_p)$ dado por

$$c_{\sigma^i,\sigma^j} = \begin{cases} 1 & \text{si } i + j < p^n \\ \zeta & \text{si } i + j \geq p^n \end{cases}$$

Por el Corolario 2.1, el problema tiene solución si y sólo si $i^*([c]) = [1]$, donde i^* es el homomorfismo inducido por la inclusión. La inclusión de c en M^* no lo modifica, luego se sigue cumpliendo que $c \in B^2(C_{p^n}, M^*)$ si y sólo si $\zeta = N_{C_{p^n}}(x) = N_{M/K}(x)$ para un $x \in M^*$. En corolario también nos dice que si esto ocurre, las soluciones son de la forma $M(\sqrt[p]{r\omega})/K$, $r \in K^*$ y un cierto $\omega \in M^*$. Observando el comienzo de la prueba del Teorema 2.1, dicho ω ha de verificar que $\sigma\omega/\omega = x^p$, donde x es precisamente aquel tal que $N_{M/K}(x) = \zeta$.

Consideremos ahora el caso $n = 1$, entonces por el Lema 2.1 $M = K(\sqrt[p]{a})$ para cierto $a \in K^*$ y nuestra extensión es

$$1 \to \mu_p \xrightarrow{\zeta \mapsto \tilde{\sigma}^p} C_{p^2} \xrightarrow{\tilde{\sigma} \mapsto \sigma} C_p \to 1$$

pudiendo tomar el generador σ de $C_p = \mathrm{Gal}(K(\sqrt[p]{a})/K)$ tal que $\sigma(\sqrt[p]{a}) = \zeta\sqrt[p]{a}$. Como ya hemos visto, el problema tiene solución si y sólo si $\zeta = N_{K(\sqrt[p]{a})/K}(x)$ para algún $x \in K(\sqrt[p]{a})^*$, y si tal cosa ocurre las soluciones son de la forma $M(\sqrt[p]{r\omega})/K$, $r \in K^*$

y un cierto $\omega \in K(\sqrt[p]{a})^*$ tal que $\sigma\omega/\omega = x^p$. Además, como C_p es cíclico, $\sigma^k x$ verifica también que $\zeta = N_{K(\sqrt[p]{a})/K}(\sigma^k x)$ para todo $\sigma^k \in C_p$, luego también nos sirve haciendo el papel de x. Entonces, tomando $\sigma^{p-1}x$

$$\omega = x(\sigma x^2)(\sigma^2 x^3)\cdots(\sigma^{p-2}x^{p-1})\sqrt[p]{a}$$

ya que

$$\frac{\sigma\omega}{\omega} = \frac{(\sigma x)(\sigma^2 x^2)\cdots(\sigma^{p-1}x^{p-1})\zeta\sqrt[p]{a}}{x(\sigma x^2)\cdots(\sigma^{p-2}x^{p-1})\sqrt[p]{a}} = \frac{(\sigma^{p-1}x^{p-1})\zeta}{x(\sigma x)\cdots(\sigma^{p-2}x)} = (\sigma^{p-1}x^{p-1})(\sigma^{p-1}x) = \sigma^{p-1}x^p.$$

Si vamos ahora a un caso más específico, $p = 2$, tenemos $M/K = K(\sqrt{a})/K$ y la extensión

$$1 \to \mu_2 \xrightarrow{-1\mapsto\tilde{\sigma}^2} C_4 \xrightarrow{\tilde{\sigma}\mapsto\sigma} C_2 \to 1$$

El problema dado por $K(\sqrt{a})/K$ y esta extensión tiene solución si y sólo si -1 es una norma en $K(\sqrt{a})/K$. Como $-a$ siempre es una norma, ya que $-a = N_{K(\sqrt{a})/K}(\sqrt{a})$, y la norma es un homomorfismo, -1 es una norma en $K(\sqrt{a})/K$ si y sólo si a lo es. Por lo tanto el problema tiene solución si y sólo si a es una norma en $K(\sqrt{a})/K$, es decir como $\sigma(\sqrt{a}) = -\sqrt{a}$, si existe $x = \alpha + \beta\sqrt{a}$ (con $\alpha, \beta \in K^*$) tales que

$$a = x(\sigma x) = (\alpha + \beta\sqrt{a})(\alpha - \beta\sqrt{a}) = \alpha^2 - \beta^2 a$$

y si en ese caso las soluciones son de la forma $M(\sqrt{r\omega})/K$, $r \in K^*$ y con $\omega = x = \alpha + \beta\sqrt{a}$, es decir de la forma $M(\sqrt{r(\alpha + \beta\sqrt{a})})/K$, $r \in K^*$.

Como $\sigma\omega/\omega = \sigma(\alpha+\beta\sqrt{a})/(\alpha+\beta\sqrt{a}) = (\alpha-\beta\sqrt{a})/(\alpha+\beta\sqrt{a})$, luego si queremos extender $\sigma \in C_2$ a $\tilde{\sigma} \in \mathrm{Gal}(M(\sqrt{r(\alpha + \beta\sqrt{a})})/K)$, se ha de cumplir

$$\tilde{\sigma}(\sqrt{r(\alpha + \beta\sqrt{a})}) = \sqrt{\frac{\alpha - \beta\sqrt{a}}{\alpha + \beta\sqrt{a}}} = \frac{\sqrt{\alpha^2 - \beta^2 a}}{\alpha + \beta\sqrt{a}} = \frac{\sqrt{a}}{\alpha + \beta\sqrt{a}}$$

por lo tanto extendemos σ a $M(\sqrt{r(\alpha + \beta\sqrt{a})})/K$ mediante

$$\sqrt{r(\alpha + \beta\sqrt{a})} \mapsto \frac{\sqrt{a}}{\alpha + \beta\sqrt{a}}\sqrt{r(\alpha + \beta\sqrt{a})}$$

Si $a = 1+c^2$ (con $c \in K$), entonces $\alpha = a/c$ y $\beta = 1/c$ verifican $\alpha^2 - \beta^2 a = a$, luego cambiando r por r/c tenemos extensiones $K(\sqrt{r(a+\sqrt{a})})/K$, $r \in K^*$ con grupo de Galois C_4.

Ejemplo 2.1. Para $K = \mathbb{Q}$ y $c = 4$, tenemos extensiones $\mathbb{Q}(\sqrt{r(5+\sqrt{5})})/\mathbb{Q}$, $r \in \mathbb{Q}^*$ con grupo de Galois C_4.

Consideremos ahora el caso $n = p = 2$, es decir la extensión

$$1 \to \mu_2 \xrightarrow{-1\mapsto\tilde{\sigma}^4} C_8 \xrightarrow{\tilde{\sigma}\mapsto\sigma} C_4 \to 1$$

y sea $M/K = K(\sqrt{a+\sqrt{a}})/K$ una extensión con grupo de Galois C_4 como la obtenida anteriormente, es decir $a = 1 + c^2$. Si $c = d^2$ y consideramos el elemento $x = \sqrt{a+\sqrt{a}/d} - d$ se tiene que

$$\begin{aligned}(\sqrt{a+\sqrt{a}/d} - d)(\sqrt{a-\sqrt{a}/d} - d)(\sqrt{a+\sqrt{a}/d} + d)(\sqrt{a-\sqrt{a}/d} + d) = \\ = (d^2 - \frac{a+\sqrt{a}}{d^2})(d^2 - \frac{a-\sqrt{a}}{d^2}) = (d^2 - \frac{a}{d^2})^2 - \frac{a}{d^4} = d^4 + \frac{a^2}{d^4} - 2a - \frac{a}{d^4} = \\ = a - 1 + \frac{a^2}{a-1} - 2a - \frac{a}{a-1} = \frac{(a-1)^2 + a^2 - 2a^2 + 2a - a}{a-1} = -1.\end{aligned}$$

Entonces x tiene norma -1. Se tiene que

$$\omega = ad^2 + d^2(d^2-1)\sqrt{a} + (a-d^2)\sqrt{a+\sqrt{a}} + (d^2-1)\sqrt{a}\sqrt{a+\sqrt{a}}$$

verifica $\sigma\omega/\omega = x^2$ y por tanto $M(\sqrt{r\omega})/K$ es solución.

Ejemplo 2.2. Si $K = \mathbb{Q}$ y $d = 1$, entonces $a = 2$ y tenemos que $\mathbb{Q}(\sqrt{r(2+\sqrt{2+\sqrt{2}})}/\mathbb{Q}$, $r \in \mathbb{Q}^*$ son extensiones con grupo de Galois C_8.

2.3.2 El grupo diedral D_4

Consideremos el grupo diedral de orden 8 dado por

$$D_4 = \langle \sigma, \tau : \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle$$

así como el grupo de Klein

$$K_4 = \langle \sigma, \tau : \sigma^2 = \tau^2 = (\sigma\tau)^2 = 1 \rangle.$$

Tenemos la siguiente extensión

$$1 \to \mu_2 \to D_4 \xrightarrow[\tau \mapsto \tau]{\sigma \mapsto \sigma} K_4 \to 1$$

Sea ahora K un cuerpo de característica distinta de 2 y consideremos la extensión $K(\sqrt{a}, \sqrt{b})/K$, $a, b \in K^*$ con grupo de Galois K_4 dado por

$$\sigma(\sqrt{a}) = -\sqrt{a}, \quad \sigma(\sqrt{b}) = \sqrt{b}$$
$$\tau(\sqrt{a}) = \sqrt{a}, \quad \tau(\sqrt{b}) = -\sqrt{b}$$

Como sabemos, el problema de inmersión tiene solución si y sólo si podemos embeber D_4 en $M^* \rtimes K_4$ de la manera adecuada. Para ello buscamos (a_σ, σ) y (a_τ, τ) tales que sus preimagenes en D_4 sean los generadores. Entonces debe cumplirse $(a_\sigma, \sigma)^4 = (a_\tau, \tau)^2 = 1$ y $(a_\tau, \tau)(a_\sigma, \sigma) = (a_\sigma, \sigma)^3(a_\tau, \tau)$. Realizando los cálculos:

$$(a_\sigma, \sigma)^4 = (a_\sigma(\sigma a_\sigma), 1)^2 = ((a_\sigma(\sigma a_\sigma))^2, 1)$$

luego $a_\sigma(\sigma a_\sigma) = -1$ (es -1 y no $+1$ porque por la conmutatividad de la parte izquierda, la imagen de -1 en $M^* \rtimes K_4$ que es $(-1, 1)$ debe coincidir con la composición de imagen en D_4 y luego en $M^* \rtimes K_4$, que es $(a_\sigma(\sigma a_\sigma), 1)$). Análogamente $(a_\tau(\tau a_\tau) = 1$. Por último

$$(a_\tau, \tau)(a_\sigma, \sigma) = (a_\tau(\tau a_\sigma), 1)$$

y

$$(a_\sigma, \sigma)^3(a_\tau, \tau) = (a_\sigma(\sigma a_\sigma)a_\sigma, \sigma)(a_\tau, \tau) = (a_\sigma(\sigma a_\sigma)a_\sigma(\sigma a_\tau), 1),$$

