Sobre el problema de inmersión de la Teoría de Galois

Teresa Crespo Vicente

SOBRE EL PROBLEMA DE INMERSION DE LA TEORÍA DE GALOIS

Teresa Crespo Vicente

Memoria presentada para aspirar al grado de Doctor en Ciencias Matemáticas.

Facultad de Matemáticas
Universidad de Barcelona.

HAGO CONSTAR que la presente memoria ha sido realizada por Teresa Crespo Vicente bajo mi dirección, en la Facultad de Matemáticas de la Universidad de Barcelona.

P. Bayer

Barcelona, septiembre de 1987

Dra. Pilar Bayer Isant.

I N D I C E

I N T R O D U C C I Ó N

El llamado problema de inmersión de la teoría de Galois tiene por datos un cuerpo K, un cuerpo L, extensión de Galois de K con grupo G finito, y una sucesión exacta de grupos finitos:

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

A partir de estos datos, se plantea la existencia de un cuerpo M, extensión de Galois de L con grupo A, que sea asimismo extensión de Galois de K con grupo E y tal que conmute el diagrama:

$$\begin{array}{ccc} E & \longrightarrow & G \\ \downarrow \wr & & \downarrow \wr \\ Gal(M|K) & \longrightarrow & Gal(L|K) \end{array} ,$$

donde el morfismo de la fila inferior asocia a un automorfismo de M sobre K su restricción a L.

Hasse (1948) generaliza la definición de extensión galoisiana de un cuerpo, mediante la introducción de las álgebras galoisianas y estudia el problema de inmersión admitiendo tam-

bién álgebras galoisianas en las soluciones. Ikeda (1960) demuestra que, a partir de un álgebra galoisiana, que sea solución a un problema de inmersión con núcleo A abeliano, sobre un cuerpo de números K, puede construirse un cuerpo solución.

Posteriormente, Höchsmann (1962) da la traducción del problema de inmersión a cohomología de grupos, en el caso en que el grupo A sea abeliano. Obtiene la obstrucción de la resolubilidad del problema de inmersión como un elemento del grupo de cohomología $H^2(G,A)$. En su planteamiento, quedan incluidas como soluciones las álgebras galoisianas. Con ello, cobra mayor importancia el teorema de Ikeda, mediante el cual puede asegurarse que, si la obstrucción es nula, existe un cuerpo solución. Höchsmann y posteriormente Neukirch (1973) dan demostraciones del teorema de Ikeda utilizando cohomología de grupos. El segundo da un enunciado más general con condiciones locales. Neukirch estudia asimismo la existencia de soluciones al problema de inmersión, imponiendo condiciones sobre la ramificación y datos locales.

Otro aspecto del problema de inmersión es el de la construcción efectiva de las soluciones. Históricamente, el primer ejemplo es debido a Dedekind (1897) que construye una extensión de Q con grupo de Galois el grupo de los cuaterniones y conteniendo la extensión $Q(\sqrt{2},\sqrt{3})$. Witt (1936) generaliza la construcción de Dedekind a cualquier extensión bicuadrática de un cuerpo K de característica distinta de 2. Más concretamente, plantea el problema de inmersión dado por K, $L = K(\sqrt{a_1},\sqrt{a_2},\sqrt{a_3})$, con $a_1a_2a_3=1$, $Gal(L|K)\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ y la sucesión exacta:

$$1 \longrightarrow \mathbb{Z}/2\,\mathbb{Z} \longrightarrow H_8 \longrightarrow \mathbb{Z}/2\,\mathbb{Z} \times \mathbb{Z}/2\,\mathbb{Z} \longrightarrow 1$$

donde H_8 es el grupo de los cuaterniones. Demuestra que la resolubilidad de este problema equivale a que la forma traza de la extensión bicuadrática $L|K$ sea equivalente a la identidad sobre K. Verificada esta condición, construye explícitamente todos los cuerpos solución a partir de un cambio de base que pase de la forma traza a la forma identidad.

Recientemente, Massy (1986) estudia problemas de inmersión sobre un cuerpo K de característica distinta de p y conteniendo las raíces p^m- ésimas de la unidad, con p primo, $m \geq 1$, dadas por una extensión de Galois L de K, con grupo G_p, abeliano de exponente p^m, y una sucesión exacta del tipo

$$1 \longrightarrow \mathbb{Z}/p\,\mathbb{Z} \longrightarrow E \longrightarrow G_p \longrightarrow 1 \ .$$

Obtiene fórmulas que permiten construir todos los cuerpos solución para cualquier problema de inmersión resoluble del tipo planteado, utilizando condiciones sobre el elemento de $H^2(G_p, \mathbb{Z}/p\,\mathbb{Z})$ asociado a la extensión.

Serre (1984) da una fórmula que permite el cálculo efectivo de la obstrucción al problema de inmersión dado por:

$$1 \longrightarrow \mathbb{Z}/2\,\mathbb{Z} \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1,$$

con $G \simeq Gal(L|K)$, donde K es un cuerpo de característica distinta de 2 , G un subgrupo del simétrico S_n y $\tilde{G}$ la antiimagen de G en $\tilde{S}_n$, un cierto doble recubrimiento de S_n. Dicha fórmula da la obstrucción al problema de inmersión en función del invariante de Hasse-Witt de la forma cuadrática traza Q_F de $F|K$, subextensión

separable de grado n de L. Queda con ello generalizada la parte del resultado de Witt, citado arriba, relativa a la resolubilidad del problema.

Utilizando la fórmula de Serre, Vila (1983) demuestra la resolubilidad sobre Q del problema de inmersión de la extensión central universal del grupo alternado A_n, para infinitos valores de n, construyendo para ello realizaciones adecuadas de A_n sobre Q. Posteriormente, Bayer,Llorente y Vila (1986) obtienen la resolubilidad sobre Q del problema de inmersión dado por la única extensión no trivial con núcleo $\mathbb{Z}/2\,\mathbb{Z}$ del grupo de Mathieu M_{12}, partiendo de la realización de M_{12} sobre Q dada por Matzat y Zeh (1986).

En esta memoria, estudiamos dos aspectos del problema de inmersión. El primero es la obtención de soluciones con condiciones de ramificación. Para ello, nos resultará más provechoso plantear el problema de inmersión en el contexto más general de la teoría de esquemas. El segundo aspecto estudiado es la construcción explícita de soluciones y nuestro objetivo es generalizar la construcción citada de Witt a las extensiones para las que es aplicable la fórmula de Serre y con G subgrupo del alternado A_n.

La memoria está subdividida en tres capítulos.

En el capítulo I, se revisa primeramente la teoría de Galois sobre esquemas. Obtenemos que todo recubrimiento principal de un esquema conexo X es suma directa de recubrimientos

galoisianos de X, isomorfos (prop. 1.7), generalizando así el resultado de Hasse de que toda K -álgebra galoisiana es suma directa de copias isomorfas de un cuerpo extensión de Galois de K.

El estudio del concepto de recubrimiento universal de un esquema conexo nos permite plantear el problema de inmersión sobre esquemas. Traduciendo a este lenguaje el problema de inmersión sobre un cuerpo de números, con conjunto de ramificación prefijado, se observa que la obstrucción a la resolubilidad de este problema viene dada por un elemento de un grupo de cohomología étale. Esto nos permite obtener condiciones para que, de la resolubilidad de un problema de inmersión sobre un cuerpo de números K, dado por una extensión central con núcleo abeliano, pueda deducirse la existencia de soluciones, con conjunto de ramificación prefijado. Dichas condiciones se expresan en términos de número de clases de ideales del anillo de enteros de K (teorema 1.20 y corolario 1.21).

Abordamos, en el capítulo II, una generalización del teorema de Ikeda, mencionado arriba. Concretamente, para un problema de inmersión sobre un cuerpo de números y dado por una extensión con núcleo abeliano, nos planteamos si es posible construir, a partir de un álgebra solución, un cuerpo solución, sin aumentar el conjunto de ramificación. Para ello, estudiamos previamente la variedad de las soluciones a un problema de inmersión sobre un cuerpo. En el caso de una extensión central, damos una respuesta afirmativa al problema planteado (teore-

ma 2.8).

Posteriormente, recordamos una formulación clásica de la obstrucción a problemas de inmersión con núcleo $\mathbb{Z}/p\,\mathbb{Z}$, con p primo, sobre un cuerpo K de característica distinta de p y conteniendo las raíces p-ésimas de la unidad. Para p=2 y una extensión a la que sea aplicable la fórmula de Serre, mencionada anteriormente, relacionamos ambas formulaciones de la obstrucción. Estos resultados se usan en el capítulo III.

El objetivo del capítulo III es construir explícitamente las soluciones al problema de inmersión, sobre un cuerpo K de característica distinta de 2, dado por extensiones a las que es aplicable la fórmula de Serre y en el caso en que G está incluido en el alternado A_n. Estas son extensiones del tipo

$$1 \longrightarrow \mathbb{Z}/2\,\mathbb{Z} \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1,$$

con $\tilde{G}$ antiimagen de G en $\tilde{A}_n$.

Se observa que se obtienen todas las soluciones al problema de inmersión, a partir de una dada. Realizamos la construcción de una solución, obteniéndola en términos de la norma espinorial de un elemento del álgebra de Clifford de Q_F (teorema 3.15). En el caso en que Q_F sea equivalente sobre K a la identidad, obtenemos la expresión explícita de la solución en función de un cambio de base que pase de Q_F a la forma cuadrática identidad (teorema 3.17). Este caso incluye el

del problema de inmersión estudiado por Witt, explicado más arriba ([S_3]3.2). Se comprueba que, para este caso, la solución obtenida coincide con la dada por Witt. Más generalmente, si Q_F es equivalente sobre K a una forma cuadrática del tipo

$$Q_q = -(X_1^2 + X_2^2 + \ldots + X_q^2) + X_{q+1}^2 + \ldots + X_n^2 \quad ,$$

obtenemos también la expresión explícita de la solución, en este caso, en función de un cambio de base que pase de Q_F a Q_q (teorema 3.24). Se observa que, para un problema de inmersión resoluble sobre Q, se verifica siempre que Q_F es equivalente sobre Q a la identidad o a una forma cuadrática del tipo Q_q. Con estos resultados, damos respuesta a la pregunta formulada por Serre ([S_3] 3.2. Remarque), que plantea el extender la construcción de Witt a otros casos.

De los resultados citados que se encuentran en la literatura, damos una referencia explícita.

Finalmente, deseo expresar mi agradecimiento a la Dra. Pilar Bayer por la orientación, el estímulo y la valiosa ayuda que me ha procurado constantemente durante la realización de este trabajo.

Quiero también agradecer al Profesor Jürgen Neukirch la amable atención que me dedicó durante su estancia en Barcelona, así como sus indicaciones sobre la generalización del teorema de Ikeda.

A mis compañeros de la Cátedra de Matemáticas de la

E.U.A.T.B. y, en especial, al Dr. Francesc Panyella, les agradezco el haberme facilitado la dedicación a este trabajo y el apoyo recibido de todos ellos.

CAPITULO I

EL PROBLEMA DE INMERSION SOBRE ESQUEMAS

Este capítulo se inicia con una revisión de la teoría de Galois sobre esquemas. Se estudian particularmente las nociones de recubrimiento principal y recubrimiento galoisiano de un esquema conexo. En el caso en que el esquema base sea X = Spec K, con K cuerpo, tales conceptos se corresponden con las nociones clásicas de álgebra galoisiana (en el sentido de Hasse) y de extensión galoisiana de K, respectivamente.

A continuación, formulamos el problema de inmersión de la Teoría de Galois en el contexto de la teoría de esquemas. El lenguaje introducido permite dar un tratamiento unificado del problema de inmersión usual sobre cuerpos y del problema de inmersión con condiciones de ramificación prefijadas.

Como resultado final del capítulo, veremos bajo que condiciones de la resolubilidad de un problema de inmersión puede deducirse la existencia de una solución con conjunto de ramificación prefijado.

Para las definiciones y notaciones de teoría general de esquemas que usaremos ver [G-D].

§1. TEORIA DE GALOIS SOBRE ESQUEMAS

El concepto básico de la teoría de Galois sobre esquemas es el de recubrimiento principal. Para introducirlo, se necesitan varias definiciones previas.

Un morfismo de esquemas $f: Y \longrightarrow X$ de tipo finito se dice que es *no ramificado en* $y \in Y$ si $\mathcal{O}_y/\mathfrak{m}_x\mathcal{O}_y$ es extensión finita y separable de $\kappa(x)$, para $x = f(y)$. Se dice que es *no ramificado* si es no ramificado en todo punto y de Y.

Proposición 1.1. ([M] I 3.2). Sea K un cuerpo, B una K-álgebra finita. Entonces el morfismo Spec B $\longrightarrow$ Spec K es no ramificado si y sólo si B es K-álgebra separable (es decir suma directa de cuerpos, extensiones separables de K). #

Un morfismo $Y \longrightarrow X$ se llama *étale* si es plano y no ramificado; se llama *recubrimiento étale* si es étale y finito.