luego $a_\tau(\tau a_\sigma) = -a_\sigma(\sigma a_\tau)$. Podemos conseguir aún más: $K(\sqrt{a}, \sqrt{b})/K(\sqrt{a})$ tiene como grupo de Galois C_2 con generador τ, luego

$$1 = a_\tau(\tau a_\tau) = N_{K(\sqrt{a}, \sqrt{b})/K(\sqrt{a})}(a_\tau)$$

y por el Lema 2.1 se tiene que $a_\tau = \tau z/z$ para un $z \in K(\sqrt{a}, \sqrt{b})^*$. Si suponemos $a_\tau = 1$ tenemos que

$$a_\sigma(\sigma(\tau z)z^{-1}) = -(\tau z)z^{-1}(\tau a_\sigma),$$

luego $a_\sigma = -\tau a_\sigma$. Para volver a lo anterior basta cambiar a_σ por $a_\sigma z(\sigma z)^{-1}$, por lo que podemos tomar $a_\tau = 1$ y buscar a_σ. Sea ahora $x = a_\sigma\sqrt{a}\sqrt{b}$, entonces

$$x(\sigma x) = a_\sigma\sqrt{a}\sqrt{b}(\sigma a_\sigma\sqrt{a}\sqrt{b}) = a_\sigma\sqrt{a}\sqrt{b}(\sigma a_\sigma)(-\sqrt{a}\sqrt{b}) = a_\sigma(\sigma a_\sigma)(-ab),$$

$$\tau x = -(\tau a_\sigma)\sqrt{a}\sqrt{b},$$

es decir $a_\sigma(\sigma a_\sigma) = -1 \iff x(\sigma x) = ab$, y $\tau a_\sigma = -a_\sigma \iff \tau x = x$. De la segunda condición tenemos que $x \in K(\sqrt{a})$ y de la primera $N_{K(\sqrt{a})/K}(x) = ab$, por lo que nuestro problema de inmersión tiene solución si y sólo si ab es una norma en $K(\sqrt{a})/K$, es decir, si existe $x = \alpha + \beta\sqrt{a}$ tal que $x(\sigma x) = ab$. Como

$$ab = x(\sigma x) = (\alpha + \beta\sqrt{a})(\alpha - \beta\sqrt{a}) = \alpha^2 - \beta^2 a,$$

es equivalente a que existan $\alpha, \beta \in K$ tales que $\alpha^2 - \beta^2 a = ab$. En tal caso, sean $a_\sigma = \sqrt{a}\sqrt{b}/(\alpha + \beta\sqrt{a})$ y $a_\tau = 1$, que verifican lo exigido y sea $\omega = \alpha + \beta\sqrt{a}$, entonces

$$\frac{\sigma(\omega)}{\omega} = \frac{\alpha - \beta\sqrt{a}}{\alpha + \beta\sqrt{a}} = \frac{(\alpha - \beta\sqrt{a})(\alpha + \beta\sqrt{a})}{(\alpha + \beta\sqrt{a})^2} = \frac{ab}{(\alpha + \beta\sqrt{a})^2} = a_\sigma^2$$

y

$$\frac{\tau\omega}{\omega} = \frac{\omega}{\omega} = 1 = a_\tau^2$$

luego las soluciones son de la forma $M(\sqrt{r(\alpha + \beta\sqrt{a})})/K = K(\sqrt{r(\alpha + \beta\sqrt{a})}, \sqrt{b})/K$, $r \in K^*$. Además, podemos extender $\sigma, \tau \in K_4$ a D_4 haciendo

$$\sigma(\sqrt{r(\alpha + \beta\sqrt{a})}) = \frac{\sqrt{a}\sqrt{b}}{\alpha + \beta\sqrt{a}}\sqrt{r(\alpha + \beta\sqrt{a})}, \quad \sigma(\sqrt{b}) = \sqrt{b};$$

y

$$\tau(\sqrt{r(\alpha + \beta\sqrt{a})}) = \sqrt{r(\alpha + \beta\sqrt{a})}, \quad \tau(\sqrt{b}) = -\sqrt{b}.$$

Ejemplo 2.3. Si $a = 1 + b$ entonces podemos hacer $\alpha = a$ y $\beta = 1$, cumpliendo $\alpha^2 - \beta^2 a = a^2 - a = a(a-1) = ab$. Por lo tanto las soluciones son de la forma $K(\sqrt{r(a + \sqrt{a})}, \sqrt{b})/K, r \in K^*$. En particular, si $K = \mathbb{Q}$ y $b = 2$ tenemos extensiones con grupo de Galois D_4:

$$\mathbb{Q}(\sqrt{r(3 + \sqrt{3})}, \sqrt{2})/\mathbb{Q}, \ r \in \mathbb{Q}^*$$

Si $b = -1$ (con a cualquiera), podemos tomar $\alpha = 0$ y $\beta = 1$, y tenemos soluciones de la forma $K(\sqrt[4]{r^2 a}, i)/K$, $r \in K^*$. En particular, si $K = \mathbb{Q}$ y $a = 2$ tenemos

$$\mathbb{Q}(\sqrt[4]{2r^2}, i)/\mathbb{Q}, \ r \in \mathbb{Q}^*$$

2.3.3 El grupo de Heisenberg módulo p

Sea p un primo distinto de 2. El grupo de Heisenberg viene dado por

$$H_{p^3} = \langle u, v, w : u^p = v^p = w^p = 1, vu = uvw, wu = uw, wv = vw \rangle$$

Sea K un cuerpo con característica distinta de p y tal que $\mu_p \subset K^*$. Sea $M = K(\sqrt[p]{a}, \sqrt[p]{b})$, $a, b \in K^*$ y consideremos la extensión M/K, cuyo grupo de Galois es $C_p \times C_p$. Sea $\zeta \in \mu_p$ una raíz primitiva y sean $\sigma, \tau \in \mathrm{Gal}(M/K)$ los generadores, dados por

$$\sigma(\sqrt[p]{a}) = \zeta\sqrt[p]{a}, \quad \sigma(\sqrt[p]{b}) = \sqrt[p]{b}$$

y

$$\tau(\sqrt[p]{a}) = \sqrt[p]{a}, \quad \tau(\sqrt[p]{b}) = \zeta\sqrt[p]{b}$$

Consideremos el problema de inmesión dado por M/K y la extensión

$$1 \to \mu_p \xrightarrow{\zeta \mapsto w} H_{p^3} \xrightarrow[v \mapsto \tau]{u \mapsto \sigma} C_p \times C_p \to 1$$

Sean (a_σ, σ) y (a_τ, τ) preimagenes en $M^* \rtimes \mathrm{Gal}(M/K)$ de σ y τ respectivamente. Por la conmutatividad sus preimagenes en H_{p^3} han de ser u y v, luego ha de cumplirse $(a_\sigma, \sigma)^p = (a_\tau, \tau)^p$, lo cual nos da

$$a_\sigma(\sigma a_\sigma) \cdots (\sigma^{p-1} a_\sigma) = 1 \ y \ a_\tau(\tau a_\tau) \cdots (\tau^{p-1} a_\tau) = 1$$

y también $(a_\tau, \tau)(a_\sigma, \sigma) = (\zeta, 1)(a_\sigma, \sigma)(a_\tau, \tau)$, lo cual nos da

$$a_\tau(\tau a_\sigma) = \zeta a_\sigma(\sigma a_\tau).$$

Nuevamente, a_τ tiene norma 1 en $M/K(\sqrt[p]{a})$ y por el Lema 2.1 luego existe $z \in M^*$ tal que $a_\tau = \tau z/z$. Como en el caso anterior, podemos suponer $a_\tau = 1$ y tenemos

$$a_\sigma(\sigma a_\sigma) \cdots (\sigma^{p-1} a_\sigma) = 1 \ y \ \tau a_\sigma = \zeta a_\sigma$$

Sea ahora $x = \sqrt[p]{b}/a_\sigma$, las condiciones de arriba son equivalentes a

$$x(\sigma x) \cdots (\sigma^{p-1} x) = b \quad y \quad \tau x = x,$$

luego el problema de inmersión es resoluble si y sólo si existe $x \in K(\sqrt[p]{a})$ tal que $N_{K(\sqrt[p]{a})/K}(x) = b$, y en dicho caso haciendo $a_\sigma = \sqrt[p]{b}/x$ y $a_\tau = 1$, ambos verifican las condiciones de arriba y por lo tanto tenemos que $\omega = x^{p-1}(\sigma x^{p-2} \cdots (\sigma^{p-2} x)$ verifica $\sigma\omega/\omega = a_\sigma^p$ y $\tau\omega/\omega = a_\tau^p$. Las soluciones son de la forma $M(\sqrt{r\omega})/K$, $r \in K^*$.

3 El grupo de Brauer

Vamos a ver el grupo de Brauer, su relación con el segundo grupo de cohomología de un grupo de Galois y sus aplicaciones al problema de inmersión.

3.1 Álgebras centrales simples

Para poder definir el grupo de Brauer, vamos a necesitar hablar de álgebras sobre un cuerpo, más concretamente de álgebras centrales simples finitas. Muchos resultados y propiedades simplemente se enunciarán y no se probaran. Las demostraciones se pueden encontrar en el Capítulo 3 de [6] y el Capítulo 4 y Capítulo 8 secciones 4 y 5 de [4].

Definición 3.1. *Dado un cuerpo K, una K-**álgebra** consiste en un anillo A y un homomorfismo de anillos $K \to Z(A)$, donde $Z(A) = \{a \in A : ab = ba \ \forall b \in A\}$ es el centro de A.*

Usualmente denotaremos A/K para indicar una K-álgebra A.

Observación 3.1. Como K es un cuerpo, el homomorfismo es inyectivo (si A no es el anillo cero) y por lo tanto podemos identificar K con su imagen en $Z(A)$. Esto dota a A de una estructura de K-espacio vectorial cuyo producto por escalar conmuta con el producto de A.

Definición 3.2. *Si con dicha identificación, $K = Z(A)$, diremos que A es un **álgebra central**.*

Cuando hablemos de la dimensión de A/K nos referiremos a la dimensión de A como K-espacio vectorial. Si dicha dimensión es finita diremos que A/K es finita. Por lo general denotaremos $[A : K] = \dim_K(A)$.

Un homomorfismo de K-álgebras es un homomorfismo de anillos K-linear, una subálgebra es un subanillo que es cerrado para el producto escalar (es decir es también un subespacio vectorial) y un ideal (a la izquierda/derecha/bilátero) es un ideal (a la izquierda/derecha/bilátero respectivamente) del anillo (que automáticamente será subespacio vectorial)

Definición 3.3. *Sea A una K-álgebra y B una subálgebra. Definimos el centralizador de B en A como*

$$C_A(B) = \{a \in A : ab = ba \ \forall b \in B\}.$$

Definición 3.4. *Diremos que un álgebra finita A/K es **simple** si no tiene ideales biláteros aparte de 0 y A.*

Definición 3.5. *Si A es un anillo de división (todo elemento menos el cero tiene inverso multiplicativo), diremos que A/K es un **álgebra de división**.*

Ejemplo 3.1. Si D/K es un álgebra de división, entonces $\mathrm{Mat}_n(D)/D$ es un álgebra simple. Consideremos las matrices E_{ij}, con 1 en la posición i, j y cero el resto. Estas matrices generan a $\mathrm{Mat}_n(D)$ como D-álgebra, luego basta probar que pertencen a todo ideal bilátero no nulo de $\mathrm{Mat}_n(D)$. Como además se verifica $E_{ki}E_{ij}E_{jl} = E_{kl}$, basta probar que todo ideal bilátero no nulo contiene a un E_{ij}. Consideremos un ideal bilátero no nulo, y sea M un elemento del mismo. Para algún par (i, j) tal que el elemento correspondiente $m_{i,j}$ de M no sea cero, se cumple que

$$m_{i,j}^{-1} E_{i,i} M E_{j,j} = E_{i,j}$$

y por lo tanto $E_{i,j}$ está en el ideal y hemos terminado.