Sea Y un esquema, G un grupo finito operando sobre Y por automorfismos, por la derecha. Para todo esquema Z, G opera por la izquierda sobre el conjunto $\mathrm{Hom}(Y,Z)$. El conjunto $\mathrm{Hom}(Y,Z)^G$ de morfismos invariantes por G depende funtorialmente de Z. Para un esquema X y un morfismo $p: Y \longrightarrow X$ invariante por G, se dice que (X,p) es *esquema cociente* de Y por G si, para todo Z, la aplicación:

$$\begin{array}{ccc} \mathrm{Hom}(X,Z) & \longrightarrow & \mathrm{Hom}(Y,Z)^G \\ g & \longmapsto & gp \end{array}$$

es biyectiva. Entonces los funtores $Z \longmapsto \mathrm{Hom}(X,Z)$ y $Z \longmapsto \mathrm{Hom}(Y,Z)^G$ son isomorfos y se dice que el segundo es representable.

El esquema cociente de Y por F está determinado salvo isomorfirmo y se indica por Y/G.

Proposición 1.2. ([G] V 1.3-1.4). Sea Y un esquema con grupo de automorfismos finito G, $p: Y \longrightarrow X$ un morfismo afín invariante por G tal que $\mathcal{O}_X \simeq p_*(\mathcal{O}_Y)^G$. Entonces X es esquema cociente de Y por G. Además, para cada abierto U de X, U es cociente de $p^{-1}(U)$ por G.

En particular, si B es anillo y G opera sobre B por la izquierda, $\mathrm{Spec}(B^G)$ es esquema cociente de Spec B por G. #

Proposición 1.3. ([G] V 1.9). Sea Y un esquema con grupo de automorfismos finito G tal que existe X = Y/G y es esquema sobre Z. Consideramos el cambio de base:

$Z' \longrightarrow Z$. Sean:

$$X' = X \underset{Z}{\times} Z' \quad , \quad Y' = Y \underset{Z}{\times} Z' \ .$$

Se tiene que G opera sobre Y' y $p' : Y' \longrightarrow X'$ es invariante.

Si Z' es plano sobre Z, entonces existe Y'/G y se cumple

$$(Y \underset{Z}{\times} Z')/G \simeq (Y / G) \underset{Z}{\times} Z' . \ \#$$

Si G es un grupo finito operando por la derecha sobre el esquema Y, se llama *grupo de descomposición* de $y \in Y$ al estabilizador G_y de y. Este grupo opera canónicamente (por la izquierda)

sobre el cuerpo residuo $\kappa(y)$. Se llama *grupo de inercia* de y al subgrupo I_y de G_y de los elementos que operan trivialmente.

Proposición 1.4. ([G] V 2.3). Sea X localmente noetheriano, $Y \longrightarrow X$ finito con las condiciones de la proposición 1.2. Entonces si I_y se reduce al neutro, Y es étale sobre X en y. #

De aquí en adelante, al escribir Y/G, supondremos hecha la hipótesis de que existe el esquema cociente de Y por G.

Proposición 1.5. ([G] V 2.4) Sea Y conexo, G fiel sobre Y. Para que $p: Y \longrightarrow X = Y/G$ sea étale es necesario y suficiente que los grupos de inercia de los puntos de Y se reduzcan al neutro. Si es así, G se identifica con el grupo de todos los X-automorfismos del X-esquema Y. #

Dados un esquema X y un conjunto E finito, se define el esquema XxE como suma directa de la familia $(X_i)_{i\in E}$ de esquemas idénticos a X. Si G es un grupo operando sobre E por la derecha, entonces G opera también por la derecha sobre XxE (operando sobre el segundo factor) y se verifica $(X \times E)/G = X \times (E/G)$.

Se llama X-*esquema con grupo* G *de operadores trivial* a un X-esquema isomorfo al esquema XxG, donde G opera sobre el segundo factor por traslaciones por la derecha.

Un *recubrimiento principal* con grupo G (finito) de un esquema localmente noetheriano X es un X-esquema, $Y \xrightarrow{p} X$, sobre el que opera G por automorfismos por la derecha, cumpliendo las condiciones equivalentes:

i) Y es finito, los grupos de inercia de los puntos de Y se reducen al neutro y X = Y/G.

ii) existe un cambio de base fielmente plano y casi compacto $X_1 \longrightarrow X$ tal que $Y_1 = Y \underset{X}{\times} X_1$ es un X_1-esquema con grupo de operadores trivial , i.e. isomorfo a $X_1 \times G$.

Llamaremos *recubrimiento galoisiano* de un esquema conexo a un recubrimiento principal conexo.

Proposición 1.6. Sea X un esquema conexo. Sea $Y \longrightarrow X$ un recubrimiento galoisiano con grupo G , H un subgrupo de G. Entonces:

1) Existe Y/H y $Y \longrightarrow Y/H$ es recubrimiento principal con grupo H.

2) Si $H \triangleleft G$, $Y/H \longrightarrow X$ es recubrimiento principal con grupo G/H.

Demostración 1) Por ser X = Y/G y H subgrupo de G, existe Y/H ([G] V 1.7). Por ser $Y \longrightarrow X$ étale y finito, $Y/H \longrightarrow X$ es étale y finito ([G] V 3.4). Ahora por ser $Y \longrightarrow X$ e $Y/H \longrightarrow X$ finitos, $Y \longrightarrow Y/H$ es finito.

Para ver que los grupos de inercia se reducen al neutro, basta observar que se tiene $H_y \subset G_y$ para los grupos de descomposición.

2) Supongamos $H \triangleleft G$. Por ser $Y \longrightarrow X$ recubrimiento principal con grupo G, existe un cambio de base plano $X' \longrightarrow X$ tal que:

$$Y' = Y \underset{X}{\times} X' \simeq X' \times G.$$

Entonces por la proposición 1.3, tenemos:

$$(Y/H) \underset{X}{\times} X' \simeq (Y \underset{X}{\times} X') / H.$$

Ahora,

$$(Y \underset{X}{\times} X') /H \simeq (X' \times G) /H \simeq X' \times (G/H),$$

por tanto, Y/H es recubrimiento principal de X con grupo G/H. #

Veamos ahora que todo recubrimiento principal no conexo de un esquema conexo es suma directa de recubrimientos galoisianos isomorfos.

Proposición 1.7. Sea X un esquema conexo, $Y \xrightarrow{p} X$ un recubrimiento principal con grupo G (finito). Entonces si Y_o es una componente conexa de Y, $Y_o \longrightarrow X$ es recubrimiento galoisiano con grupo $G_o = \{g \in G \,/\, Y_o{}^g = Y_o\}$ y se tiene un isomorfismo de X-esquemas:

$$Y \simeq Y_o \times (G/G_o),$$

donde G/G_o es el conjunto de clases laterales por la derecha.

Demostración. Sea Y_o una componente conexa de Y, sea $G_o = \{g \in G \,/\, Y_o{}^g = Y_o\}$. Sea $s \in G - G_o$, entonces $Y_o{}^s$ es una componente conexa de Y, y tenemos:

$$G_{Y_o^s} := \{g \in G / \ (Y_o^s)^g = Y_o^s\} = s^{-1} G_o s.$$

Veamos que todas las componentes conexas de Y son de la forma Y_o^s, para algún s de G. Sea C una componente conexa de Y. Si C no es del tipo Y_o^s, ninguno de sus puntos es igual a y_o^s, con y_o de Y_o, ya que si fuera así, tendríamos $C^{s^{-1}} \cap Y_o = \{y_o\} \neq \emptyset$ y por tanto $C^{s^{-1}} = Y_o$. Sea y un punto de C , x = p(y). Por ser $Y \longrightarrow X$ finito, existe un entorno afín U = Spec A de x, tal que $V = p^{-1}(U)$ = Spec B, con B A-álgebra finita (es decir finito-generada como A-módulo). Entonces U = V/G, es decir $A = B^G$. Las componentes conexas de V son la intersección de V con las componentes conexas de Y. Por otra parte, son de la forma Spec B_i, con B_i álgebra sin idempotentes, para $B = \oplus B_i$ una descomposición de B. Sea V_o = Spec B_o = C ∩ V. Si $\sqcup V_o^s \neq V$, entonces $\oplus B_o^s \neq B$. Sea e el idempotente primitivo de B tal que $Be = B_o$, entonces el elemento $\sum_{s \in G} e^s$ es invariante por G y no está en A. Se llega pues a contradicción.

Definimos el morfismo:

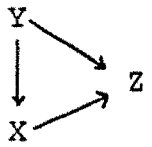
$$Y_o \times (G / G_o) \longrightarrow Y$$
$$(y, G_o s) \longmapsto y^s$$

Es isomorfismo de X-esquemas y G-morfismo.

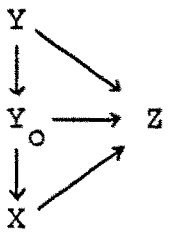
Veamos que $Y_o \longrightarrow X$ es recubrimiento principal con grupo G_o. El morfismo $Y_o \longrightarrow X$ es finito por serlo $Y \longrightarrow X$. Comprobemos que X es esquema cociente de Y_o por G_o. Sea $Y_o \longrightarrow Z$ un morfismo de esquemas invariante por G_o. Entonces la composición

$$Y \simeq Y_o \times (G/G_o) \longrightarrow Y_o \longrightarrow Z,$$

donde el primer morfismo es la proyección sobre el primer factor, es invariante por G. Por tanto, por ser $Y/G = X$, existe un morfismo $X \longrightarrow Z$ tal que



conmuta. Entonces, en el diagrama:



el triángulo inferior conmuta. Finalmente $Y_o \longrightarrow X$ es étale por serlo $Y \simeq Y_o \times (G/G_o) \longrightarrow X$. Por ser Y_o conexo, los grupos de inercia de los puntos de Y_o se reducen pues al neutro (prop. 1.5). #

Proposición 1.8. Sean G un grupo finito, G_o un subgrupo de G, X un esquema conexo, localmente noetheriano, $Y \longrightarrow X$ un recubrimiento principal con grupo G_o.

Entonces, $Y \times (G/G_o) \longrightarrow X$ es recubrimiento principal con grupo G, donde G/G_o es el conjunto de clases laterales por la derecha.

Demostración. Definimos la acción de G sobre $Y \times (G/G_o)$ en la forma siguiente:

$$(y, G_o s)^t = (y^t, G_o st),$$

para $(y, G_o s) \in Y \times (G/G_o)$, $t \in G$.

Por ser $Y \longrightarrow X$ recubrimiento principal con grupo G_o, existe un cambio de base $X' \longrightarrow X$, fielmente plano y casi-compacto, tal que $Y \underset{X}{\times} X' \simeq X' \times G_o$. Por tanto tenemos

$$(Y \times (G/G_o)) \underset{X}{\times} X' = (Y \underset{X}{\times} X') \times (G/G_o) \simeq X' \times G_o \times (G/G_o) \simeq X' \times G,$$

es decir, $Y \times (G/G_o) \longrightarrow X$ es recubrimiento principal con grupo G. #

Enunciando conjuntamente las proposiciones 1.7 y 1.8, se obtiene que, dados un esquema X y un grupo G finito, hay una correspondencia 1-1 entre recubrimientos principales de X con grupo G y recubrimientos galoisianos de X con grupo un subgrupo de G.

Si X=Spec K, con K cuerpo, un recubrimiento galoisiano Y de X con grupo G es de la forma Y = Spec L, con L cuerpo extensión de Galois de K con grupo G. En efecto, por ser $Y \longrightarrow X$ finito y X afín, Y es afín y basta aplicar la proposición 1.1 para obtener que L es extensión separable de K. Además, por ser X conexo, L es cuerpo. Por la proposición 1.2 se tiene $K = L^G$.

De la proposición 1.7 puede entonces deducirse que un recubrimiento principal Y de X=Spec K con grupo G es de la forma Y=Spec B, con B K-álgebra, suma directa de cuerpos isomorfos a una extensión de Galois L|K con grupo G_o, grupo de descomposi

ción de un primo de B, y conjugados por un elemento de G. De 1.8 deducimos que, dada una extensión de Galois L|K con grupo G_o, subgrupo de G, podemos construir un álgebra B tal que Spec B es recubrimiento principal de Spec K con grupo G.

En este caso, se recupera un resultado de Hasse ([H]§1). Hasse define un álgebra galoisiana sobre un cuerpo K, con grupo G como una K-álgebra B, finita, separable y tal que G opera sobre B por K-automorfismos de manera que B es isomorfa como G-módulo a K[G]. Aplicando de nuevo la proposición 1.1 y que un morfismo finito es afín, se obtiene que las K-álgebras finitas y separables se corresponden unívocamente con los recubrimientos étales de Spec K. Ahora, si B es K-álgebra finita separable e Y = Spec B, los puntos y de Y están en correspondencia uno a uno con las componentes L de la descomposición de B en suma directa de cuerpos. El grupo de descomposición de y es el subgrupo G_o de G formado por los elementos que dejan fijo L. La condición de que B sea isomorfa a K[G] como G-módulo equivale entonces a que los grupos de inercia de los puntos de Y se reduzcan al neutro y a que sea $K = B^G$, es decir Spec K = Y/G. Por tanto, la noción de K-álgebra galoisiana se corresponde con la de recubrimiento principal de Spec K.

Hasse demuestra que cada álgebra galoisiana B, sobre un cuerpo K, con grupo G, contiene un cuerpo L, extensión de Galois de K con grupo un subgrupo G_o de G y que B es suma directa de cuerpos isomorfos a L y conjugados por un elemento de G. L se llama cuerpo núcleo del álgebra galoisiana B y está determinado salvo conjugación. Asimismo, Hasse demuestra que, dados

un cuerpo K y una extensión de Galois L de K con grupo de Galois G_o, subgrupo de un grupo G, puede dotarse a LxG/G_o de estructura de K-álgebra galoisiana con grupo G.

Introducimos a continuación la noción de recubrimiento universal de un esquema conexo.

Sean X un esquema localmente noetheriano y conexo, x un punto geométrico de X. Sea C la categoría de los recubrimientos étales Y de X. Para un objeto Y de C, definimos:

F(Y) = conjunto de puntos geométricos de Y sobre x.

F es un funtor de C en la categoría de conjuntos finitos.
F es pro-representable, es decir existe un sistema proyectivo ordenado filtrante $(P_i)_{i\in I}$ de objetos de C de manera que se cumpla:

$$F(Y) = \varinjlim_i \operatorname{Hom}_C(P_i, Y),$$

isomorfismo de funtores dado por $(f_i) \longmapsto (f_i \circ p_i)$, para $f_i \in \operatorname{Hom}_C(P_i, Y)$, y donde (p_i) es un elemento fijado de $\varprojlim_i F(P_i)$. Se llama *recubrimiento universal de* X *en el punto* x al sistema proyectivo $P=(P_i)_{i\in I}$. Es un pro-objeto de la categoría C.

Los recubrimientos galoisianos forman un sistema cofinal en el sistema de los P_i, y se verifica:

Aut $P = \varprojlim_i$ Aut P_i, tomando límite sobre los P_i galoisianos. Aut P es pues un grupo pro-finito. Se define el *grupo fundamental de* X *en el punto* x como el grupo opuesto de Aut P. Opera pues sobre P por la derecha. Se indica por $\pi_1(X,x)$.

Partiendo de puntos geométricos distintos, se obtienen recubrimientos universales isomorfos (como pro-recubrimientos étales de X) y grupos fundamentales isomorfos. Definimos $\tilde{X}$, recubrimiento universal de X, como pro-recubrimiento étale de X isomorfo a los P y G_X, *grupo de Galois absoluto de* X como isomorfo a los $\pi_1(X,x)$.

Hay una equivalencia de categorías de C en la categoría de conjuntos finitos sobre los que G_X opera en forma continua dada por

$$Y \longmapsto \text{Hom } (P,Y) = \varinjlim_i \text{Hom } (P_i,Y).$$

En el caso de los recubrimientos principales, se obtiene que dar un recubrimiento principal Y de X con grupo G y un punto y de F(Y) equivale a dar un morfismo

$$\varphi: \pi_1(X,x) \longrightarrow G .$$

$\pi_1(X,x)$ opera sobre G a través de φ por traslaciones por la izquierda y, haciendo corresponder el punto y fijado al neutro de G, se tiene

$$\text{Hom } (P,Y) = F(Y) = G.$$

El recubrimiento principal Y es conexo si y sólo si φ es epimorfismo y entonces se tiene:

$$\text{Aut}_X\ Y = \text{Hom } (P,Y) = F(Y) = G .$$

Si Y es un recubrimiento principal de X con grupo G, no conexo, e Y_o es la componente conexa del punto y fijado, Y_o es recubrimiento galoisiano de X con grupo G_o, subgrupo de G (cf. 1.7). Entonces la imagen del morfismo:

$$\varphi: \pi_1(X,x) \longrightarrow G ,$$

correspondiente al par (Y,y), es G_o ; haciendo corresponder el punto y al neutro de G_o, tenemos:

$$G_o = F(Y_o) = \mathrm{Aut}_X Y_o .$$

Veamos ahora cual es el grupo fundamental del espectro de un cuerpo y de un esquema normal.

Proposición 1.9. ([G] V 8.1). Sea $X = \mathrm{Spec}\ K$, con K cuerpo y sea Ω una extensión algebraicamente cerrada de K, sea x el punto geométrico de X que define. Sea $\bar{K}$ la clausura separable de K en Ω. Entonces existe un isomorfismo canónico de $\pi_1(X,x)$ en el grupo de Galois de $\bar{K}$ sobre K. #

Más generalmente, tenemos:

Proposición 1.10. ([G] V 8.2). Sea X un esquema conexo, localmente noetheriano y normal, sea $K = K(X)$ su cuerpo de funciones, sea Ω una extensión algebraicamente cerrada de K(X) que define un punto geométrico x' de $X' = \mathrm{Spec}\ K(X)$, y un punto geométrico x de X. Entonces el morfismo:

$$\pi_1(X',x') \longrightarrow \pi_1(X,x)$$

es exhaustivo. Identificando $\pi_1(X',x')$ con $\mathrm{Gal}(\bar{K}|K)$, grupo de Galois de la clausura separable $\bar{K}$ de K en Ω, el núcleo del morfismo anterior se corresponde por la teoría de Galois con la subextensión de $\bar{K}|K$, compuesta de las extensiones finitas de K en Ω, no ramificadas sobre X. #

Como consecuencia de esta proposición, y teniendo en cuenta que los $Y \dashrightarrow X$ galoisianos se corresponden unívocamente con los cocientes finitos de $\pi_1(X,x)$, se obtiene que, para un esquema conexo, localmente noetheriano y normal, con cuerpo de funciones K, las extensiones de Galois de K no ramificadas sobre X se corresponde con los recubrimientos galoisianos de X.

Más concretamente, si X es un esquema conexo, localmente noetheriano y normal, $Y \xrightarrow{p} X$ un recubrimiento galoisiano de X, con Y normal, K(X) y K(Y) los cuerpos de funciones de X e Y respectivamente, $K(Y)|K(X)$ es extensión de Galois con grupo G. En efecto, por ser $Y \longrightarrow X$ no ramificado en el punto genérico de Y, se tiene $K(Y)|K(X)$ extensión finita y separable. Además para cada abierto afín U=Spec A de X se tiene $p^{-1}(U) =$ =Spec B con B tal que $B^G = A$ (prop. 1.2), y por ser K(Y) y K(X) cuerpos de fracciones de B y A respectivamente se tiene $K(Y)^G = K(X)$.

Veamos ahora la construcción inversa para un caso particular de esquema normal que utilizaremos más adelante. Sea Θ un anillo de Dedekind, K su cuerpo de fracciones, S un conjunto finito de primos de $\Theta = \Theta_K$, $L|K$ una extensión de Galois con grupo G, no ramificada fuera de S. Entonces, X=Spec Θ_K-S es abierto de Spec Θ_K y por tanto tiene estructura de esquema. Sea S' el conjunto de primos de Θ_L, anillo de enteros de L que contraen a primos de S. Entonces Y = Spec Θ_L-S' tiene estructura de esquema, como abierto de Spec Θ_L. Tenemos que $Y \longrightarrow X$ es recubrimiento de Galois con grupo G. En efecto, se cumple

$\Theta_L^G = \Theta_L \cap K = \Theta_K$, por tanto, por ser X abierto de Spec Θ_K e Y la antiimagen de X en Spec Θ_L se tiene X = Y/G (prop 1.2). Además, por ser L|K no ramificada sobre X los grupos de inercia de los puntos de Y se reducen al neutro.

Proposición 1.11. Sea X un esquema localmente noetheriano, conexo, $Y \xrightarrow{p} X$ un recubrimiento galoisiano con grupo G. Sea x un punto geométrico de X, sea y el punto de Y sobre x determinado por el neutro de G. Entonces se tiene una sucesión exacta:

$$1 \longrightarrow \pi_1(Y,y) \longrightarrow \pi_1(X,x) \longrightarrow G \longrightarrow 1.$$

Demostración. Al recubrimiento galoisiano $Y \xrightarrow{p} X$, le corresponde un epimorfismo: $\pi_1(X,x) \longrightarrow G$, y se tiene $G \simeq \mathrm{Hom}(P,Y) = F(Y)$. El neutro de G determina un punto geométrico y sobre x. El núcleo está formado por los elementos de $\pi_1(X,x)$ que son Y-morfismos y dejan fijo y. Por ([G] V 6.13) se tiene un monomorfismo $\pi_1(Y,y) \longrightarrow \pi_1(X,x)$, cuya imagen es el abierto de $\pi_1(X,x)$ formado por los elementos sobre Y que dejan fijo y. #

§2. PLANTEAMIENTO DEL PROBLEMA DE INMERSION

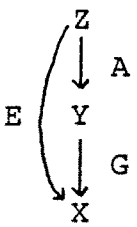
Procederemos ahora a dar el enunciado del problema de inmersión en el contexto general de la teoría de esquemas. Sea X un esquema conexo, localmente noetheriano. *Un problema de inmersión* sobre X viene dado por los siguientes datos:

1) un recubrimiento galoisiano $Y \longrightarrow X$ con grupo G finito.

2) una sucesión exacta de grupos finitos:

$$(E):\ 1 \longrightarrow A \xrightarrow{i} E \xrightarrow{j} G \longrightarrow 1\ .$$

Llamaremos *solución al problema de inmersión* a un esquema Z, cumpliendo las condiciones:



1) $Z \xrightarrow{p_X} X$ es recubrimiento principal con grupo E.

2) $Z \xrightarrow{p_Y} Y$ es recubrimiento principal con grupo A.

3) El morfismo $F(p_Y): F(Z)=\mathrm{Hom}(\tilde{X},Z) \longrightarrow F(Y)=\mathrm{Hom}(\tilde{X},Y)$ dado por p_Y, hace conmutativo el diagrama:

$$\begin{array}{ccc} E & \xrightarrow{\quad j \quad} & G \\ \wr\downarrow & & \wr\downarrow \\ F(Z) & \xrightarrow{F(p_Y)} & F(Y)\ . \end{array}$$

Damos ahora un enunciado alternativo del problema de inmersión en términos de morfismos de grupos.

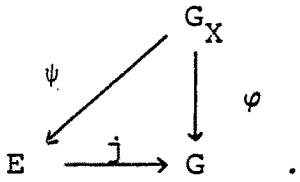
Sea X un esquema conexo, localmente noetheriano, G_X su grupo de Galois absoluto. Plantear un *problema de inmersión* sobre X es dar un epimorfismo φ de G_X en un grupo finito G y una sucesión exacta de grupos finitos.

$$1 \longrightarrow A \xrightarrow{i} E \xrightarrow{j} G \longrightarrow 1\ ,$$

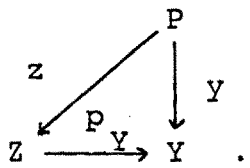
es decir un diagrama del tipo:

$$\begin{array}{ccccccccc} & & & & & & G_X & & \\ & & & & & & \downarrow\varphi & & \\ 1 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{j} & G & \longrightarrow & 1\ . \end{array}$$

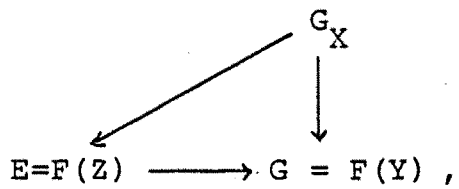
Llamaremos *solución al problema de inmersión* a un morfismo $\psi: G_X \longrightarrow E$, que haga conmutativo el diagrama



Veamos que los dos enunciados son efectivamente equivalentes. Sea Z una solución al problema de inmersión en su primera forma. Sea $z \in F(Z) = \mathrm{Hom}(P,Z)$ el elemento correspondiente al neutro de E, sea $y \in F(Y) = \mathrm{Hom}(P,Y)$ el elemento correspondiente al neutro de G. Entonces por la condición 3), tenemos que el morfismo de F(Z) en F(Y), inducido por $p_Y: Z \longrightarrow Y$, envia z a y, es decir que es conmutativo el diagrama:

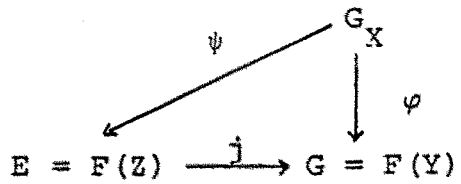


Aplicando el funtor F, obtenemos el diagrama conmutativo:



por tanto F(z) es solución al problema de inmersión en su segunda forma.

Recíprocamente, sea $\psi: G_X \dashrightarrow E$ un morfismo solución al problema de inmersión en su segunda forma. Dar ψ equivale a dar un recubrimiento principal $Z \longrightarrow X$, con grupo $E = F(Z)$. Tenemos el diagrama conmutativo:



y la flecha horizontal da un morfismo $Z \longrightarrow Y$, por la equivalencia de categorías. Sea x un punto geométrico de X, sean y el punto geométrico de Y sobre x correspondiente al neutro de G, z el punto geométrico de Z sobre x correspondiente al neutro de E. Entonces el núcleo del morfismo $F(Z) \longrightarrow F(Y)$ está formado por los puntos geométricos z de Z sobre y. Por ser G_Y el núcleo de φ: $G_X \longrightarrow G$, tenemos un morfismo:

$$G_Y \longrightarrow \{\text{puntos geométricos de Z sobre y}\} = A,$$

por tanto $Z \longrightarrow Y$ es recubrimiento galoisiano con grupo A. El esquema Z es pues solución al problema de inmersión en su primera forma.