Como las únicas matrices que conmutan con todas son los productos de un escalar por la identidad, tenemos que $Z(D) \simeq Z(\mathrm{Mat}_n(D))$, y como $K \subseteq Z(D)$ tenemos que $\mathrm{Mat}_n(D)/K$ es un álgebra simple, y es central si D/K es central.

Por simplificar, denotaremos a las álgebras finitas centrales simples y las álgebras finitas centrales de división por sus siglas en inglés, CSA y CDA respectivamente.

Observación 3.2. Si A es una CDA, en particular es una CSA, ya que al ser todo elemento de A una unidad, cualquier ideal no nulo ha de contener al 1 y por lo tanto es el total.

Una ventaja que tienen las álgebras simples, es que las podemos ver como un álgebra de matrices sobre un álgebra de división. Es el Teorema de Wedderburn (que en realidad es para anillos, pero lo formulamos directamente para álgebras), para el cuál hacen falta un par de resultados previos:

Definición 3.6. *Sea A/K un álgebra y M un A-módulo. Diremos que M es **simple** si es no nulo y sus únicos submódulos son 0 y M.*

Ejemplo 3.2. Si D es un anillo de división, entonces D^n es simple como $\mathrm{Mat}_n(D)$-módulo. Si no lo fuera, es decir si existiera un submódulo propio no nulo $M \subset D^n$, sería cerrado para la multiplicación por matrices. Sin embargo, al ser D un anillo de división, entonces para todo par de vectores existe una matriz que lleva uno en otro, luego tomando uno en M y otro en $D^n \setminus M$ tenemos una contradicción.

Lema 3.1 (Schur). Sea A/K un álgebra y M, N dos A-módulos simples. Entonces todo homomorfismo no nulo $\varphi : M \to N$ es un isomorfismo. En particular $\mathrm{End}_A(M)$ es un álgebra de división.

Demostración. Sea $\varphi : M \to N$ un homomorfismo no nulo. Entonces $\mathrm{Ker}\,\varphi$ es un submódulo de M. Como M es simple, y φ es no nulo, $\mathrm{Ker}\,\varphi$ es 0. Por un razonamiento análogo, es sobreyectivo (la imagen es un submódulo de N no nulo, luego ha de ser N). Por lo tanto todo φ es un isomorfismo. En el caso particular de $\mathrm{End}_A(M)$, todo elemento no nulo es un isomorfismo y por lo tanto tiene inverso. ∎

Lema 3.2 (Rieffel). Sea A una K-álgebra simple, I un ideal por la izquierda no nulo de A y $D = \mathrm{End}_A(I)$. Consideremos la estructura de M como D-módulo dada por $\varphi \cdot x = \varphi(x)$, $\varphi \in D$, $x \in I$. En tonces la aplicación

$$\lambda_I : A \to \mathrm{End}_D(I), a \mapsto (x \mapsto ax)$$

es un isomorfismo.

Demostración. Primero veamos que la aplicación $x \mapsto ax$, con $a \in A$ es un D-endomorfismo. Si $\varphi \in D$, entonces $\varphi \cdot ax = \varphi(ax) = a\varphi(x) = a\varphi \cdot x$ para todo $x \in I$.

Como λ_I no es nulo, su núcleo es un ideal bilátero propio de A, y como A es simple entonces ha de ser 0, por lo que λ_I es inyectiva.

Veamos ahora que $\lambda_I(I)$ es un ideal por la izquierda de $\mathrm{End}_D(I)$. Sean $\varphi \in \mathrm{End}_D(I)$ y $x \in I$. Entonces $\varphi \cdot \lambda_I(x)$ es la aplicación $y \mapsto \varphi(xy)$. Como la aplicación $y \mapsto yx$, $x \in I$ es un elemento de $\mathrm{End}_A(I) = D$ y φ es un D-endomorfismo, tenemos $\varphi(xy) = \varphi(x)y$. Por lo tanto $\varphi \cdot \lambda_I(x) = \lambda_I(\varphi(x))$ y hemos probado que $\lambda_I(I)$ es un ideal por la izquierda de $\mathrm{End}_D(I)$.

Consideremos ahora el ideal por la derecha IA de A definido como:

$$IA = \{\sum_{i=1}^{r} x_i a_i : r \in \mathbb{N},\ x_i \in I,\ a_i \in A\},$$

Entonces, al ser I un ideal por la izquierda, IA es bilátero y por ser A simple (e IA es no nulo) tenemos que $IA = A$. Por lo tanto podemos escribir $1 = \sum x_i a_i$. Entonces, para cualquier $\varphi \in \mathrm{End}_D(I)$ tenemos:

$$\varphi = \varphi \cdot 1 = \varphi\lambda_I(1) = \sum_i \varphi\lambda_I(x_i)\lambda_I(a_i),$$

y como hemos probado antes que $\lambda_I(I)$ es un ideal por la izquierda, tenemos que $\varphi\lambda_I(x_i) \in \lambda_I(I)$ para todo i y hemos probado que $\varphi \in \lambda_I(I)$, y por tanto la sobreyectividad.

Lema 3.3. Si A/K es un álgebra simple finita entonces tiene A-submódulos simples y además son todos isomorfos entre sí.

Demostración. Como A es de dimensión finita, toda cadena descendente de ideales se estabiliza en algún momento (los ideales de un álgebra son subespacios, luego una contención estricta de ideales implica un salto de dimensión). Sea I un ideal por la izquierda minimal. Este ideal es un submódulo, y al ser minimal es simple.

Sea ahora M otro A-submódulo simple y consideremos el ideal de M formado por los $a \in A$ tales que $am = 0$ para todo $m \in M$. Como M es no nulo dicho ideal es propio, y como M es simple entonces el ideal ha de ser 0. Es decir, no existe ningún $a \in A$ no nulo tal que $am = 0$ para todo $m \in M$. En particular ninguno de I lo verifica y por lo tanto podemos tomar $m \in M$ tal que $xm \neq 0$ para algún $x \in I$. Con esto, el homomorfismo $x \mapsto xm$ es no nulo y como I y M son simples, es un isomorfismo por el Lema de Schur (3.1).

Teorema 3.1 (Wedderburn). *Sea A/K un álgebra finita simple. Entonces existen un entero $n \geq 1$ y un álgebra de división D con $K \subset D$ tales que A es isomorfa a $M_n(D)$. Más aún D es único salvo isomorfismo.*

Demostración. Sea I un ideal por la izquierda minimal, que en particular es un A-módulo simple, dado por el lema anterior (3.3). Por el Lema de Schur (3.1), $D = \mathrm{End}_A(I)$ es un álgebra de división, y por el Lema de Rieffel (3.2) tenemos un isomorfismo $A \simeq \mathrm{End}_D(I)$. Ahora, como D es un álgebra de división, podemos utilizar el mismo argumento que con espacios vectoriales para al fijar una base obtener un isomorfismo $\mathrm{End}_D(I) \simeq \mathrm{Mat}_n(D)$, donde n es la dimensión de I sobre D.

Supongamos que D' es otro álgebra de división con $\mathrm{Mat}_m(D') \simeq A$. Como D^n y D'^m son respectivamente $\mathrm{Mat}_n(D)$- y $\mathrm{Mat}_m(D')$-módulos simples, así como I, tenemos por el Lema 3.3 que $D^n \simeq D'^m$ y por tanto

$$D \simeq \mathrm{End}_A(D^n) \simeq \mathrm{End}_A(L) \simeq \mathrm{End}_A(D'^m) \simeq D'$$

y por lo tanto $D \simeq D'$.

Proposición 3.1. Si D/K y D'/K son dos CDAs tales que $\mathrm{Mat}_r(D) \simeq \mathrm{Mat}_s(D')$ para $r, s \in \mathbb{N}$, entonces $D \simeq D'$ y $r = s$.

Demostración. En particular hemos visto que $A = \mathrm{Mat}_r(D) \simeq \mathrm{Mat}_s(D')$ es un álgebra simple (Ejemplo 3.1), por lo que por el Teorema de Wedderburn (3.1) D es único salvo isomorfismo. Tenemos por tanto que $D \simeq D'$, y por tanto $r = s$.

Teorema 3.2 (Skolem-Noether). *Sea A/K una CSA y B una subálgebra simple de A. Entonces todo homomorfismo de K-álgebras $B \to A$ es de la forma $b \mapsto ubu^{-1}$ para un $u \in A$ invertible.*

3.1.1 Producto tensorial de álgebras

Dadas dos K-álgebras A y B, consideramos su producto tensorial como espacios vectoriales y definimos la multiplicación mediante

$$(a \otimes b)(a' \otimes b') = (aa') \otimes (bb'), \quad a, a' \in A,\ b, b' \in B.$$

Por lo tanto el producto tensorial $A \otimes_K B$ es una K-álgebra.

En el caso especial $B/K = L/K$ una extensión de cuerpos, podemos convertir $A \otimes_K L$ en una L-álgebra mediante

$$x(a \otimes y) = a \otimes (xy)$$

A este L-álgebra se le llama la **extensión escalar** de A, denotado A_L. Si M es una extensión de L, se verifica $A_M = (A_L)_M$, y si B es otra K-álgebra, se tiene que $(A \otimes_K B)_L = A_L \otimes_L B_L$.

Observación 3.3. El producto tensorial de K-álgebras hereda las siguientes propiedades del producto tensorial de módulos:

- $A \otimes_K B \simeq B \otimes_K A$.
- $(A \otimes_K B) \otimes_K C \simeq A \otimes_K (B \otimes_K C)$.
- $A \otimes_K K \simeq A$.

Proposición 3.2. Si A es una K-álgebra, entonces $\mathrm{Mat}_n(A) \simeq \mathrm{Mat}_n(K) \otimes_K A$.

Proposición 3.3. Si A/K es una CSA entonces $A \otimes_K A^{op} \simeq \mathrm{Mat}_n(K)$, donde A^{op} es la denominada **álgebra opuesta**, es decir A con la multiplicación $a \cdot b = ba$.

Teorema 3.3. *Sea A/K un álgebra y B una subálgebra central simple finita. Entonces $A \simeq B \otimes_K C_A(B)$. Además hay una biyección entre los ideales de A y los de $C_A(B)$ y se cumple que $Z(A) = Z(C_B(A))$. En particular, si A/K es una CSA también lo es $C_A(B)/K$.*

Proposición 3.4. Si A/K y B/K son CSAs entonces $A \otimes_K B$ también lo es.