Además, los esquemas conexos solución se corresponden con los epimorfismos solución.

Llamaremos *solución propia* del problema de inmersión a una solución que sea un esquema Z conexo o, equivalentemente, un morfismo ψ exhaustivo. Llamaremos *solución impropia* a una solución que no sea propia.

Caso particular: Problema de inmersión sobre un cuerpo

En el caso en que el esquema X es el espectro de un cuerpo K, hemos visto (cf. §1) que un recubrimiento galoisiano de X con grupo G es de la forma Spec L, con L cuerpo extensión de Galois de K con grupo G y que un recubrimiento principal de X

con grupo G es de la forma Spec B, con B-álgebra galoisiana sobre K con grupo G.

Entonces, plantear un problema de inmersión con los datos: $Y = \text{Spec } L \longrightarrow X = \text{Spec } K$; G ; (E) : $1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$ equivale a plantear el problema de inmersión clásico de la teoría de Galois con los datos:

$$L|K \ ; \quad G \ , \ (E) \ .$$

Una solución propia es un cuerpo M, extensión de Galois de L con grupo A que sea asimismo extensión de Galois de K con grupo E y tal que el morfismo $\text{Gal}(M|K) \longrightarrow \text{Gal}(L|K)$, que, a un automorfismo de M sobre K, asocia su restricción a L, haga conmutativo el diagrama:

$$\begin{array}{ccc} E & \longrightarrow & G \\ \downarrow\wr & & \downarrow\wr \\ \text{Gal}(M|K) & \longrightarrow & \text{Gal}(L|K) \end{array} \ .$$

Obsérvese que, si $\bar{K}$ es una clausura separable de K, se tiene $\text{Gal}(M|K) = \text{Hom}_K(M,\bar{K})$ y $\text{Gal}(L|K) = \text{Hom}_K(L,\bar{K})$.

Una solución impropia al problema de inmersión planteado es una L-álgebra galoisiana B con grupo A, que sea asimismo K-álgebra galoisiana con grupo E y tal que el morfismo : $\text{Hom}_K(B,\bar{K}) \longrightarrow \text{Hom}_K(L,\bar{K})$: que, a un morfismo de B en una clausula separable $\bar{K}$ de K, le asocia su composición con la inclusión $L \longrightarrow B$, haga conmutativo el diagrama

$$\begin{array}{ccc} E & \longrightarrow & G \\ \downarrow\wr & & \downarrow\wr \\ \text{Hom}_K(B,\bar{K}) & \longrightarrow & \text{Hom}_K(L,\bar{K}) \end{array} \ .$$

Obsérvese que, si planteamos el problema de inmersión en

su segunda forma y $\psi: G_K \longrightarrow E$ es un morfismo solución, la extensión de K correspondiente a Ker ψ es el cuerpo solución, si ψ es exhaustivo y el cuerpo núcleo del álgebra solución, si ψ no es exhaustivo.

Más en general, sean Θ_K y Θ_L anillos de Dedekind de cuerpos de fracciones K y L respectivamente y tales que L|K es extensión de Galois con grupo G finito, no ramificada fuera del conjunto S de primos de Θ_K. Sea S' el conjunto de primos de Θ_L que contraen a primos de S.

Entonces

$$Y = \text{Spec } \Theta_L - S' \longrightarrow X = \text{Spec } \Theta_K - S$$

es recubrimiento galoisiano con grupo G, como habíamos visto a continuación de 1.10.

Plantear un problema de inmersión con los datos:

$$Y \longrightarrow X \ ; \ G \ ; \ (E): \ 1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

equivale entonces a plantear el problema de inmersión con los datos:

$$L|K \ ; \ G \ ; \ (E)$$

y la condición adicional de que las soluciones sean no ramificadas fuera de S. Más concretamente, a una solución propia M, le exigimos que la extensión M|K sea no ramificada fuera de S, a una solución impropia B le exigimos que su cuerpo núcleo (o, equivalentemente, cada uno de los sumandos isomorfos de su descomposición en suma directa de cuerpos) sea extensión de K, no ramificada fuera de S. La solución propia M o, en su

caso, el cuerpo núcleo de la solución impropia B, será la subextensión de K^S, máxima extensión separable de K, no ramificada fuera de S, correspondiente al núcleo del morfismo $\psi: G_K^S \longrightarrow E$, solución al problema de inmersión en su segunda forma.

§3. TRADUCCION COHOMOLOGICA DEL PROBLEMA DE INMERSION

Cohomología étale

La *topología étale* de un esquema X es la categoría $X_{ét}$ de los morfismos étales $U \longrightarrow X$. Se consideran estos morfismos como abiertos de X. Dados $U \longrightarrow X$, $V \longrightarrow X$ étales, $U \times_X V \longrightarrow X$ juega el papel de la intersección.

Un recubrimiento étale de un X-esquema $U \longrightarrow X$ es una familia $\{U_i \xrightarrow{\phi_i} U\}$ de morfismos étales de X-esquemas, exhaustiva, es decir, tal que $U = \bigsqcup \phi_i(U_i)$.

Un *prehaz abeliano étale* sobre X o un prehaz abeliano sobre $X_{ét}$ es un funtor contravariante:

$$F : X_{ét} \longrightarrow (ab)$$

de la categoría $X_{ét}$ en la categoría de grupos abelianos. El funtor F asocia a cada $U \longrightarrow X$ étale un grupo abeliano F(U), el grupo de secciones de F sobre U; para cada morfismo en $X_{ét}$: $V \longrightarrow U$ se tiene un morfismo $res_{V,U} : F(U) \longrightarrow F(V)$.

Un morfismo $f: F \longrightarrow G$ de prehaces étales abelianos sobre X se define como un morfismo de funtores contravariantes.

Para cada $U \longrightarrow X$ étale se tiene un morfismo $f_U : F(U) \longrightarrow G(U)$ y para $V \longrightarrow U$ morfismo en $X_{ét}$, es conmutativo el diagrama

$$\begin{array}{ccc} F(U) & \xrightarrow{f_U} & G(U) \\ \Big\downarrow{\scriptstyle res_{V,U}} & & \Big\downarrow{\scriptstyle res_{V,U}} \\ F(V) & \xrightarrow{f_V} & G(V) \end{array} .$$

Un prehaz étale F es *haz étale* si, para cada $U \longrightarrow X$ étale y cada recubrimiento $\{U_i \longrightarrow U\}$, es exacto el diagrama:

$$F(U) \longrightarrow \prod_i F(U_i) \rightrightarrows \prod_{i,j} F(U_i \underset{U}{\times} U_j) .$$

Los dos morfismos de la derecha son los inducidos por las proyecciones $U_i \underset{U}{\times} U_j \longrightarrow U_i$ y $U_i \underset{U}{\times} U_j \longrightarrow U_j$. La exactitud significa que el morfismo de la izquierda es inyectivo y su imagen es el grupo de los elementos de $\prod_i F(U_i)$ sobre los que coinciden los dos morfismos de la derecha.

Dado un prehaz abeliano étale F sobre un esquema X, existe un único haz abeliano étale $F^{\#}$ dotado de un morfismo $F \longrightarrow F^{\#}$ tal que, para cada morfismo $F \longrightarrow G$ de F en un haz abeliano étale G, existe un único morfismo $F^{\#} \longrightarrow G$ tal que conmuta el diagrama

$$\begin{array}{ccc} F & \longrightarrow & F^{\#} \\ & \searrow \quad \swarrow & \\ & G & \end{array}$$

$F^{\#}$ se llama *haz asociado al prehaz* F.

A continuación, veremos ejemplos de haces étales represen

tados por esquemas en grupos. Un *esquema en grupos* (conmutativo) es un X-esquema G tal que $\mathrm{Hom}_X(U,G)$ es grupo (conmutativo) para cada $U \longrightarrow X$ étale y además, para cada $U \longrightarrow V$, morfismo de X-esquemas étales,

$$\mathrm{Hom}_X(V,G) \longrightarrow \mathrm{Hom}_X(U,G)$$

es morfismo de grupos.

Si $G \longrightarrow X$ es un esquema en grupos conmutativo, el funtor

$$F: X_{ét} \longrightarrow (ab)$$

$$U \longmapsto F(U) = \mathrm{Hom}_X(U,G)$$

es haz abeliano sobre $X_{ét}$. Es el *haz étale representado por el esquema en grupos* G.

Ejemplo 1 : Haz constante:

Sea A un grupo abeliano. El haz constante con valores en A es el haz A_X representado por el esquema en grupos XxA, con la estructura de grupo inducida por A . Si $U \longrightarrow X$ es étale, tenemos:

$$A_X(U) = \mathrm{Hom}_X(U,XxA) = \coprod_{U_i \in \pi_o(U)} \mathrm{Hom}_X(U_i,XxA) = \prod_{\pi_o(U)} A ,$$

donde $\pi_o(U)$ es el conjunto de componentes conexas de U.

Ejemplo 2 : Grupo multiplicativo:

El grupo multiplicativo $(G_m)_X$ es el haz representado por el esquema en grupos:

$$(G_m)_X = \mathrm{Spec}\ (\mathbb{Z}[t,t^{-1}]) \underset{\mathrm{Spec}\ \mathbb{Z}}{\times} X .$$

Para $U \longrightarrow X$ étale, tenemos:

$$\begin{aligned}(G_m)_X(U) &= \mathrm{Hom}_X\,(U, \mathrm{Spec}\,(\mathbb{Z}[t,t^{-1}]) \times X) \\ &= \mathrm{Hom}\,(U, \mathrm{Spec}\,(\mathbb{Z}[t,t^{-1}])) \\ &= \mathrm{Hom}\,(\mathbb{Z}[t,t^{-1}], \Gamma(U, \mathcal{O}_U)) \\ &= \Gamma(U,\mathcal{O}_U)^*.\end{aligned}$$

Ejemplo 3: Haz de las raíces de la unidad.

El haz $(\mu_n)_X$ de raíces n-ésimas de la unidad es el representado por el esquema en grupos

$$(\mu_n)_X = \mathrm{Spec}\,(\mathbb{Z}[t]/(t^n-1)) \underset{\mathrm{Spec}\,\mathbb{Z}}{\times} X\,.$$

Para $U \longrightarrow X$ étale, tenemos:

$$\begin{aligned}(\mu_n)_X(U) &= \mathrm{Hom}_X(U, \mathrm{Spec}\,(\mathbb{Z}[t]/(t^n-1)) \times X) \\ &= \mathrm{Hom}\,(U, \mathrm{Spec}\,(\mathbb{Z}[t]/(t^n-1))) \\ &= \mathrm{Hom}\,(\mathbb{Z}[t]/(t^n-1), \Gamma(U,\mathcal{O}_U)) \\ &= \{s \in \Gamma(U,\mathcal{O}_U) \;/\; s^n = 1\} \\ &= \mu_n\,(\Gamma\,(U,\mathcal{O}_U))\,.\end{aligned}$$

Para cada $n \in \mathbb{N}$ tenemos la sucesión exacta

$$0 \longrightarrow (\mu_n)_X \longrightarrow (G_m)_X \xrightarrow{\cdot\, n} (G_m)_X$$

donde el morfismo de la derecha viene dado por $s \longmapsto s^n$.

Además, se tiene:

Proposición 1.12 ([T] 4.4.1) Si n es invertible sobre X, es decir primo con car k(x) para cada $x \in X$, entonces se tiene la siguiente sucesión exacta de morfismos de haces abelianos sobre $X_{ét}$:

$$0 \longrightarrow (\mu_n)_X \longrightarrow (G_m)_X \longrightarrow (G_m)_X \longrightarrow 0 \ .$$

Esta sucesión se llama *sucesión de Kummer* sobre X. #

Si f: Y $\longrightarrow$ X es morfismo de esquemas, induce un morfismo de topologías étales:

$$f^{-1}: X_{ét} \longrightarrow Y_{ét} \quad , \quad U \longmapsto U \underset{X}{\times} Y \ .$$

Si F es haz étale abeliano sobre Y, el funtor:

$$f_*F: X_{ét} \longrightarrow (ab) \quad , \ U \longmapsto F(f^{-1}U) = F(U \underset{X}{\times} Y)$$

es un haz étale abeliano sobre X. El haz f_*F se llama *haz imagen directa* de F por f: Y $\longrightarrow$ X. Se tiene que f_* es un funtor de la categoría H_Y de haces abelianos sobre $Y_{ét}$ en la categoría H_X de haces abelianos sobre $X_{ét}$. Tiene un funtor adjunto por la izquierda:

$$f^*: \ H_X \longrightarrow H_Y \ ,$$

que por tanto verifica:

$$\mathrm{Hom}_{H_Y}(f^*F, G) \simeq \mathrm{Hom}_{H_X}(F, f_*G) \ ,$$

isomorfismo funtorial en $F \in H_X$ y en $G \in H_Y$.

Si f: Y $\longrightarrow$ X es étale (o pro-étale), y F un haz abeliano sobre $X_{ét}$, el funtor f*F, *imagen inversa* de F por f viene definido simplemente por

$$f^*F(V) = F(V) \quad \text{para} \quad V \longrightarrow Y \quad \text{étale.}$$

Haces étales inducidos por un módulo.

Sea $\pi\colon Y \longrightarrow X$ un X-esquema y $G = \mathrm{Aut}_X Y$ su grupo de automorfismos. Para cada G-módulo A continuo (es decir, tal que G opera sobre A a través de un cociente finito) podemos definir en forma canónica un haz abeliano $A_{Y|X}$ sobre $X_{ét}$ en la forma siguiente. Sea A_Y el haz constante sobre $Y_{ét}$ a valores en A y $\pi_* A_Y$ su imagen directa en $X_{ét}$. Si $U \longrightarrow X$ es étale, entonces el grupo:

$$(\pi_* A_Y)(U) = A_Y(Y \underset{X}{\times} U) = \mathrm{Hom}\,(\pi_o (Y \underset{X}{\times} U), A)$$

puede dotarse de estructura de G-módulo, a partir de la acción de G sobre $\pi_o(Y \underset{X}{\times} U)$ y sobre A, definiendo:

$$h^s = s\, h\, s^{-1}, \text{ para } h\colon \pi_o(Y \underset{X}{\times} U) \longrightarrow A,\ s \in G.$$

El haz $A_{Y|X} : X_{ét} \longrightarrow (ab)$ asociado al prehaz

$$U \longmapsto (\pi_* A_Y)(U)^G$$

se llama *haz inducido sobre* $X_{ét}$ *por el* G-*módulo* A.

Proposición 1.13. ([N_1]2.4.3). Si $\pi\colon Y \longrightarrow X$ es recubrimiento galoisiano con grupo G, entonces las transformaciones

$$A \longmapsto A_{Y|X} \qquad \text{y} \qquad F \longmapsto F(Y)$$

son equivalencias casi inversas una de otra entre la categoría de G-módulos continuos A y la categoría de haces abelianos F sobre $X_{ét}$, constantes sobre Y, es decir, los funtores compuestos

$$A \longmapsto F(A_{Y|X}) \qquad \text{y} \qquad F \longmapsto F(Y)_{Y|X}$$

son isomorfos al funtor identidad de la categoría de G-módulos continuos, y de haces abelianos sobre $X_{ét}$, respectivamente. #

Un haz abeliano F sobre $X_{ét}$ se llama *no ramificado* cuando es constante sobre el recubrimiento universal $\tilde{X}$ de X. Por la proposición anterior, los haces abelianos no ramificados sobre $X_{ét}$ se corresponden unívocamente con los G_X-módulos continuos.

Cohomología étale de haces abelianos.

La categoría H_X de haces abelianos sobre $X_{ét}$ es categoría abeliana con suficientes inyectivos. Por tanto, existen para cada funtor aditivo exacto por la izquierda

$$F: \ H_X \longrightarrow (ab)$$

los funtores derivados por la derecha $R^q F$. Para $U \longrightarrow X$ étale fijo, consideramos el funtor:

$$\Gamma_U : H_X \longrightarrow (ab) \quad \text{definido por: } \Gamma_U(F) = F(U).$$

Γ_U es aditivo y exacto por la izquierda. Si F es haz abeliano sobre $X_{ét}$, definimos:

$$H^q(U,F) = R^q \Gamma_U(F),$$

llamado *q-ésimo grupo de cohomología* de U con valores en F. Se indica también por $H^q_{ét}(U,F)$.

Veamos ahora como se relaciona la cohomología étale con la cohomología galoisiana.

Proposición 1.14 ([T] II 2-2). Sea K un cuerpo, $\bar{K}$ una clausura algebraica separable de K y G_K el grupo de Galois de $\bar{K}|K$, grupo pro-finito.

i) Hay una equivalencia de categorías entre la categoría de haces abelianos sobre $(\text{Spec } K)_{ét}$ y la categoría de G_K-módulos continuos dada por:

$$F \longmapsto \varinjlim F(\text{Spec } K') = F(\bar{K})$$

donde K' recorre todas las subextensiones de $\bar{K}$, finitas sobre K.

ii) Para cada haz abeliano F sobre $(\text{Spec } K)_{ét}$ se tienen isomorfismos ∂-funtoriales:

$$H^q_{ét}(\text{Spec } K, F) \simeq H^q(G_K, F(\bar{K})),$$

donde el grupo de la derecha es de cohomología galoisiana. #

Más en general, a partir de la proposición 1.13, se tiene:

Proposición 1.15. Sea X un esquema conexo, $\tilde{X}$ su recubrimiento universal, G_X su grupo de Galois absoluto. Para cada haz abeliano F sobre $X_{ét}$, no ramificado, se tienen isomorfismos:

$$H^q_{ét}(X,F) \simeq H^q(G_X, F(\tilde{X}))$$

donde $F(\tilde{X}) = \varinjlim F(Y)$, con Y recorriendo los recubrimientos étales de X.

Demostración. La correspondencia entre haces abelianos no ramificados sobre X y G_X-módulos continuos viene dada por:

$F \longmapsto F(\tilde{X})$ para F haz no ramificado sobre $X_{ét}$

$A \longmapsto A_{\tilde{X}|X}$ con $A_{\tilde{X}|X}$ definido por $A_{\tilde{X}|X}(U) = A^{G_U}$,

si $U \longrightarrow X$ étale, $G_U = \mathrm{Aut}_U \tilde{X}$.

Los grupos de cohomología están definidos por:

$H^q(X,F) = R^q \Gamma_X(F)$, para F haz abeliano sobre $X_{ét}$

$H^q(G_X,A) = R^q(A^{G_X})$, para A G_X-módulo continuo.

Dada una sucesión exacta de haces abelianos no ramificados sobre X:

$$(S_1): 0 \longrightarrow F' \longrightarrow F \longrightarrow F'' \longrightarrow 0,$$

es exacta la sucesión:

$$(S_2): 0 \longrightarrow F'(\tilde{X}) \longrightarrow F(\tilde{X}) \longrightarrow F''(\tilde{X}) \longrightarrow 0.$$

Para (S_1) la sucesión de funtores derivados de Γ_X es:

$$0 \longrightarrow F'(X) \longrightarrow F(X) \longrightarrow F''(X) \xrightarrow{\partial_1} H^1(X;F') \longrightarrow H^1(X,F) \longrightarrow \ldots$$

$$\ldots \longrightarrow H^q(X,F') \longrightarrow H^q(X,F) \longrightarrow H^q(X,F'') \longrightarrow H^{q+1}(X,F') \longrightarrow \ldots$$

y para (S_2) la sucesión de funtores derivados de $(.)^{G_X}$ es:

$$0 \longrightarrow F'(\tilde{X})^{G_X} \longrightarrow F(\tilde{X})^{G_X} \longrightarrow F''(\tilde{X})^{G_X} \xrightarrow{\partial_1} H^1(G_X,F'(\tilde{X})) \longrightarrow \ldots$$

$$\ldots \longrightarrow H^q(G_X,F'(\tilde{X})) \longrightarrow H^q(G_X,F(\tilde{X})) \longrightarrow H^q(G_X,F''(\tilde{X}))$$

$$\longrightarrow H^{q+1}(G_X, F'(\tilde{X}) \longrightarrow \ldots$$

Ahora, por la equivalencia de categorías, se cumple:

$F'(\tilde{X})^{G_X} = F'(X)$, $F(\tilde{X})^{G_X} = F(X)$, $F''(\tilde{X})^{G_X} = F''(X)$,

por tanto, se tiene la igualdad para q=0, y por ([T] 0.21):

$$H^q(X,F) \simeq H^q(G_X, F(\tilde{X}), \text{ para todo } q \geq 0. \ \#$$

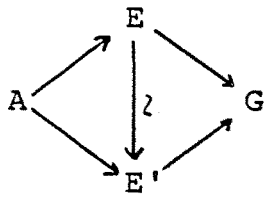
Aplicación al problema de inmersión

Dada una sucesión exacta: $1 \longrightarrow A \longrightarrow E \dashrightarrow G \longrightarrow 1$ de grupos finitos con núcleo A abeliano, A tiene una estructura de G-módulo, definida en la forma siguiente: E opera sobre A por conjugación y por ser A abeliano, A opera trivialmente sobre sí mismo, por tanto $G \cong E/A$ opera sobre A. Si para cada s de G fijamos una antiimagen u_s en E, se tiene

$$u_s\, u_t = a_{s,t}\, u_{st} \qquad \text{con} \quad a_{s,t} \in A.$$

Los elementos $a_{s,t}$ definen un 2-cociclo de G en A, que determina un elemento de $H^2(G,A)$.

Hay una correspondencia 1-1 entre clases de isomorfía de extensiones de A por G y elementos de $H^2(G,A)$, para las posibles estructuras de G-módulo de A, donde se dice que 2 extensiones E y E' de A por G son isomorfas si existe un isomorfismo $E \xrightarrow{\sim} E'$ que haga conmutativo el diagrama:



Dado un epimorfismo φ: $G' \longrightarrow G$, queda definida, a través de φ, una estructura de G'-módulo para A y φ induce un morfismo:

$$\varphi^*: H^2(G,A) \longrightarrow H^2(G',A),$$

llamado morfismo de inflación. Si $\varepsilon \in H^2(G,A)$ ésta representado por un cociclo $a_{s,t}$, con s y t elementos de G,

$$(s',t') \longmapsto a_{\varphi(s'),\varphi(t')} \text{ , para } s',t' \text{ de } G',$$

es un representante de $\varphi^*\varepsilon$.

Proposición 1.16. Sean X un esquema conexo, localmente noetheriano, $Y \longrightarrow X$ un recubrimiento galoisiano con grupo G, dado por el epimorfismo $\varphi : G_X \longrightarrow G$. Sean

$$(E): \quad 1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

una sucesión exacta de grupos con núcleo A abeliano, $\varepsilon \in H^2(G,A)$ el elemento correspondiente a (E). Entonces el problema de inmersión dado por $Y|X$, G, (E) tiene solución si y sólo si el elemento $\varphi^*\varepsilon$ de $H^2(G_X,A)$ es nulo.

Demostracion. Consideramos el diagrama con filas exactas:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & E \underset{G}{\times} G_X & \xrightarrow{p_2} & G_X & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle p_1} & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{f} & G & \longrightarrow & 1 \end{array} ,$$

donde $E \underset{G}{\times} G_X := \{(e,s) \in E \times G_X \ / \ f(e) = \varphi(s)\}$, y p_1, p_2 son las proyecciones sobre cada factor.

La extensión de grupos de la fila superior se corresponde con el elemento $\varphi^*\varepsilon$ de $H^2(G_X,A)$ ya que, si $\{u_s\}_{s \in G}$ es un sistema de representantes de G en E, un sistema de representantes de G_X en $E \underset{G}{\times} G_X$ es $\{v_\sigma\}_{\sigma \in G_X}$ con:

$$v_\sigma = (u_{\varphi(\sigma)} , \sigma)$$

y, por verificarse, para σ, τ de G_X:

$$v_\sigma \cdot v_\tau = (a_{\varphi(\sigma),\varphi(\tau)} \ u_{\varphi(\sigma\tau)} , \sigma\tau) = a_{\varphi(\sigma),\varphi(\tau)} \ v_{\sigma\tau} ,$$

la clase del 2-cociclo determinado por $\{v_\sigma\}$ es $\varphi^*\varepsilon$.

Que $\varphi^*\varepsilon$ sea nulo equivale a que exista una sección

$$q : G_X \longrightarrow G \underset{G}{\times} G_X$$

tal que $p_2 \circ q = id_{G_X}$. Entonces $\psi = p_1 \circ q$ verifica:

$$f \circ \psi = f \circ p_1 \circ q = \varphi \circ p_2 \circ q = \varphi.$$

Recíprocamente, si existe ψ tal que $f \circ \psi = \varphi$, podemos definir una sección q por $q(\sigma) = (\psi(\sigma), \sigma)$ para $\sigma \in G_X$. #

Si en la proposición anterior, tomamos como esquema X el espectro de un cuerpo K, se recupera un resultado de Höchsmann ([HO] 1.1), en el que da la equivalencia entre la resolución del problema de inmersión sobre K y la anulación de la imagen de ε por el morfismo de inflación en $H^2(G_K, A)$, donde G_K es el grupo de Galois absoluto de K. El hecho que hace posible la generalización del resultado es que, a cada recubrimiento principal de un esquema X conexo con grupo E, le corresponde un morfismo del grupo de Galois absoluto de X , G_X, en E, de la misma manera que, a un álgebra galoisiana sobre un cuerpo K con grupo E, le corresponde un morfismo del grupo de Galois absoluto de K, G_K, en E.