3.1.2 Cuerpos de descomposición

Definición 3.7. *Dada una CSA A/K y una extensión de cuerpos L/K, diremos que L es un cuerpo de descomposición de A, si $A_L \simeq \mathrm{Mat}_n(L)$ para un $n \in \mathbb{N}$.*

Proposición 3.5. Sean un cuerpo K, una extensión L/K y A/K y B/K dos CSAs:

1. L es cuerpo de descomposición de $\mathrm{Mat}_n(K)$ para todo $n \in \mathbb{N}$.
2. Si $A \simeq \mathrm{Mat}_n(B)$ para algún $n \in \mathbb{N}$, entonces L es cuerpo de descomposición de A si y sólo si lo es de B
3. Si L es cuerpo de descomposición de A, lo es también de A^{op}.
4. Si L es cuerpo de descomposición de A y B, lo es de $A \otimes_K B$.

Teorema 3.4. *Si D/K es una CDA, entonces una extensión finita L/K es cuerpo de descomposición de D si y sólo si L es subcuerpo de algún $A = \mathrm{Mat}_r(D)$ tal que $C_A(L) = L$.*

Proposición 3.6. Sea A/K una CSA. Entonces A tiene un cuerpo de descomposición que es Galois sobre K.

3.2 El grupo de Brauer

Ya tenemos todos los ingredientes para definir el grupo de Brauer y ver por qué nos interesa.

Dadas dos CSAs A/K y B/K, diremos que son equivalentes y denotaremos $A \sim B$ si existen $r, s \in \mathbb{N}$ tales que $\mathrm{Mat}_r(A) \simeq \mathrm{Mat}_s(B)$. Esta relación es una relación de equivalencia. Como se verifica $A \sim B \Rightarrow A \otimes_K C \sim B \otimes_K C$ podemos definir la operación $[A][B] = [A \otimes_K B]$, donde $[A]$ denota la clase de equivalencia de A.

Esta relación es equivalente a: $A \sim B$ si $\mathrm{Mat}_r(K) \otimes_K A \simeq \mathrm{Mat}_s(K) \otimes_K B$. Por lo tanto, sean D y D' las CDAs tales que $A \simeq \mathrm{Mat}_n(K) \otimes_K D$ y $B \simeq \mathrm{Mat}_m(K) \otimes_K D'$.

Si $A \sim B$, entonces $\mathrm{Mat}_{rn}(D) \simeq \mathrm{Mat}_{sm}(D')$ y se tiene $rn = sm$ y $D \simeq D'$. Por lo tanto una clase $[A]$ contiene una única clase de isomorfismos de CDAs.

El conjunto de estas clases de equivalencia junto a la operación que acabamos de definir forman un grupo abeliano que llamamos **grupo absoluto de Brauer**, $\mathrm{Br}(K)$, cuyo elemento neutro es $[K]$ y el inverso de $[A]$ es $[A^{op}]$.

Dada una extensión de cuerpos L/K, tenemos un homomorfismo $res_{L/K} : \mathrm{Br}(K) \to \mathrm{Br}(L)$ dado por $[A] \mapsto [A_L]$. Definimos el **grupo relativo de Brauer** $\mathrm{Br}(L/K)$ como el núcleo de este homomorfismo, es decir el subgrupo formado por las clases $[A]$ tales que $A_L \sim 1 \in \mathrm{Br}(L)$.

Como toda CSA A/K tiene un cuerpo de descomposición Galois sobre K, entonces

$$\mathrm{Br}(K) = \bigcup_{M/K Galois} \mathrm{Br}(M/K)$$

3.2.1 Productos cruzados y conexión con cohomología

Sea M/K una extensión de Galois de grado n y grupo de Galois $G = \mathrm{Gal}(M/K)$. Ahora construimos un M-espacio vectorial con base indexada por los elementos de G, por lo que los elementos de dicho espacio vectorial se pueden escribir de manera única como

$$\sum_{\sigma \in G} a_\sigma e_\sigma,$$

donde e_σ es el vector de la base con índice σ. Para dotar a este espacio vectorial de estructura de K-álgebra definimos el producto mediante

$$e_\sigma a = (\sigma a) e_\sigma, \quad e_\sigma e_\tau = c_{\sigma,\tau} e_{\sigma\tau}$$

donde $c_{\sigma,\tau} \in M^*$. Por lo tanto, dados $\alpha = \sum_{\sigma \in G} a_\sigma e_\sigma$ y $\beta = \sum_{\tau \in G} b_\tau e_\tau$, se tiene

$$\alpha\beta = \sum_{\sigma \in G} a_\sigma e_\sigma \sum_{\tau \in G} b_\tau e_\tau = \sum_{\sigma,\tau \in G} c_{\sigma,\tau} (\sigma b_\tau) e_{\sigma\tau}.$$

Para que este producto sea asociativo, debe cumplirse que $(e_\sigma e_\tau) e_\rho = e_\sigma (e_\tau e_\rho)$, y como

$$(e_\sigma e_\tau) e_\rho = c_{\sigma,\tau} e_{\sigma\tau} e_\rho = c_{\sigma,\tau} c_{\sigma\tau,\rho} e_{\sigma\tau\rho},$$

$$e_\sigma (e_\tau e_\rho) = e_\sigma c_{\tau,\rho} e_{\tau\rho} = (\sigma c_{\tau,\rho}) e_\sigma e_{\tau\rho} = (\sigma c_{\tau,\rho}) c_{\sigma,\tau\rho} e_{\sigma\tau\rho},$$

y por tanto se tiene que cumplir que

$$c_{\sigma,\tau}c_{\sigma\tau,\rho} = (\sigma c_{\tau,\rho})c_{\sigma,\tau\rho}$$

Es decir, si consideramos la aplicación $c : G \times G \to M^*$, $(\sigma, \tau) \mapsto c_{\sigma,\tau}$, se verifica que $c \in Z^2(G, M^*)$. Por último, la condición $e_\sigma a = (\sigma a)e_\sigma$ implica en particular que $e_\sigma x = xe_\sigma$ para $x \in K$, luego tenemos bien definida la estructura de K-álgebra. Al álgebra que acabamos de construir la denominamos el **producto cruzado de M y G respecto de** c y escribimos (M, G, c).

Observación 3.4. Si recordamos las propiedades de los sistemas de factores, se cumplía que $c_{1,\tau} = c_{1,1}$ y $c_{\tau,1} = \tau c_{1,1}$. Esto junto a $e_\sigma e_\tau = c_{\sigma,\tau}e_{\sigma\tau}$ implica que $e_1 = c_{1,1}$ o $1 = c_{1,1}^{-1}e_1$.

Proposición 3.7. $A = (M, G, c)$ es un álgebra simple central sobre K de dimensión n^2 y $C_A(M) = M$.

Demostración. La dimensión de A como K-espacio vectorial la tenemos por $[A : K] = [A : M][M : K] = n^2$.

Sea I un ideal propio de A. Consideremos el homomorfismo $A \to A/I$, $a \mapsto \tilde{a} = a + I$, que es sobreyectivo. Tenemos por lo tanto que todo elemento de A/I se puede escribir como $\sum_{\sigma\in G} a_\sigma \tilde{e}_\sigma$, $a_\sigma \in M$. Por lo tanto los $\tilde{e}_\sigma$ son un sistema de generadores de A/I. Veamos ahora que son linealmente independientes. Como la extensión M/K es Galois, existe $\theta \in M$ tal que $M = K(\theta)$ (teorema del elemento primitivo). Consideremos ahora la aplicación $A/I \to A/I$, $x \mapsto x\theta$. La aplicación es M-linear y verifica $\tilde{e}_\sigma\theta = (\sigma\theta)\tilde{e}_\sigma$, por lo que $\tilde{e}_\sigma$ es un autovector con autovalor $\sigma\theta$. Como $K(\theta)/K$ es Galois, los $\sigma\theta$ son distintos y por tanto los $\tilde{e}_\sigma$ son linealmente independientes. Con esto tenemos que A/I tiene dimensión n sobre M (y n^2 sobre K) independientemente de I, luego I ha de ser cero y A es simple.

Sea ahora $x \in C_A(M)$, es decir $xb = bx$ para todo $b \in M$. Escribimos $x = \sum_{\sigma\in G} a_\sigma e_\sigma$ y tenemos

$$0 = \sum_{\sigma\in G} a_\sigma e_\sigma b - \sum_{\sigma\in G} ba_\sigma e_\sigma = \sum_{\sigma\in G} (b - (\sigma b)a_\sigma e_\sigma$$

luego $ba_\sigma = (\sigma b)a_\sigma$ para todo $\sigma \in G$ y todo $b \in M$. En particular, si tomamos $b = \theta$ (el elemento primitivo de antes), $\theta \neq \sigma\theta$ y tenemos que $a_\sigma = 0$ para todo $\sigma \neq 1$. Por lo tanto $x = a_1e_1 = a_1c_{1,1} \in M$ y tenemos $C_A(M) = M$ (la inclusión contraria es obvia).

Por último, dado $x \in Z(A)$ tenemos en particular que $x \in C_A(M)$ luego $x \in M$. Además, $e_\sigma x = xe_\sigma$, luego $(\sigma x)e_\sigma = e_\sigma x = xe_\sigma$ para todo $\sigma \in G$ y por tanto $x \in K$. Tenemos entonces que $Z(A) = K$ y A es central.

Como $C_A(M) = M$, por el Teorema 3.4, M es cuerpo de descomposición de D, siendo D la CDA tal que por el Teorema 3.1 $A \simeq \mathrm{Mat}_r(D)$. Por lo tanto M también es cuerpo de descomposición de A, lo que implica que $A_M \sim \mathrm{Mat}_n(M)$. Por lo tanto $[A] \in \mathrm{Br}(M/K)$.

Partiendo de un $c \in Z^2(G, M^*)$ (el que definía la multiplicación en (M, G, c)), hemos obtenido un $[(M, G, c)] \in \mathrm{Br}(M/K)$. Sea ahora $c' \in Z^2(G, M^*)$ tal que $[c] = [c']$ en $H^2(G, M^*)$. Entonces

$$c'_{\sigma,\tau} = c_{\sigma,\tau}(a_\sigma(\sigma a_\tau)a_{\sigma\tau}^{-1})$$

para $\sigma, \tau \in G$ y una aplicación $a : G \to M^*$. Sea $A' = (M, G, c')$ con base $\{e'_\sigma : \sigma \in G\}$ (la base "canónica"). Si fijamos $u_\sigma = a_\sigma e_\sigma$, los u_σ forman una base de $A = (M, G, c)$. Por las relaciones de multiplicación de los e_σ:

$$u_\sigma b = a_\sigma u_\sigma b = a_\sigma(\sigma b)e_\sigma = (\sigma b)u_\sigma$$

y

$$u_\sigma u_\tau = a_\sigma e_\sigma a_\tau e_\tau = a_\sigma(\sigma a_\tau)e_\sigma e_\tau = a_\sigma(\sigma a_\tau)c_{\sigma\tau}e_{\sigma\tau} = a_\sigma(\sigma a_\tau)c_{\sigma\tau}a_{\sigma\tau}^{-1}u_{\sigma\tau} = c'_{\sigma\tau}u_\sigma.$$

Por lo tanto podemos definir un isomorfismo $A \to A'$, $\sum a_\sigma u_\sigma \mapsto \sum a_\sigma e'_\sigma$. Por lo tanto A y A' son isomorfos y obviamente $[A] = [A']$ en $\mathrm{Br}(M/K)$. Por lo tanto tenemos una aplicación $H^2(G, M^*) \to \mathrm{Br}(M/K)$, $[c] \mapsto [(M, G, c)]$ que está bien definida.

Esta aplicación es en realidad un homomorfismo:

Proposición 3.8. $(M, G, c) \otimes_K (M, G, d) \sim (M, G, cd)$.

Demostración. Teorema 8.9, sección 8.4 de [4] (página 479).

Y finalmente (y el motivo de nuestro interés por el grupo de Brauer), es un isomorfismo:

Teorema 3.5. *Sea M/K una extensión de Galois y $G = \mathrm{Gal}(M/K)$. Entonces la aplicación $H^2(G, M^*) \to \mathrm{Br}(M/K)$, $[c] \mapsto [M, G, c]$ es un isomorfismo.*

Demostración. Veamos primero que es sobreyectivo: Sea A/K una CSA con cuerpo de descomposición M, entonces existe una CDA D tal que $A \simeq \mathrm{Mat}_r(D)$, $r \in \mathbb{N}$ y

además M también es cuerpo de descomposición de D. Entonces por el Teorema 3.4 M es subcuerpo de $B = \mathrm{Mat}_s(D)$ para un $s \in \mathbb{N}$ y $C_B(M) = M$. Obviamente $A \sim B$. Si consideramos ahora la aplicación $M \to M$, $a \mapsto \sigma a$ (con $\sigma \in G$), en particular es una inmersión de M en B y por el Teorema 3.2 $\sigma a = u_\sigma a u_\sigma^{-1}$ para un $u_\sigma \in A$ invertible. Tenemos

$$(\sigma a)u_\sigma = u_\sigma a, \ y\ u_\sigma^{-1}(\sigma a) = a u_\sigma^{-1}$$

por lo que

$$u_\sigma u_\tau u_{\sigma\tau}^{-1} a = a u_\sigma u_\tau u_{\sigma\tau}^{-1}$$

y $u_\sigma u_\tau u_{\sigma\tau}^{-1} \in C_B(M)$. Como $C_B(M) = M$, podemos escribir $u_\sigma u_\tau = c_{\sigma,\tau} u_{\sigma\tau}^{-1}$ para una aplicación $c : G \times G \to M^*$. La asociatividad nos da que $c \in Z^2(G, M^*)$ y si nos fijamos hemos construido el producto cruzado (M, G, c) como subálgebra de B. Ahora bien, tenemos que M es un subálgebra de B, luego por el Teorema 3.3 $B \simeq M \otimes_K C_B(M)$. Por lo tanto $[B : K] = [M : K][C_B(M) : K] = [M : K]^2 = n^2 = [(M, G, c) : K]$. Por lo tanto $(M, G, c) \simeq B$ y $[M, G, c] = [A]$.

Veamos ahora la inyectividad: Sean $[M, G, c] = [M, G, d]$. Nuestro objetivo es probar que $[c] = [d]$. Tanto (M, G, c) como (M, G, d) tienen la misma dimensión, luego por construcción es obvio que son isomorfas. Sea $\varphi : (M, G, c) \to (M, G, d)$ un isomorfismo, en particular $\varphi|_M$ es una inmersión de M en (M, G, d), luego por el Teorema 3.2 existe $u \in (M, G, d)$ invertible tal que $\varphi(a) = uau^{-1}$ para todo $a \in M$. Si ahora hacemos $\varphi' : (M, G, c) \to (M, G, d)$, $\varphi'(x) = u^{-1}\varphi(x)u$, obviamente sigue siendo un isomorfismo, y además $\varphi'(a) = a$ para todo $a \in M$. Esto junto a las reglas de multiplicación de las bases u_σ y v_σ de (M, G, c) y (M, G, d) respectivamente resulta en

$$v_\sigma \varphi(u_\sigma)^{-1} a = v_\sigma (\sigma a)^{-1} \varphi(u_\sigma)^{-1} = a v_\sigma \varphi(u_\sigma)^{-1}$$

para todo $a \in M$. Por lo tanto $v_\sigma \varphi(u_\sigma)^{-1} \in C_{(M,G,d)}(M) = M$ y existe una aplicación $a : G \to M^*$ tal que $a_\sigma = v_\sigma \varphi(u_\sigma)^{-1}$. Entonces

$$d_{\sigma,\tau} = v_\sigma v_\tau v_{\sigma\tau}^{-1} = a_\sigma \varphi(u_\sigma) a_\tau \varphi(u_\tau) \varphi(u_{\sigma\tau})^{-1} a_{\sigma\tau}^{-1} = a_\sigma (\sigma a_\tau) \varphi(u_\sigma) \varphi(u_\tau) \varphi(u_{\sigma\tau})^{-1} a_{\sigma\tau}^{-1} = a_\sigma (\sigma a_\tau) a_{\sigma\tau}^{-1} c_{\sigma,\tau}$$

y por lo tanto $[d] = [c]$ tal y como queríamos. ∎

Proposición 3.9. Sea L/K una extensión de Galois y M/K una subextensión de Galois con grupos $G = \mathrm{Gal}(L/K)$ y $H = \mathrm{Gal}(M/K)$. Entonces la inflación $\inf : H^2(H, M^*) \to H^2(G, L^*)$ corresponde con la inclusión $\mathrm{Br}(M/K) \subseteq \mathrm{Br}(L/K)$.

Demostración. Consideremos el producto cruzado (M, H, c), la restricción $G \to H$, $\sigma \mapsto \tilde{\sigma}$, y $\{x_1, \ldots, x_r\}$ una base de L/M. Queremos probar que $[(M, G, c)] = [(L, H, \inf c)] \in \mathrm{Br}(L/K)$.

Obviamente L es un M-espacio vectorial, y dado $a \in L$, la aplicación $x \mapsto ax$ es un endomorfismo, luego tiene una representación matricial $B(a)$ en la base fijada. Consideremos ahora la aplicación $L \to \mathrm{Mat}_r(M)$, $a \mapsto B(a)$, que es un homomorfismo de álgebras inyectivo ($B(a)$ es la matriz diagonal aI). Por lo tanto tenemos una inmersión de L en $\mathrm{Mat}_r(M) \subseteq \mathrm{Mat}_r((M, H, c))$.

Consideremos ahora la aplicación $\sum_i a_i x_i \mapsto \sum_i a_i(\sigma x_i)$, con $a_i \in L$ y $\sigma \in G$, que es de nuevo un M-endomorfismo en L, y cuya matriz respecto de la base fijada denotamos V'_σ. Además, teniendo en cuenta que V'_σ manda a $\sum_i(\sigma a_i)a_i$ en $\sum_i a_i(\sigma x_i)$ tenemos que $V'_\sigma(\sigma V'_\tau) = V'_{\sigma\tau}$. Hagamos ahora $V_\sigma = \sigma^{-1}V'_\sigma$, entonces

$$V_{\sigma\tau} = \tau^{-1}\sigma^{-1}V'_{\sigma\tau} = (\tau^{-1}\sigma^{-1}V'_\sigma(\sigma V'_\tau)) = (\tau^{-1}V_\sigma)V_\tau.$$

Consideremos la base $\{u_\tau : \tau \in H\}$ de (M, H, c). Consideramos la proyección canónica $G \to H$ y denotemos $\tilde{\sigma}$ a la imagen de $\sigma \in G$. Entonces definimos $W_\sigma = u_{\tilde{\sigma}}IV_\sigma$, que verifica

$$W_\sigma W_\tau = u_{\tilde{\sigma}}IV_\sigma u_{\tilde{\tau}}IV_\tau = u_{\tilde{\sigma}}u_{\tilde{\tau}}I(\tau^{-1}V_\sigma)V_\tau = u_{\tilde{\sigma}}u_{\tilde{\tau}}IV_{\sigma\tau} = c_{\tilde{\sigma},\tilde{\tau}}IW_{\sigma\tau}.$$

Además de esta igualdad también se verifica

$$W_\sigma B(a) = u_{\tilde{\sigma}}aIV_\sigma = (\sigma a)u_{\tilde{\sigma}}IV_\sigma = B(\sigma a)W_\sigma.$$

En ambas igualdades hemos utilizado que los coeficientes de V_σ y $B(a)$ están en L (representan un L-endomorfismo) y por lo tanto la acción de $\mathrm{Gal}(L/K)$ coincide con la de $\mathrm{Gal}(M/K)$, luego podemos "intercambiar" σ y $\tilde{\sigma}$ cuando operan sobre dichas matrices.

Con todo esto tenemos $(L, G, \inf c)$ dentro de $\mathrm{Mat}_r(M)$ y por tanto en $\mathrm{Mat}_r((M, H, c))$. Si calculamos las dimensiones, tenemos por un lado que si $[L : M] = r$, $[L : K] = n$ y $[M : K] = s$, entonces $n = rs$. Por otro lado

$$[\mathrm{Mat}_r((M, H, c)) : K] = r^2s^2 = n^2 = [(L, G, \inf c)],$$

luego $(L, G, \inf c) \simeq \mathrm{Mat}_r((M, H, c))$ y por tanto $(L, G, \inf c) \sim (M, H, c)$ en $\mathrm{Br}(L/K)$ tal y como queríamos. ∎

Proposición 3.10. Sea L/K una extensión de Galois con $G = \mathrm{Gal}(L/K)$ y sea M/K una subextensión con $H = \mathrm{Gal}(L/M)$. Entonces la restricción $\mathrm{res} : H^2(G, M^*) \to H^2(H, M^*)$ corresponde con la restricción

$$\begin{aligned} \mathrm{Br}(L/K) &\to \mathrm{Br}(L/M) \\ [A] &\mapsto [A_M] \end{aligned}$$

Sea M/K Galois con $G = \mathrm{Gal}(M/K)$ y $|G| = n$. Entonces $c^n = 1$ para todod $c \in Z^2(G, M^*)$, por lo que $(M, G, c)^n \sim 1$ en $\mathrm{Br}(K)$. Esto se puede afinar más: sea A/K una CSA y D/K la CDA correspondiente al Teorema 3.1 tal que $A \simeq \mathrm{Mat}_r(D)$. Entonces se tiene $[A : K] = n^2 = r^2 d$, donde $d = [D : K]$. Como D es en particular una CSA, $d = s^2$ para algún $s \in \mathbb{N}$ y por tanto tenemos $n = rs$. Como D es único salvo isomorfismo, s es único y lo llamamos **índice** de A y denotamos $s(A) = s$.

Proposición 3.11. Sea A/K una CSA. Entonces $A^{s(A)} \sim 1$ en $\mathrm{Br}(K)$.