Veamos ahora, que mediante la proposición 1.16, podemos dar también la obstrucción a un problema de inmersión sobre un cuerpo de números, con condiciones de ramificación.

Sea Θ un anillo de Dedekind, K su cuerpo de fracciones. Si L|K es extensión de Galois con grupo G, no ramificada fuera de S, conjunto finito de primos de Θ, el epimorfismo

$G_K \longrightarrow G$, correspondiente a $L|K$, factoriza a través de G_K^S, grupo de Galois de la máxima extensión de K no ramificada fuera de S, grupo isomorfo al grupo de Galois absoluto del esquema Spec Θ-S (cf.prop. 1.10). Como consecuencia de la proposición 1.16, tenemos:

Corolario 1.17. Sea $L|K$ una extensión de Galois con grupo G, no ramificada fuera de S, dada por el epimorfismo $\varphi: G_K^S \longrightarrow G$, sea:

$$(E): \quad 1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

una sucesión exacta de grupos con núcleo A abeliano, sea $\varepsilon \in H^2(G,A)$ el elemento correspondiente a (E).

El problema de inmersión dado por $L|K$, G, (E) tiene solución no ramificada fuera de S si y sólo si el elemento $\varphi^*(\varepsilon)$ de $H^2(G_K^S, A)$ es nulo. #

Dada una extensión de grupos $1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$, A tiene una estructura de G-módulo. A través de un epimorfismo $\varphi: G_X \longrightarrow G$, con G_X grupo de Galois absoluto de un esquema X, A hereda una estructura de G_X-módulo continuo (si G es finito). Entonces podemos construir el haz abeliano no ramificado sobre X, $A_{\tilde{X}|X}$, asociado a A, y por las proposiciones 1.13 y 1.15, tenemos:

$$H^2(G_{\tilde{X}}, A) \simeq H^2_{\acute{e}t}(X, A_{\tilde{X}|X})$$

es decir, podemos considerar la obstrucción al problema de in

mersión sobre X como elemento de un grupo de cohomología étale.

§4. RESOLUCION DEL PROBLEMA DE INMERSION CON CONDICIONES DE RAMIFICACION

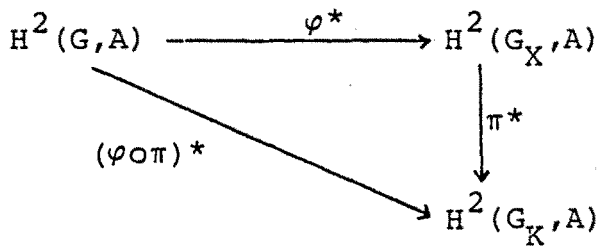
Sea X un esquema normal, K su cuerpo de funciones. Por la proposición 1.10 tenemos un epimorfismo $G_K \xrightarrow{\pi} G_X$ del grupo de Galois absoluto de K en el de X. Por tanto, a cada problema de inmersión definido sobre X, podemos asociarle un problema de inmersión sobre K. Diremos que el problema de inmersión sobre X *es resoluble sobre* K si es resoluble el problema de inmersión sobre K asociado. En lo que sigue veremos en qué condiciones la resolubilidad sobre K implica la resolubilidad sobre X.

Proposición 1.18. Sea X un esquema normal casi compacto con cuerpo de funciones K. Sea G_X el grupo de Galois absoluto de X, G_K el grupo de Galois absoluto de K. Sea A un G_X-módulo continuo. Entonces son equivalentes.

1) Para todo problema de inmersión sobre X, dado por una sucesión exacta de grupos con núcleo A, la resolubilidad del problema sobre K implica su resolubilidad sobre X.

2) El morfismo de inflación $H^2(G_X, A) \longrightarrow H^2(G_K, A)$ es inyectivo.

Demostración. Sea $\pi : G_K \longrightarrow G_X$ el epimorfismo dado por la proposición 1.10. Para cada epimorfismo $\varphi: G_X \longrightarrow G$, con G finito, tal que A herede estructura de G-módulo a través de φ (es decir tal que el núcleo de φ opere trivialmente sobre A), el diagrama



es conmutativo. Si π^* es inyectivo, para cada $\varepsilon \in H^2(G,A)$ tal que $(\varphi o\pi)^*(\varepsilon) = 0$ se cumple $\varphi^*(\varepsilon) = 0$, por tanto aplicando la proposición 1.16 a Spec K y a X, se tiene 1).

Recíprocamente, supuesto 2), sea $\psi \in H^2(G_X,A)$ tal que $\pi^*\psi=0$. Por ser $H^2(G_X,A) = \varinjlim H^2(G,A)$, con G recorriendo los cocientes finitos de G_X, tenemos, para algún cociente finito de G_X, $\psi= p^*\varepsilon$, con

$$p^*: H^2(G,A) \longrightarrow H^2(G_X,A)$$

inducido por $p: G_X \longrightarrow G$. Entonces se cumple: $0=\pi^*\psi= (\pi op)^*\varepsilon$, es decir el problema de inmersión dado por p es resoluble sobre K, por tanto lo es sobre X, es decir, se tiene $\psi=p^*\varepsilon = 0$.#

Proposición 1.19. Sean X, K, G_X, G_K, como en la proposición anterior. Sea $n \in \mathbb{N}$ tal que X no contenga los divisores de n (i.e. $(n,k(x))= 1$ para cada $x \in X$) y tal que el haz $(\mu_n)_X$ de raices n-ésimas de la unidad sea no ramificado sobre X. Entonces, el núcleo del morfismo de inflación

$$\pi^*: H^2(G_X, \mathbb{Z}/n\mathbb{Z}) \longrightarrow H^2(G_K, \mathbb{Z}/n\mathbb{Z}) \quad ,$$

donde $\mathbb{Z}/n\mathbb{Z}$ tiene la estructura de módulo trivial sobre G_X y G_K, es isomorfo a $H^1(X,(G_m)_X)/n.H^1(X,(G_m)_X)$.

Demostración. Por ser $(\mu_n)_X$ no ramificado, podemos aplicar la proposición 1.15 y obtenemos

$$H^2(X,\mu_n) = H^2(G_X,\mu_n(\bar{X})) = H^2(G_X, \mathbb{Z}/n\mathbb{Z}).$$

La condición (car k(x),n) = 1 para cada x de X da que la sucesión

$$1 \longrightarrow (\mu_n)_X \xrightarrow{i} (G_m)_X \xrightarrow{.n} (Gm)_X \longrightarrow 1$$

es exacta (prop. 1.12) y podemos escribir la sucesión exacta de cohomología asociada.

$$\cdots \longrightarrow H^1(X,G_m) \xrightarrow{.n} H^1(X,G_m) \xrightarrow{\partial} H^2(X,\mu_n) \xrightarrow{i^*} H^2(X,G_m) \longrightarrow \cdots$$

Sobre Spec K, es exacta la sucesión:

$$1 \longrightarrow (\mu_n)_{\text{Spec K}} \longrightarrow (G_m)_{\text{Spec K}} \longrightarrow (G_m)_{\text{Spec K}} \longrightarrow 1$$

y la sucesión exacta de cohomología asociada es

$$\begin{array}{ccccccc} \cdots \longrightarrow & H^1(\text{Spec K},G_m) & \xrightarrow{\partial} & H^1(\text{Spec K},\mu_n) & \longrightarrow & H^2(\text{Spec K},G_m) & \longrightarrow \cdots \\ & \| & & \| & & \| & \\ & H^1(G_K, \bar{K}^*) & & H^1(G_K, A) & & H^2(G_K, \bar{K}^*) & \end{array}$$

donde $H^1(G_K, \bar{K}^*) = 0$, por el teorema 90 de Hilbert.

Tenemos el diagrama conmutativo

$$\begin{array}{ccc} H^2(X,\mu_n) & \xrightarrow{i^*} & H^2(X,G_m) \\ \downarrow & & \downarrow \\ H^2(G_K,A) & \xrightarrow{i_K^*} & H^2(G_K,\bar{K}^*) \end{array} ,$$

con i_K^* inyectiva, y $H^2(X,G_m) \longrightarrow H^2(G_K, \bar{K}^*)$ inyectiva ([M]III 2.22)
Por tanto Ker π^*= Ker i^*.
Calculamos Ker i^* utilizando la sucesión exacta sobre X:
Ker i^*= Im ∂ = $H^1(X,G_m)$/Ker ∂ = $H^1(X,G_m)$ / Im (.n) =

$$= H^1(X,G_m)) \;/\; n.\; H^1(X,G_m) \;.\; \#$$

Teorema 1.20. Sea K un cuerpo de números, Θ_K su anillo de enteros, S un conjunto finito de primos de Θ_K. Sea A un grupo abeliano de exponente n . Suponemos que S contiene los primos que dividen n y los que ramifican en $K(\zeta_n)|K$, para ζ_n raíz primitiva n-ésima de 1. Entonces son equivalentes:
1) Todo problema de inmersión resoluble sobre K y dado por una sucesión exacta de grupos que sea extensión central de A, tiene solución no ramificada fuera de S.
2) El número de S-clases de ideales de Θ_K es primo con n.

Demostración. Sea X = Spec Θ_K-S. Por toda extensión central, A queda dotado de estructura de G-módulo trivial y por tanto de módulo trivial sobre G_X y G_K. Por la proposición 1.18, la condición 1) equivale a que el morfismo de inflación

$$\pi^*: H^2(G_X,A) \longrightarrow H^2(G_K,A)$$

sea inyectivo. Sea $A \simeq \oplus\, \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$, descomposición de A en suma directa de grupos cíclicos, con cada p_i primo. Por ser A módulo trivial, el isomorfismo de A con $\oplus\, \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ lo es también de G_X – y G_K – módulos. Por tanto, tenemos:

$H^2(G_X,A) \simeq \oplus\ H^2(G_X, \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$; $H^2(G_K,A) \simeq \oplus\ H^2(G_K, \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$

y π^* es suma directa de los morfismos

$$\pi_i^*: H^2(G_X, \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) \longrightarrow H^2(G_K, \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}).$$

Por tanto π^* es inyectivo si y sólo si lo es cada π_i^*. Por la proposición 1.19, se tiene

$$\text{Ker } \pi_i^* = H^1(X, G_m) \,/\, p_i^{\alpha_i}.H^1(X,G_m) \ ,$$

para cada i, ya que, por contener S los primos que dividen p_i y los que ramifican en $K(\zeta_{p_i^{\alpha_i}})|K$, X cumple las condiciones (car k(x), $p_i^{\alpha_i}$) = 1, para cada x de X, y $(\mu_{p_i^{\alpha_i}})_X$ es no ramificado sobre X.

Veamos ahora que $H^1(X,G_m) \,/\, p_i^{\alpha_i} \,.\, H^1(X,G_m) = 0$, para cada $p_i^{\alpha_i}$, equivale a la condición 2) del enunciado. Calculamos $H^1(X,G_m)$ para $X = \text{Spec } \Theta_K - S$. Para ello, establecemos una serie de isomorfismos:

1) $H^1_{ét}(X,G_m) = H^1(X,\mathcal{O}_X^*)$, grupo de cohomología del grupo multiplicativo del haz estructural $\mathcal{O}_X$ de X para la topologia de Zariski ([M] III 4.9).

2) $H^1(X,\mathcal{O}_X^*) \simeq$ Pic X, grupo de Picard de X, es decir, grupo de clases de isomorfía de haces invertibles sobre X ([G_1] 0.5.6.3).

3) Pic X $\simeq$ Ca Cl X, grupo de divisores de Cartier sobre X, módulo equivalencia lineal ([HA] II 6.15), ya que X es íntegro, por ser un abierto de Spec Θ_K.

4) Ca Cl X $\simeq$ Cl X, grupo de divisores de Weil sobre X, módulo equivalencia lineal ([HA] II 6.11) ya que X es íntegro, noetheriano, separado y localmente factorial. En efecto, X es noe

theriano por ser subesquema abierto del esquema noetheriano Spec Θ_K ([G_1]I 4.1.7); es separado ya que $X \hookrightarrow$ Spec Θ_K es morfismo separado por ser inmersión abierta y Spec Θ_K es separado por ser afín ([G_1]I 5.2.2. y 5.3.1 (i)-(ii)); es localmente factorial por ser $(\Theta_K)_{\mathfrak{p}}$ dominio de factorización única para cada $\mathfrak{p} \in$ Spec Θ_K .

5) Sea $I_K(S) = \{\mathfrak{a}$ ideal de $\Theta_K / \mathfrak{p} \nmid \mathfrak{a}$ para $\mathfrak{p} \in S\}$.

Tenemos un isomorfismo:

$$\begin{aligned} \text{Div } (X) &\longrightarrow I_K(S) \\ \Sigma n_x\, x &\longmapsto \pi \mathfrak{p}_x^{n_x} = \mathfrak{a} \end{aligned}$$

del grupo de divisores de Weil de X en el grupo de S-ideales de Θ_K, dónde $\mathfrak{p}_x$ es el primo de Θ_K correspondiente al punto x de X. Al divisor principal (f) de Div(X), con $f \in K^*$, le corresponde el ideal generado por f. Por tanto si P_K es el grupo de ideales principales de Θ_K, tenemos:

$$Cl(X) \simeq I_K(S) \,/\, (I_K(S) \cap P_K) = Cl^S(\Theta_K),$$

grupo de S-clases de ideales de Θ_K.