3.3 Álgebras cíclicas

Sea M/K una extensión de Galois cíclica con $C_n = \mathrm{Gal}(M/K)$ y fijemos un generador $\sigma \in C_n$. Entonces ya vimos en los ejemplos del capítulo anterior (2.3.1) que teníamos el isomorfismo

$$H^2(C_n, M^*) \simeq (M^*)^{C_n}/N_{M/K}(M^*)$$

y por lo tanto

$$\mathrm{Br}(M/K) \simeq K^*/N_{M/K}(M^*).$$

donde si $a \in K^*$ es el elemento que determinaba el sistema de factores c, ahora le corresponde la clase de $[M, C_n, c]$, donde (M, C_n, c) no es más que el K-álgebra $M[u]$, donde $u^n = a$ y $ux = (\sigma x)u$, $x \in M$. A este producto cruzado (M, C_n, c) lo denotamos por (M, σ, a) y decimos que es el **álgebra cíclica** definida por la extensión M/K.

Definición 3.8. *Sea K un cuerpo de característica distinta de 2. Una K-álgebra Q se dirá que es un **álgebra de cuaterniones** si Q está generada sobre K por elementos i y j con las relaciones $i^2 = a$, $j^2 = b$ y $ji = -ij$, con $a, b \in K^*$. Esta álgebra tiene dimensión 4 sobre K y una base es $\{1, i, j, ij\}$*

Dados $a, b \in K^*$, el álgebra de cuaterniones correspondiente la denotamos por $(a, b/K)$.

Ejemplo 3.3. Los cuaterniones "clásicos", $(-1, -1/\mathbb{R})$.

El álgebra de matrices $\mathrm{Mat}_2(K)$: dados $x, b \in K^*$ y $a = x^2$, las matrices

$$I = \begin{pmatrix} x & 0 \\ 0 & -x \end{pmatrix} \text{ y } J = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$$

generan $\mathrm{Mat}_2(K)$ y verifican $I^2 = a\,\mathrm{Id}$, $J^2 = b\,\mathrm{Id}$ y $JI = -IJ$, por lo que tenemos un isomorfismo $K[i, j] \simeq \mathrm{Mat}_2(K)$.

Proposición 3.12. Sea K un cuerpo de característica distinta de 2. Entonces toda CSA A/K de dimensión 4 es isomorfa a un álgebra de cuaterniones.

Demostración. Sea A/K una CSA de dimensión 4, sabemos que existe una CDA D tal que $A \simeq \mathrm{Mat}_r(D)$. Entonces tenemos $4 = [A : K] = [\mathrm{Mat}_r(D) : D] : [D : K] = r^2[D : K]$. Tenemos por lo tanto dos opciones: si $r = 1$ entonces $A \simeq D$, luego A es una CDA; si $r = 2$ entonces $D = K$ y $A \simeq \mathrm{Mat}_2(K)$.

Tenemos entonces dos casos. Si $A \simeq \mathrm{Mat}_2(K)$, por el ejemplo anterior hemos terminado. Por lo tanto veamos el caso en que A/K es una CDA.

Sea $d \in A \setminus K$ y consideremos un polinomio irreducible $f \in K[x]$ tal que $f(d) = 0$. Por lo tanto tenemos una inmersión $K[X]/\langle f \rangle \to A$ y por lo tanto $K(d)$ es una subálgebra de A. Calculando dimensones, $4 = [A : K] = [A : K(d)][K(d) : K]$ y tenemos que $[K(d) : K] = 2$ ya que $d \notin K$ y $K(d) \neq D$. Por lo tanto $d = \sqrt{a}$ para un $a \in K^*$ que no sea un cuadrado. Por el Teorema 3.4, $K(\sqrt{a})$ es cuerpo de descomposición de $A \otimes_K K(\sqrt{a})$ y por lo tanto $A \in \mathrm{Br}(K(\sqrt{a})/K)$. Ahora bien, $\mathrm{Br}(K(\sqrt{a})/K) \simeq \mathrm{Gal}(K(\sqrt{a})/K) = C_2$, por lo que como estamos en el caso $A \nsim K$ tenemos que $A = (K(\sqrt{a}), \sigma, b)$ para un $b \in K^*$ y σ el generador de $C_2 = \mathrm{Gal}(K(\sqrt{a})/K)$.

Fijando ahora $i = \sqrt{a}$ y $j = u$ (el correspondiente al álgebra cíclica que hemos visto al principio de la sección), entonces $A = K[i, j]$ con $i^2 = a$, $j^2 = b$ y $ji = -ij$. Por lo tanto A es un álgebra de cuaterniones. ∎

Como hemos visto en esta prueba, $(K(\sqrt{a}), \sigma, b)$ es un álgebra de cuaterniones para $a, b \in K^*$ si a no es un cuadrado. También, utilizando esta construcción y lo que vimos sobre los sistemas de factores de grupos cíclicos, $(a, b/K) \sim 1$ si y sólo si b es una norma en $K(\sqrt{a})/K$.

Las clases de álgebras de cuaterniones en $\mathrm{Br}(K)$ son más fáciles de tratar:

Proposición 3.13. Denotemos por (a, b) a la clase de $(a, b/K)$ en $\mathrm{Br}(K)$. Entonces se verifica:

1. $(a, b) = (b, a)$ y $(ax^2, by^2) = (a, b)$ para $x, y \in K^*$.
2. $(a, -a) = 1$ y $(a, 1 - a) = 1$ para $a \in K^* \setminus \{1\}$.
3. $(a, a) = (a, -1)$.
4. $(aa', b) = (a, b)(a', b)$ y $(a, bb') = (a, b)(a, b')$

Podemos generalizar el concepto de los cuaterniones de la siguiente manera:

Definición 3.9. *Sea p primo, K un cuerpo de característica distinta de p y $\zeta \in K$ una raíz p-ésima de la unidad primitiva. Entonces dados $a, b \in K^*$ definimos el* ***álgebra p-cíclica****, que denotamos $(a, b/K)_p$, como el álgebra generada sobre K por los elementos i y j verificando $i^p = a$, $j^p = b$ y $ji = \zeta ij$.*

Un álgebra p-cíclica tiene dimensión p y razonando de manera similar a los cuaterniones va a ser o bien el álgebra cíclica (M, σ, b) con $M = K(\sqrt[p]{a})$ y $\sigma(\sqrt[p]{a}) = \zeta\sqrt[p]{a}$, cuando a no es una pontencia p-ésima; y cuando sí lo sea, vamos a tener el álgebra $\mathrm{Mat}_p(K)$. Igualemente, $(a, b/K)_p \sim 1$ si y sólo si b es una norma en $K(\sqrt[p]{a})/K$.

Y se van a cumplir propiedades similares a las de las álgebras de cuaterniones:

Proposición 3.14. Denotemos por $(a, b)_p$ a la clase de $(a, b/K)_p$ en $\mathrm{Br}(K)$. Entonces se verifica:

1. $(a, b)_p(b, a)_p = 1$ y $(ax^p, by^p)_p = (a, b)_p$ para $x, y \in K^*$.
2. $(aa', b)_p = (a, b)_p(a', b)_p$ y $(a, bb')_p = (a, b)_p(a, b')_p$.

3.4 El problema de inmersión

Si recordamos el Corolario 2.1, dado un cuerpo K con característica distinta de p primo tal que $\mu_p \subseteq K^*$, una extensión de Galois M/K con $G = \mathrm{Gal}(M/K)$ y

$$1 \to \mu_p \to E \xrightarrow{\pi} G \to 1$$

una extensión central con clase de cohología $[c] \in H^2(G, \mu_p)$, entonces el problema de inmersión $(M/K, E, \pi, \mu_p)$ es resoluble si y sólo si $i^*([c]) = [1] \in M^*$. Ahora, por el Teorema 3.5, esto ocurre si y sólo si $[M, G, c] = 1 \in \mathrm{Br}(M/K) \subseteq \mathrm{Br}(K)$.

Definición 3.10. *A la clase $[(M, G, c)]$ la denominaremos* ***la obstrucción*** *del problema de inmersión, mientras que un representante $A \sim (M, G, c)$ diremos que es* ***una*** *obstrucción.*

Dada una obstrucción (M, G, c), con base $\{u_\sigma : \sigma \in G\}$, podemos expresarla en función de E: Consideremos la extensión central notación de la extensión

$$1 \longrightarrow \mu_m \xhookrightarrow{i} F \xrightarrow{u_\sigma \mapsto \sigma} G \longrightarrow 1$$

donde F es subgrupo de (M, G, c) generado por los u_σ y μ_m (recordemos que $u_\sigma u_\tau = c_{\sigma,\tau} u_{\sigma\tau}$ y $c_{\sigma,\tau} \in \mu_m$). Calculemos la clase de esta extensión, que pertenece a $H^2(G, \mu_m)$.

Tomando como sección a $\sigma \mapsto u_\sigma$, como $u_\sigma u_\tau = c_{\sigma,\tau} u_{\sigma,\tau}$ la clase va a ser $[c] \in H^2(G, \mu_m)$. Como ambas extensiones tiene la misma clase, son equivalentes y existe un isomorfismo $F \to E$ que conmuta con las extensiones. Por dicha conmutatividad, envía a $\mu_m \subseteq F$ en $\operatorname{Ker} \pi \subseteq E$ y podemos entonces ver (M, G, c) generado sobre M por E identificando $\operatorname{Ker} \pi$ con μ_m. Para la multiplicación con elementos de M, cosideramos la acción de E a través de π (es decir $(\sigma x) = (\pi(\sigma)x)$), $\sigma \in E$, $x \in M$).

El Teorema 3.3 nos dice que dada una CSA A/K, si encontramos una subálgebra B que también sea CSA, entonces $A \simeq B \otimes_K C_A(B)$, y $C_A(B)$ también es una CSA. Por lo tanto el objetivo es intentar que esa subálgebra B sea o de cuaterniones o p-cíclica, y repetir el proceso con $C_A(B)$ para tener una descomposición de A (siendo A la obstrucción).

3.5 Ejemplos

Con todo esto, volvamos a los ejemplos del capítulo anterior:

3.5.1 Grupos cíclicos

Sea K un cuerpo de característica distinta de p primo y tal que $\mu_p \subseteq K$ y sea M/K una extensión de Galois cíclica de grado p^n, $n \in \mathbb{N}$. Escojamos un generador $\sigma \in C_{p^n} = \operatorname{Gal}(M/K)$ y una raíz primitiva $\zeta \in \mu_p$ y consideremos la extensión

$$1 \to \mu_p \xrightarrow{\zeta \mapsto \tilde{\sigma}^{p^n}} C_{p^{n+1}} \xrightarrow{\tilde{\sigma} \mapsto \sigma} C_{p^n} \to 1$$

Entonces, hemos visto que la obstrucción del problema $(M/K, C_{p^{n+1}}, \pi, \mu_p)$ es la clase $[M, \sigma, \zeta] \in \operatorname{Br}(K)$ del álgebra cíclica (M, σ, ζ).

Para $n = 1$ tenemos $M = K(\sqrt[p]{a})$ para algún $a \in K^*$ y el generador $\sigma \in \operatorname{Gal}(M/K)$ viene dado por $\sigma(\sqrt[p]{a}) = \zeta \sqrt[a]{p}$. Por lo tanto la obstrucción es la clase del álgebra p-cíclica $(a, \zeta)_p \in \operatorname{Br}(K)$.

Si además tomamos $p = 2$ tenemos el álgebra de cuaterniones $(a, -1/K)$, y por las propiedades de las mismas $(a, -1) = (a, a)$ en $\operatorname{Br}(K)$. Por lo tanto, el problema tiene solución si y sólo si $(a, a) \sim 1$, lo cuál ocurre si y sólo si a es una norma en $K(\sqrt{a})/K$ tal y cómo vimos en el capítulo anterior.

3.5.2 El grupo diedral D_4

Análogo al capítulo anterior, consideremos la extensión $K(\sqrt{a}, \sqrt{b})/K$ con $\mathrm{Gal}(K(\sqrt{a}, \sqrt{b})/K) = K_4$, generadores $\sigma, \tau \in K_4$ (recordemos que $\sigma(\sqrt{a}) = -\sqrt{a}$ y $\tau(\sqrt{b}) = -\sqrt{b}$) y la extensión

$$1 \to \mu_2 \to D_4 \xrightarrow[\tau \mapsto \tau]{\sigma \mapsto \sigma} K_4 \to 1$$

Entonces, como $\mathrm{Ker}\, \pi = \{1, \sigma^2\}$, tenemos que (M, K_4, c) esta generado por u_σ y u_τ que verifican

$$u_\sigma^4 = 1,\ u_\tau^2 = 1,\ u_\tau u_\sigma = u_\sigma^3 u_\tau$$

las relaciones de E y $u_\sigma^2 = -1$ por $\mathrm{Ker}\, \pi = \mu_2$. Por lo tanto, tomando $u = u_\sigma$ y $u = u_\tau$, (M, K_4, c) esta generado sobre M por u y v verificando

$$u^2 = -1,\ v^2 = 1,\ vu = -uv,$$

$$ux = (\sigma x)u,\ vx = (\tau x)v,\ \forall x \in M$$

Si consideramos la subálgebra $K[u, v]$, tenemos entonces que es el álgebra de cuaterniones $Q = (-1, 1/K)$. Calculemos $C_{(M,K_4,c)}(Q)$. Primero tenemos que $\sqrt{a}v \in C_{(M,K_4,c)}(Q)$ ya que tenemos

$$\sqrt{a}vv = v\sqrt{a}v,\ \sqrt{a}vu = -\sqrt{a}uv = u\sqrt{a}v,\ \sqrt{a}vuv = v\sqrt{a}uv = -vu\sqrt{a}v = uv\sqrt{a}v.$$

Análogamente ocurre con $\sqrt{b}u$. Entonces tenemos que $K[\sqrt{a}v, \sqrt{b}u] \subseteq C_{(M,K_4,c)}(Q)$ y la igualdad por dimensión. Como $(\sqrt{a}v)^2 = a$, $(\sqrt{b}u) = -b$ y $\sqrt{a}v\sqrt{b}u = -\sqrt{b}u\sqrt{a}v$, entonces $K[\sqrt{a}v, \sqrt{b}u] = (a, -b/K)$. Por lo tanto la obstrucción es $(-1, 1)(a, -b) = (a, -b) = (a, ab) \in \mathrm{Br}(K)$, y el problema es resoluble si y sólo si ab es una norma en $K(\sqrt{a})/K$.

3.5.3 El grupo de Heisenberg

Como vimos en 2.3.3, sea p un primo distinto de 2 y consideremos el grupo de Heisenberg H_{p^3}, la extensión $M/K = K(\sqrt[p]{a}, \sqrt[p]{b})/K$ con $\mathrm{Gal}(M/K) = C_p \times C_p$ y σ, τ dos generadores. Consideremos el problema dado por M/K y la extensión

$$1 \to \mu_p \xrightarrow{\zeta \mapsto w} H_{p^3} \xrightarrow[v \mapsto \tau]{u \mapsto \sigma} C_p \times C_p \to 1$$

Entonces $(M, C_p \times C_p, c)$ está generado sobre M por E haciendo $w = \zeta$, es decir por los elementos u y v tales que

$$u^p = v^p = 1 \quad y \quad uv = \zeta vu$$

con las reglas de multiplicación

$$ux = (\sigma x)u \quad y \quad vx = (\tau x)v,\ x \in M$$

Tenemos entonces que $K[u, v] \simeq (1, 1/K)_p$ es una subálgebra p-cíclica, y por un razonamiento parecido al del ejemplo anterior, su centralizador es $K[\sqrt[p]{b}u^{p-1}, \sqrt[p]{a}v] \simeq (b, a/K)_p$. Por lo tanto la obstrucción es $(1, 1)_p(b, a)_p = (b, a)_p \in \mathrm{Br}(K)$.

3.5.4 Extensiones de D_4

Sea K un cuerpo de característica distinta de 2, M/K una extensión de Galois con grupo de Galois $\mathrm{Gal}(M/K) = D_4$ y consideremos los problemas de inmersión dados por M/K y las extensiones centrales no escindidas de la forma

$$1 \to \mu_2 \to E \to D_4 \to 1$$

La extensión M/K la tomamos como vimos en el Ejemplo 2.3.2, es decir $M = K(\sqrt{r(\alpha + \beta\sqrt{a}}, \sqrt{b})$ con $a, b \in K^*$ tales que a/b no es un cuadrado, $\alpha, \beta \in K$ tales que $\alpha^2 - a\beta^2 = ab$ y $r \in K^*$. Además, $\sigma, \tau \in D_4$ vienen dados por

$$\sigma(\sqrt{r(\alpha + \beta\sqrt{a})}) = \frac{\sqrt{a}\sqrt{b}}{\alpha + \beta\sqrt{a}}\sqrt{r(\alpha + \beta\sqrt{a})}, \quad \sigma(\sqrt{b}) = \sqrt{b};$$

y

$$\tau(\sqrt{r(\alpha + \beta\sqrt{a})}) = \sqrt{r(\alpha + \beta\sqrt{a})}, \quad \tau(\sqrt{b}) = -\sqrt{b}.$$

Nuestro objetivo es dar una descomposición de la obstrucción para todos estos problemas. Para eso vamos a dar la imagen del homomorfismo $H^2(D_4, \mu_2) \to \mathrm{Br}(M/K)$ resultante de componer la inclusión $H^2(D_4, \mu_2) \hookrightarrow H^2(D_4, M^*)$ con el isomorfismo $H^2(D_4, M^*) \simeq \mathrm{Br}(M/K)$.

Empecemos caracterizando $H^2(D_4, \mu_2)$: supongamos que tenemos una extensión central

$$1 \to \mu_2 \to E \to D_4 \to 1$$

con clase de cohomología $\gamma \in H^2(D_4, \mu_2)$.Entonces si tomamos preimágenes $s, t \in E$ de los generadores $\sigma, \tau \in D_4$ e identificando Ker π con μ_2 se debe de cumplir

$$s^4 = \epsilon_1, \quad t^2 = \epsilon_2, \quad ts = \epsilon_3 s^3 t,$$

con $(\epsilon_1, \epsilon_2, \epsilon_3) \in \mu_2^3$. Asociamos este elemento de μ_2^3 a la clase γ y tenemos una aplicación $H^2(D_4, \mu_2) \to \mu_2^3$. Para ver que la aplicación está bien definida supongamos que tomamos preimágenes distintas $s', t' \in E$. Entonces tanto s y s' como t y t' se diferencian en un elemento de ker π, es decir en un elemento de μ_2, por lo que

$$s'^4 = s^4 = \epsilon_1, \quad t'^2 = t^2 = \epsilon_2, \quad t's'(s'^3t')^{-1} = ts(s^3t)^{-1} = \epsilon_3,$$

y por lo tanto la imagen de γ no depende de los generadores escogidos.

Para ver que esta aplicación es un homomorfismo, tenemos que utilizar la suma de Baer (Definición 1.11). Dadas dos extensiones con clases de cohomología γ y γ' respectivamentes y con imágenes $(\epsilon_1, \epsilon_2, \epsilon_3)$ y $(\epsilon_1', \epsilon_2', \epsilon_3')$ respectivamente, y preimágenes s, t y s', t'; entonces si consideramos la suma de Baer de ambas extensiones (que tiene clase de cohomología $\gamma\gamma'$) podemos tomar como preimágenes (s, s') y (t, t'). Por lo tanto, utilizando que los elementos de μ_2 son sus propios inversos, la imagen de dicha extensión sería $(\epsilon_1\epsilon_1', \epsilon_2\epsilon_2', \epsilon_3\epsilon_3')$ tal y como queríamos.

Este homomorfismo es inyectivo, ya que si tomamos la clase trivial $[1] \in H^2(D_4, \mu_2)$, la extensión correspondiente tiene $E = \mu_2 \times D_4$ y claramente su imagen es $(1, 1, 1) \in \mu_2^3$.

Para ver que es sobreyectivo (y por tanto un isomorfismo) vamos a tomar generadores de μ_2^3, en particular $(-1, 1, 1)$, $(1, -1, 1)$ y $(1, 1, -1)$, y vamos a dar una extensión central con imagen cada generador.

Consideremos el grupo semidiédrico

$$QD_8 = \langle u, v : u^8 = v^2 = 1,\ vu = u^3v \rangle$$

y la extension

$$1 \longrightarrow \mu_2 \xrightarrow{-1 \mapsto u^4} QD_8 \xrightarrow[v \mapsto \tau]{u \mapsto \sigma} D_4 \longrightarrow 1$$

Entonces tomando $s = u$ y $t = v$ la imagen correspondiente es $(-1, 1, 1)$

Ahora consideremos el producto semidirecto $C_4 \rtimes C_4$ (tomando la acción de C_4 en sí mismo mediante la operación de grupo) que lo podemos ver como

$$C_4 \rtimes C_4 = \langle u, v : u^4 = v^4 = 1,\ vu = u^3v \rangle$$

Entonces la extensión

$$1 \longrightarrow \mu_2 \xrightarrow{-1\mapsto v^2} C_4 \rtimes C_4 \xrightarrow[v\mapsto\tau]{u\mapsto\sigma} D_4 \longrightarrow 1$$

tiene imagen $(1,-1,1)$ (tomando $s=u$, y $t=v$).

Por último consideremos el pull-back de $D_4 \to C_2$ y $C_4 \to C_2$, que lo podemos ver como

$$D_4 \curlywedge C_4 = \langle u, v, w : u^4 = v^2 = w^2 = 1,\ uw = wu,\ vw = wv,\ vu = u^3vw\rangle$$

La extensión

$$1 \longrightarrow \mu_2 \xrightarrow{-1\mapsto w} D_4 \curlywedge C_4 \xrightarrow[v\mapsto\tau]{u\mapsto\sigma} D_4 \longrightarrow 1$$

tiene imagen $(1,1,-1)$ (tomando $s=u$, $t=v$).

Hemos visto que generadores de μ_2^3 tienen preimagen en $H^2(D_4,\mu_2)$ luego el homomorfismo es sobreyectivo (y por tanto es un isomorfismo). Tenemos entonces que estas tres extensiones y sus clases son generadores de $H^2(D_4,\mu_2)$. Por lo tanto viendo sus imágenes en $\mathrm{Br}(M/K)$ (es decir las obstrucciones de esos 3 problemas), tendremos el resto.