Siguiendo la cadena de isomorfismos, tenemos:

$$H^1(X, G_m) \simeq Cl^S(\Theta_K).$$

Sea ahora h_S el número de S-clases de ideales de Θ_K, es decir, el orden de $Cl^S(\Theta_K)$. Que h_S sea primo con n equivale a que sea primo con cada $p_i^{\alpha_i}$, es decir a que $p_i^{\alpha_i}$ sea invertible en $Cl^S(\Theta_K)$, por tanto a:

$$Cl^S(\Theta_K) \,/\, p_i^{\alpha_i}\, Cl^S(\Theta_K) = 0$$

que equivale a que se cumpla para cada i :

$$H^1_{ét}(X, G_m) / p_i^{\alpha_i} H^1_{ét}(X, G_m) = 0.\#$$

Corolario 1.21. Con las mismas hipótesis del teorema anterior, sea h el número de clases de ideales de Θ_K. Si $(h,n)=1$, entonces todo problema de inmersión resoluble sobre K tiene solución no ramificada fuera de S.

Demostración. $X = \text{Spec } \Theta_K - S$ es abierto de $\text{Spec } \Theta_K$, por tanto tenemos un morfismo exhaustivo:

$$Cl(\text{Spec } \Theta_K) = Cl(\Theta_K) \longrightarrow Cl(X).$$

([HA] II 6.5). Entonces h_S, orden de Cl(X), divide h, orden de $Cl(\Theta_K)$. Por tanto $(h,n) = 1$ implica $(h_S,n) = 1$ y por el teorema se obtiene el resultado. #

Ejemplo. Sea M_{12} el grupo de Mathieu. Matzat y Zeh ([MA-Z]) dan una realización de M_{12} sobre Q, especializando en valores enteros $t \equiv 1 \pmod{66}$ una realización de M_{12} sobre Q(T). El conjunto de ramificación de la extensión es $S = \{2,3,5, d_1(t)\}$ con $d_1(t) = 5^{15}\, t^2 - 2^{22}\, 3^{18}$.

Consideramos el problema de inmersión dado por la extensión central universal de M_{12}

$$1 \longrightarrow \mathbb{Z}/2\,\mathbb{Z} \longrightarrow \tilde{M}_{12} \longrightarrow M_{12} \longrightarrow 1 .$$

Sea m_{12} el elemento de $H^2(M_{12}, \mathbb{Z}/2\,\mathbb{Z})$ asociado a esta extensión. Se tiene ([B-LL-V]) $\inf m_{12} = 0$ en $H^2(G_Q, \mathbb{Z}/2\,\mathbb{Z})$ para $t \geq -197$, $t \equiv 1 \pmod 4$ y $d_1(t)$ primo.

Aplicando el corolario obtenemos inf $m_{12} = 0$ en $H^2(G_{\mathbb{Q}}^S, \mathbb{Z}/2\,\mathbb{Z})$ para los mismos casos ya que 2 está en S.

Además en este caso (ver cap. II nota 2.10) todas las soluciones al problema de inmersión son propias, por tanto el problema de inmersión tiene una solución propia que no aumenta el conjunto de ramificación.

Observación. Neukirch ([N_2]) obtiene un resultado similar al teorema 1.20, con las mismas hipótesis sobre S y A calculando el núcleo del morfismo de inflación

$$H^2(G_K^S, \mathbb{Z}/p^\alpha\,\mathbb{Z}) \longrightarrow H^2(G_K, \mathbb{Z}/p^\alpha\,\mathbb{Z})$$

en función de los grupos de unidades $U_{\mathfrak{p}}$ de los completados $K_{\mathfrak{p}}$ de K en los primos $\mathfrak{p}$ de Θ_K ([N_2] 8.1). Para ello, utiliza principalmente teoría de Kummer y los teoremas de dualidad de Tate, así como los resultados que obtiene sobre la resolubilidad del problema de inmersión con datos locales. De ello deduce que la resolubilidad del problema de inmersión implica la existencia de solución no ramificada fuera de S, en el caso en que el número de clases de ideales del cuerpo $K(\zeta_p \alpha)$ sea primo con p, para cada p^α tal que $\mathbb{Z}/p^\alpha\,\mathbb{Z}$ es una componente de la descomposición de A en suma directa de cíclicos y en el caso en que K es el cuerpo $\mathbb{Q}$ de los racionales.

CAPITULO II

EL PROBLEMA DE INMERSION SOBRE CUERPOS

Para un problema de inmersión sobre un cuerpo de números K y dado por una extensión central con núcleo A abeliano, hemos hallado condiciones para que, de la resolubilidad del problema, pueda deducirse la existencia de soluciones no ramificadas fuera de un conjunto finito prefijado de primos del anillo de enteros de K (cf 1.20). Por otra parte, mediante el teorema de Ikeda ([I]), se obtiene que todo problema de inmersión resoluble sobre un cuerpo de números, dado por una extensión de grupos con núcleo abeliano, tiene una solución propia. Dados un cuerpo de números K y un conjunto finito S de primos del anillo de enteros Θ_K de K, consideramos, en este capítulo, un problema de inmersión sobre K, con la condición adicional de que las soluciones sean no ramificadas fuera de S. Para este problema, nos interesa analizar bajo qué condiciones puede construirse una solución propia a partir de una impropia. Para ello, estudiaremos previamente la variedad de las soluciones de un problema de inmersión sobre un cuerpo.

Posteriormente, revisamos formulaciones de la obstrucción

a problemas de inmersión sobre cuerpos, dados por extensiones con núcleo $\mathbb{Z}/p\mathbb{Z}$, con p primo y $\mathbb{Z}/2\mathbb{Z}$, que usaremos en el capítulo III.

§1. SOLUCIONES PROPIAS Y NO RAMIFICADAS

Empezamos introduciendo la sucesión de Hochschild-Serre asociada a un problema de inmersión.

Sea Θ un anillo de Dedekind , K su cuerpo de fracciones, S un conjunto de primos de Θ, G_K^S el grupo de Galois de la máxima extensión de K no ramificada fuera de S. En particular, si S es todo Spec Θ, menos el punto genérico, tenemos $G_K^S = G_K$, grupo de Galois absoluto de K. Consideramos el problema de inmersión dado por:

$$\begin{array}{ccccccccc} & & & & & & G_K^S & & \\ & & & & & & \downarrow \varphi & & \\ 1 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{j} & G & \longrightarrow & 1 \end{array}$$

al que llamaremos,de ahora en adelante *problema de inmersión sobre el par* (K,S).

A es G-módulo y G_K^S-módulo a través de φ. Si L|K es la extensión de Galois con grupo G dada por φ, el núcleo de φ es $G_L^{S'}$, grupo de Galois de la máxima extensión de L no ramificada fuera de S', siendo S' el conjunto de primos de Θ_L que contraen a primos de S (prop. 1.10). $G_L^{S'}$ opera trivialmente sobre A. A la sucesión exacta (cf. prop. 1.11):

$$1 \longrightarrow G_L^{S'} \longrightarrow G_K^S \longrightarrow G \longrightarrow 1 \ ,$$

podemos asociarle la sucesión exacta de Hochschild-Serre ([L] VI Th 1):

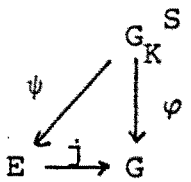
$$0 \longrightarrow H^1(G,A) \xrightarrow{\inf} H^1(G_K^S,A) \xrightarrow{\text{res}} H^1(G_L^{S'},A)^G \xrightarrow{\text{tg}} H^2(G,A) \xrightarrow{\inf} H^2(G_K^S,A),$$

donde inf: $H^2(G,A) \longrightarrow H^2(G_K^S,A)$ es el morfismo φ^* definido en el capítulo I (cf. prop. 1.17). Además, por ser la operación de $G_L^{S'}$ sobre A trivial tenemos:

$$H^1(G_L^{S'},A) = \text{Hom}(G_L^{S'},A) \text{ y } H^1(G_L^{S'},A)^G = \text{Hom}_{G_K^S}(G_L^{S'},A)$$

dónde $\text{Hom}_{G_K^S}(G_L^{S'},A)$ indica el grupo de morfismos de G_K^S-módulos (G_K^S opera sobre $G_L^{S'}$ por conjugación y sobre A a través de G).

El problema de inmersión tiene solución sobre (K,S) si existe un morfismo ψ: $G_K^S \longrightarrow E$ que haga conmutativo el diagrama



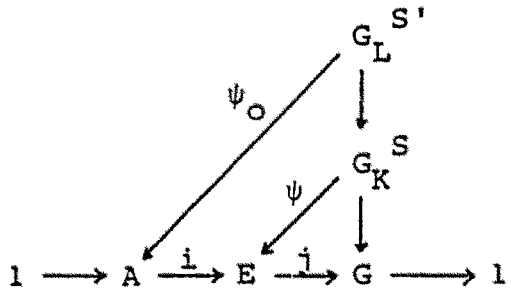
Teniendo en cuenta que el planteamiento del problema de inmersión sobre (K,S) mediante morfismos de grupos se expresa exactamente de la misma manera que sobre K, cambiando G_K por G_K^S (Cap. I §2), obtenemos que los resultados conocidos para el problema de inmersión sobre K ([HO] 2.1) son válidos sobre (K,S) con los cambios pertinentes, tal como los expresamos a continuación.

Por ser $G_L^{S'}$ el núcleo de φ, la restricción de ψ a $G_L^{S'}$ tiene imagen contenida en Ker j=i(A). Por tanto se tiene un

morfismo:

$$\psi_o : G_L^{S'} \longrightarrow A$$

que es G_K^S -morfismo. La situación obtenida se resume en el diagrama:



Si ε es elemento de $H^2(G,A)$ correspondiente a la extensión:

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1 \ ,$$

la resolubilidad del problema de inmersión equivale a inf $\varepsilon = 0$ en $H^2(G_K^S, A)$ y, por la sucesión exacta de Hochschild-Serre, a que ε esté en la imagen de

$$tg : H^1(G_L^{S'}, A)^G \longrightarrow H^2(G,A) \ ,$$

morfismo de transgresión. La restricción a $G_L^{S'}$ de un morfismo ψ de G_K^S en E tal que $j\circ\psi=\varphi$ tiene imagen ε por el morfismo de transgresión. Recíprocamente, un G_K^S-morfismo ψ_o de $G_L^{S'}$ en A tal que $tg\ \psi_o = \varepsilon$ puede ampliarse a un morfismo $\psi: G_K^S \longrightarrow E$ tal que $j\circ\psi=\varphi$.

Veamos ahora la estructura del conjunto de todas las soluciones. Por lo anterior, podemos pensarlo como la antiimagen de ε por el morfismo de transgresión.

Proposición 2.1. ([N_3] 1.1). El conjunto $\mathcal{L}_\varepsilon^S$ de las soluciones al problema de inmersión sobre (K,S) dado por el epimorfismo $\varphi: G_K^S \longrightarrow G$ y el elemento ε de $H^2(G,A)$ es un espacio afín sobre $H^1(G_K^S,A)/\ H^1(G,A)$, es decir, si $\psi_o \in \mathrm{Hom}_{G_K^S}(G_L^{S'},A)$ es solución al problema de inmersión, todas las soluciones son ψ_o + res x, con $x \in H^1(G_K^S,A)$, y, para $x \in H^1(G,A)$, ψ_o y ψ_o + res x dan la misma solución. #

Llamaremos *solución general* del problema de inmersión al conjunto de las extensiones de L correspondientes a Ker ψ_o, con $\psi_o: G_L^{S'} \longrightarrow A$ recorriendo el espacio de las soluciones. Equivalentemente (cf I §2), la solución general es el conjunto de los cuerpos solución y los cuerpos núcleos de las álgebras solución.

Proposición 2.2. En el caso particular en que A sea $\mathbb{Z}/n\mathbb{Z}$, con estructura de G-módulo trivial, y K contenga el grupo μ_n de raíces n-ésimas de la unidad, si $L(\sqrt[n]{a})$ es una solución al problema de inmersión, o un cuerpo núcleo de un álgebra solución, la solución general es:

$$L(\sqrt[n]{ra}),\ \text{con r recorriendo } U_K(S)\ /\ K^n \cap U_K(S),$$

siendo $U_K(S)$ el grupo de S-unidades de K.

En el caso $G_K^S = G_K$, es $U_K(S) = K^*$.