El grupo QD_8

Consideramos la extensión

$$1 \longrightarrow \mu_2 \xrightarrow{-1\mapsto u^4} QD_8 \xrightarrow[v\mapsto\tau]{u\mapsto\sigma} D_4 \longrightarrow 1$$

y la D_4-extensión M/K dada al principio. La obstrucción $A=(M,D_4,c)$ está generada sobre M por los generadores $u,v\in E$ y la identificación $\mathrm{Ker}\,\pi=\mu_2$, es decir

$$u^4=-1,\ v^2=1,\ vu^3=u^3v$$

y

$$ux=(\sigma x)u \text{ y } vx=(\tau x)v,\ x\in M.$$

Buscamos ahora una subálgebra de cuaterniones Q. Como primer generadores tomamos $\sqrt{a}$ y buscamos ahora un elemento que anticonmute con $\sqrt{a}$ y cuyo cuadrado esté en K. Como $\sigma\sqrt{a}=-\sqrt{a}$, las potencias impares de u anticonmutan con $\sqrt{a}$, y como $(u+u^3)^2=u^2+2u^4+u^6=-2\in K$, tenemos que $Q=K[\sqrt{a},u+u^3]\simeq(a,-2/K)$

es una subálgebra de cuaterniones de A. Tenemos entonces que $A \simeq Q \otimes_K C_A(Q)$. Ahora buscamos una subálgebra de cuaterniones de $C_A(Q)$: primero $\sqrt{b}$ conmuta con $\sqrt{a}$ y con u, luego también con $u+u^3$ y está en $C_A(Q)$; luego v conmuta con $\sqrt{a}$ (ya que $(\tau\sqrt{a}) = \sqrt{a}$) y también con $u+u^3$, ya que $uv = vu^3$ y $vu = u^3v$. Además, v anticonmuta con $\sqrt{b}$ (igual que u lo hacía con $\sqrt{a}$) y por lo tanto tenemos una subálgebra de cuaterniones $Q' = K[\sqrt{b}, v] \simeq (b, 1/K)$ de $C_A(Q)$ y la descomposición $A \simeq Q \otimes_K Q' \otimes_K C_A(Q')$. Como $C_{C_A(Q)}(Q')$ es una CSA de dimensión 4 (la obstrucción era de dimensión $8^2 = 64$), va a ser un álgebra de cuaterniones y por tanto calculándola tendremos la descomposición entera. Dado que $C_{C_A(Q)}(Q') = C_A(Q \cdot Q')$ (es fácil de probar), tenemos que $\sqrt{b}u^2$ conmuta con los generadores de Q y los de Q' y por lo tanto $\sqrt{b}u^2 \in C_A(Q \cdot Q')$. Para encontrar el otro generador buscamos $\theta \in C_A(Q \cdot Q')$ que verifique

$$\theta\sqrt{b}u^2 = -\sqrt{b}u^2\theta, \quad y \quad \theta^2 \in K^*.$$

Se tiene que $\theta = \sqrt{r(\alpha+\beta\sqrt{a})} - \sigma(\sqrt{r(\alpha+\beta\sqrt{a})})u^2$ verifica las condiciones y $\theta^2 = 2r\alpha$. Por lo tanto $C_A(Q \cdot Q') = K[\sqrt{b}u^2, \theta] \simeq (-b, 2r\alpha/K)$ y la obstrucción del problema es

$$(a,-2)(b,1)(-b,2r\alpha) = (a,-2)(-b,2r\alpha) \in \mathrm{Br}(K).$$

El grupo $C_4 \rtimes C_4$

En este caso el problema esta dado por M/K y la extensión

$$1 \longrightarrow \mu_2 \xrightarrow{-1\mapsto v^2} C_4 \rtimes C_4 \xrightarrow[v\mapsto\tau]{u\mapsto\sigma} D_4 \longrightarrow 1$$

cuya clase tiene representante $c_{\sigma^i\tau,\sigma^j\tau} = -1$. Si observamos ahora la extensión

$$1 \longrightarrow \mu_2 \xrightarrow{-1\mapsto\sigma^2} C_4 \xrightarrow{\sigma\mapsto\sigma} C_2 \longrightarrow 1$$

su clase tiene representante $c'_{\sigma,\sigma} = -1$. Ahora bien, si consideramos el cociente $D_4/\langle\sigma\rangle \simeq C_2$ (mediante $\kappa : D_4 \to C_2/\ \tau \mapsto \sigma$). Por lo tanto, como

$$c_{\sigma^i\tau,\sigma^j\tau} = -1 = c'_{\sigma,\sigma} = c'_{\kappa(\sigma^i\tau),\kappa(\sigma^j\tau)}$$

tenemos que esta segunda extensión corresponde a la inflación de la primera.

Viendo D_4 como $\mathrm{Gal}(M/K)$ tenemos que $\kappa D_4 \to C_2$ como $D_4 \to \mathrm{Gal}(K(\sqrt{b})/K)$. Por la Proposición 3.9, la obstrucción de nuestro problema original se corresponde con

la obstrucción dada por la segunda extensión y $K(\sqrt{b})/K$. Como hemos visto en el ejemplo de los grupos cíclicos (para $n = 1$ y $p = 2$) dicha obstrucción es $(b, -1) = (b, b) \in \mathrm{Br}(K)$.

Por lo tanto, el problema es resoluble si y sólo si existen $a, b \in K^*$ tales que a/b no es un cuadrado y $(a, ab) = 1$, es decir ab es una norma en $K(\sqrt{a})/K$ (la condición de la D_4-extensión), y $(b, b) = 1$.

El grupo $D_4 \curlywedge C_4$

Por último, tenemos el problema dado por M/K y la extensión

$$1 \longrightarrow \mu_2 \xrightarrow{-1 \mapsto u\kappa} D_4 \curlywedge C_4 \xrightarrow[v \mapsto \tau]{u \mapsto \sigma} D_4 \longrightarrow 1$$

Un razonamiento análogo al del anterior caso, con $\kappa : D_4 \to C_2$, $\sigma^2 \mapsto \sigma$ tenemos que esta extensión corresponde a la inflación de la extensión

$$1 \to \mu_2 \to C_4 \to \mathrm{Gal}(K(\sqrt{a})/K) \to 1$$

y por tanto la obstrucción es $(a, -1) = (a, a) \in \mathrm{Br}(K)$.

El problema es resoluble si y sólo si existen $a, b \in K^*$ tales que a/b no es un cuadrado y $(a, ab) = (a, a) = 1$, es decir $(a, b) = (a, a) = 1$.

El caso general

Con esto tenemos el siguiente resultado:

Proposición 3.15. Sea M/K una D_4-extensión como hemos descrito al principio y consideremos el problema de inmersión dado por M/K y la extensión central no escindida

$$1 \to \mu_2 \to E \to D_4 \to 1$$

Tomemos preimágenes $s, t \in E$ de los generadores $\sigma, \tau \in D_4$. La obstrucción del problema es

$$[(a, -2)(-b, 2r\alpha)]^i (b, -1)^j (a, -1)^k \in \mathrm{Br}(K)$$

donde $s^4 = (-1)^i$, $t^2 = (-1)^j$ y $ts = (-1)^k s^3 t$..

Con esto podemos ver más ejemplos fácilmente:

El grupo D_8

Sea M/K nuestra D_4-extensión, consideremos el grupo diedral

$$D_8 = \langle \sigma, \tau : \sigma^8 = \tau^2 = 1,\ \tau\sigma = \sigma^7\tau \rangle$$

y la extensión

$$1 \longrightarrow \mu_2 \xrightarrow{-1\mapsto\sigma^4} D_8 \xrightarrow[\tau\mapsto\tau]{\sigma\mapsto\sigma} D_4 \longrightarrow 1$$

Tomando $s = \sigma$ y $t = \tau$ tenemos que $s^4 = -1$, $t^2 = 1$ y $ts = -s^7t$, luego la obstrucción es

$$[(a,-2)(-b,2r\alpha](a,-1) = (a,2)(-b,2)(-b,r\alpha) = (ab,2)(-b,r\alpha) \in \mathrm{Br}(K)$$

Luego el problema es resoluble si y sólo si existen $a, b \in K^*$ tales que a/b no es un cuadrado y $(a, ab) = 1$, es decir ab es una norma en $K(\sqrt{a})/K$ (la condición de la D_4-extensión), y $(ab,2)(-b,r\alpha) = 1 \in \mathrm{Br}(K)$. Como $(a,b)^2 = 1 \in \mathrm{Br}(K)$, esto último equivale a decir que $(ab,2) = (-b,r\alpha)$ y como $r \in K^*$ no está fijado equivale a decir que existe $x \in K^*$ tal que $(ab,2) = (-b,x)$. Si $\alpha = 0$ no hay problema ya que entonces $-b$ es un cuadrado ($-b = \beta^2$) en K y por tanto visto que $(-b,0) \simeq \mathrm{Mat}_2(K) = [1] \in \mathrm{Br}(K)$.

El grupo Q_{16}

De nuevo M/K habitual, consideramos el grupo de cuaterniones

$$Q_{16} = \langle u, v : u^8 = 1,\ v^2 = u^4,\ vu = u^7v \rangle$$

y la extensión

$$1 \longrightarrow \mu_2 \xrightarrow{-1\mapsto u^4} Q_{16} \xrightarrow[v\mapsto\tau]{u\mapsto\sigma} D_4 \longrightarrow 1$$

Entonces, tomando $s = u$ y $t = v$ tenemos que $s^4 = -1$, $t^2 = -1$ y $ts = -s^3t$ por lo que la obstrucción es

$$[(a,-2)(-b,2r\alpha](b,-1)(a,-1) = (ab,2)(-b,r\alpha)(b,-1) \in \mathrm{Br}(K).$$

y por tanto el problema es resoluble si y sólo si existen $a, b \in K^*$ tales que a/b no es un cuadrado y $(a, ab) = 1$, y existe $x \in K^*$ tal que $(ab,2)(b,-1) = (-b,x)$.

Bibliografía

[1] Brown, K. *Cohomology of Groups*. Graduate Texts in Mathematics. Springer New York, 2012.

[2] Gille, P., and Szamuely, T. *Central Simple Algebras and Galois Cohomology*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006.

[3] Ishkhanov, V., Lur′e, B., and Faddeev, D. *The Embedding Problem in Galois Theory*. American Mathematical Society, June 1997.

[4] Jacobson, N. *Basic Algebra II: Second Edition*. Dover Books on Mathematics. Dover Publications, 2012.

[5] Ledet, A. On 2-groups as galois groups. *Canadian Journal of Mathematics 47*, 6 (1995), 1253–1273.

[6] Ledet, A. *Brauer Type Embedding Problems*. No. Vol. 21 in Fields Institute Monographs. AMS, 2005.

[7] Neukirch, J., Schmidt, A., and Wingberg, K. *Cohomology of Number Fields*. Springer Berlin Heidelberg, 2008.

[8] Vila, N. On the inverse problem of Galois theory. *Publ. Mat. 36*, 2B (1992), 1053–1073 (1993).