Demostración. $\mathrm{Hom}(G_L^{S'}, \mathbb{Z}/n\mathbb{Z})$ se corresponde con las extensiones de Galois de L, no ramificadas fuera de S' y con grupo de Galois un subgrupo de $\mathbb{Z}/n\mathbb{Z}$. Como L contiene μ_n, por teoría de Kummer ([A-T] VI 2 th.3-4),tenemos:

$$\mathrm{Hom}(G_L^{S'}, \mathbb{Z}/n\mathbb{Z}) \simeq (U_L(S') \cdot L^{*n})/L^{*n} \simeq U_L(S')/(L^{*n} \cap U_L(S')),$$

donde $U_L(S')$ indica el grupo de S'-unidades de L, es decir, el formado por los elementos de L que son unidades en el anillo de enteros del completado $L_{\mathfrak{p}}$, para todos los primos $\mathfrak{p}$ fuera de S'. El isomorfismo está definido en la forma siguiente: Sea ζ_n una raíz primitiva n-ésima de 1. Si a es un elemento de $U_L(S')$, sea α una raíz n-ésima de a. El morfismo

$$g_a: G_L^{S'} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

correspondiente a a, está definido por:

$$g_a(s) = d \quad \text{si} \quad s(\alpha) = \zeta_n^{\,d} \cdot \alpha .$$

La imagen de g_a es el grupo de Galois de $L(\sqrt[n]{a})|L$. Si ψ_o, ψ_1 son elementos de $\mathrm{Hom}(G_L^{S'}, \mathbb{Z}/n\mathbb{Z})$ correspondientes a los elementos a, b de $U_L(S')$, a $\psi_o + \psi_1$ le corresponde a.b, es decir la extensión $L(\sqrt[n]{ab})|L$.

Ahora, por ser $\mathbb{Z}/n\mathbb{Z}$ G-módulo trivial, es G_K^S-módulo trivial y tenemos:

$$H^1(G_K^S, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}(G_K^S, \mathbb{Z}/n\mathbb{Z}) \simeq U_K(S) \,/\, (K^{*n} \cap U_K(S)),$$

donde $U_K(S)$ indica el grupo de S-unidades de K, volviendo a aplicar la teoría de Kummer. #

Veamos ahora como pueden obtenerse soluciones propias a

partir de una impropia.

Proposición 2.3. Sea A isomorfo a $\mathbb{Z}/p^{\alpha}\mathbb{Z}$ como grupos. Sea $\psi_o \in \mathrm{Hom}_G(G_L^{S'}, A)$ una solución impropia al problema de inmersión. Entonces todas las soluciones propias son ψ_o + res x, con x elemento de orden p^{α} en $H^1(G_K^S, A)/H^1(G, A)$.

Demostración. Si $\psi_o: G_L^{S'} \longrightarrow A$ es no exhaustivo, su imagen $\psi_o(G_L^{S'})$ es un subgrupo de A distinto del total, por tanto anulado por $p^{\alpha-1}$. El morfismo de multiplicación por $p^{\alpha-1}$ de A en A es G-morfismo, por tanto induce un morfismo:

$$H^1(G_L^{S'}, A)^G \xrightarrow{.p^{\alpha-1}} H^1(G_L^{S'}, A)^G$$

y si $p^{\alpha-1}$ anula la imagen de ψ_o, tenemos $p^{\alpha-1}.\ \psi_o = 0$. Recíprocamente, si $p^{\alpha-1}.\ \psi_o$ es cero en $H^1(G_L^{S'}, A)^G$, ψ_o no es exhaustivo.

Dada ψ_o solución impropia, veamos de todas las soluciones ψ_o + res x cuales son las propias. Tenemos que ψ_o + res x impropia equivale a $p^{\alpha-1}.\ (\psi_o + \mathrm{res}\ x) = 0$ y, por ser $p^{\alpha-1}.\ \psi_o = 0$, a $p^{\alpha-1}.\ (\mathrm{res}\ x) = 0$. Como $H^1(G_K^S, A)/H^1(G, A)$ es isomorfo a la imagen de la restricción, $p^{\alpha-1}.\ (\mathrm{res}\ x) = 0$ equivale a que $p^{\alpha-1}$ anule la clase de x en $H^1(G_K^S, A)/H^1(G, A)$. Las soluciones propias corresponden pues a elementos de orden p^{α} de $H^1(G_K^S, A)/H^1(G,A)$. #

Sea A un G-módulo trivial, $A \simeq \oplus\ \mathbb{Z}/p_i^{\alpha_i}$ su descomposición en producto de grupos cíclicos, con p_i primos. Entonces tenemos:

$$H^1(G_L^{S'},A) \simeq \oplus\ H^1(G_L^{S'},\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$$

y también:

$$H^1(G_L^{S'},A)^G \simeq \oplus\ H^1(G_L^{S'},\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^G\ .$$

Se dice que los elementos $h_1, h_2, \ldots, h_k$ de un grupo abeliano H de exponente n son *independientes* si una igualdad del tipo:

$$x_1h_1 + x_2h_2 + \ldots + x_kh_k = 0 \quad , x_i \in \mathbb{Z}\ ,$$

se verifica sólo si cada x_i es divisible por el orden de h_i, para $i = 1,2,\ldots,k$.

En el caso en que el grupo H sea el grupo de los morfismos de un grupo G en un grupo cíclico finito C, los morfismos $h_1, h_2, \ldots, h_k$ son independientes si y sólo si el morfismo que determinan:

$$\begin{aligned} h:\ G &\longrightarrow h_1(G) \oplus h_2(G) \oplus \ldots \oplus h_k(G) \\ g &\longrightarrow (h_1(g),h_2(g),\ldots,h_k(g)) \end{aligned}$$

es exhaustivo (Ver [HO] §2).

Sea n el exponente de A. Un elemento ψ de $H^1(G_L^{S'},A)^G$ será una solución propia al problema de inmersión si y sólo si cada

una de sus componentes ψ_i en la descomposición en suma directa es exhaustiva y los morfismos obtenidos componiendo las ψ_i con las inclusiones:

$$\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

son morfismos independientes.

Proposición 2.4. Para cada primo p que divide n = exp A, sea v_p la valoración de n en p y supongamos que existen elementos de orden p^{v_p} independientes en:

$$H^1(G_K^S, \mathbb{Z}/p^{v_p}\mathbb{Z})/H^1(G, \mathbb{Z}/p^{v_p}\mathbb{Z}),$$

en número mayor que el p-rango a_p de A.

Entonces todo problema de inmersión dado por un elemento ε de $H^2(G,A)$, resoluble sobre (K,S), tiene una solución propia no ramificada fuera de S.

Demostración. Sea $\psi_o \in H^1(G_L^{S'},A)^G$ una solución impropia del problema de inmersión. Buscamos un elemento x de $H^1(G_K,A)$ tal que $\psi = \psi_o + \text{res } x$ sea solución propia. Para cada divisor primo p de n = exp A, sea A_p la p-componente primaria de A. Para que ψ sea exhaustivo, basta que sea exhaustiva cada componente ψ_p de ψ en $H^1(G_L^{S'},A_p)$. Podemos suponer pues $n = p^v$, con p primo, $v = v_p$.

Sea A_o la imagen de ψ_o. Sea $A_o = \oplus\, \mathbb{Z}/p^{\alpha_i}\mathbb{Z}$ su descomposición en suma directa de grupos cíclicos. Los morfismos:

$$G_L^{S'} \xrightarrow{\psi_{o,i}} \mathbb{Z}/p^{\alpha_i}\mathbb{Z} \longrightarrow \mathbb{Z}/p^{v}\mathbb{Z} \quad ,$$

donde $\psi_{o,i}$ son las componentes de ψ_o en cada $H^1(G_L^{S'}, \mathbb{Z}/p^{\alpha_i}\mathbb{Z})$, son r morfismos independientes.

Sean $y_1, y_2, \ldots, y_s$, con $s \geq r$, elementos independientes de orden p^v de

$$H^1(G_K^S, \mathbb{Z}/p^v\mathbb{Z}) \,/\, H^1(G, \mathbb{Z}/p^v\mathbb{Z}).$$

Veamos que existe un y_j tal que $\psi_o \oplus \text{res } y_j$ es exhaustivo. Si no fuera así, tendríamos s relaciones de dependencia:

$$\lambda_1^j \psi_{o,1} + \lambda_2^j \psi_{o,2} + \ldots + \lambda_r^j \psi_{o,r} + \mu_j \text{ res } y_j = 0,$$

con λ_i^j, μ_j en $\mathbb{Z}$. Por ser los $\psi_{o,i}$ independientes, μ_j no es divisible por p^v. Los elementos μ_j res y_j son pues no nulos e independientes en $H^1(G_L^{S'}, \mathbb{Z}/p^v\mathbb{Z})$, por serlo los res y_j. Generan pues un subgrupo de p-rango s .De las relaciones de dependencia, se deduce que éste está incluído en el generado por los $\psi_{o,i}$, de p-rango r,menor que el p-rango de A. Llegamos pues a contradicción.

Tenemos así un y de $H^1(G_K^S, \mathbb{Z}/p^v\mathbb{Z})$ tal que:

$$\psi_o \oplus \text{res } y: G_L^{S'} \longrightarrow A_o \oplus \mathbb{Z}/p^v\mathbb{Z}$$

es exhaustivo. Sea a un elemento de A-Im ψ_o, sea x el elemento de $H^1(G_K^S, A) = \text{Hom}(G_K^S, A)$ obtenido componiendo y con el morfismo de $\mathbb{Z}/p^v\mathbb{Z}$ en A que envía el 1 al elemento a. Entonces en la imagen de $\psi_o \oplus \text{res } x$ están, además de los elementos del tipo $(a_o, 0)$, con $a_o \in \text{Im } \psi_o$, el elemento $(0, a)$. Por tanto, $\psi_o + \text{res } x$

tiene imagen mayor que ψ_o.

Reiterando el proceso, llegamos a obtener ψ exhaustivo.#

Veamos ahora cuando hay suficientes elementos independientes de orden p^{v_p} en cada $H^1(G_K^S, \mathbb{Z}/p^{v_p}\mathbb{Z})/H^1(G, \mathbb{Z}/p^{v_p}\mathbb{Z})$.

Proposición 2.5. Sea K un cuerpo de números. Si K contiene las raíces p^α -ésimas de la unidad y S contiene los primos que dividen p, en $H^1(G_K^S, \mathbb{Z}/p^\alpha\mathbb{Z})$ hay (#S) elementos de orden p^α independientes.

Demostración. Por la demostración de 2.2., tenemos:

$$H^1(G_K^S, \mathbb{Z}/p^\alpha\mathbb{Z}) \simeq U_K(S)/K^{*p^\alpha} \cap U_K(S) ,$$

con $U_K(S)$ grupo de S-unidades de K. Ahora ([GO] 3-3-11), tenemos:

$$U_K(S) \simeq W_K \times V_K(S),$$

con W_K grupo de raices de la unidad de K y $V_K(S)$ grupo abeliano libre de rango (#S)-1. Por tanto $\zeta_p k$, raiz primitiva p^k-ésima de 1, con k máximo exponente tal que $\zeta_p k$ esté en K, y los generadores de $V_K(S)$ son elementos de orden p^α de $U_K(S)/(K^{*p^\alpha} \cap U_K(S))$, independientes. Por tanto en $H^1(G_K^S, \mathbb{Z}/p^\alpha\mathbb{Z})$ hay (#S) elementos de orden p^α independientes.#

Proposición 2.6. Sea K un cuerpo de números, S un conjunto finito de primos de θ_K que contenga los primos que dividen p y

los que ramifican en $K(\zeta_{p^\alpha}) \mid K$. Entonces, en $H^1(G_K^S, \mathbb{Z}/p^\alpha\mathbb{Z})$ hay (#S)-1 elementos de orden p^α independientes.

Demostración. Sea ζ_{p^α} una raiz primitiva p^α-ésima de 1. Sea F el grupo de Galois de $K(\zeta_{p^\alpha}) \mid K$. Sea S' el conjunto de primos de $\Theta_{K(\zeta_{p^\alpha})}$, anillo de enteros de $K(\zeta_{p^\alpha})$ que contraen a primos de S. Tenemos la sucesión exacta.

$$1 \longrightarrow G_{K(\zeta_{p^\alpha})}^{S'} \longrightarrow G_K^S \longrightarrow F \longrightarrow 1,$$

y el morfismo de restricción

$$\begin{array}{ccc} H^1(G_K^S, \mathbb{Z}/p^\alpha\mathbb{Z}) & \xrightarrow{\text{res}} & H^1(G_{K(\zeta_{p^\alpha})}^{S'}, \mathbb{Z}/p^\alpha\mathbb{Z})^F \\ \| & & \| \\ \text{Hom}(G_K^S, \mathbb{Z}/p^\alpha\mathbb{Z}) & & \text{Hom}_F(G_{K(\zeta_{p^\alpha})}^{S'}, \mathbb{Z}/p^\alpha\mathbb{Z}) \end{array}$$

Por la demostración de 2.2, tenemos

$$\text{Hom}(G_{K(\zeta_{p^\alpha})}^{S'}, \mathbb{Z}/p^\alpha\mathbb{Z}) \simeq U_{K(\zeta_{p^\alpha})}(S')/K(\zeta_{p^\alpha})^{*p^\alpha} \cap U_{K(\zeta_{p^\alpha})}(S')),$$

donde el elemento g_a, correspondiente al elemento a de $U_{K(\zeta_n)}(S')$ por el isomorfismo, está definido por:

$$g_a(s) = d \quad \text{si} \quad s(\alpha) = \zeta_{p^\alpha}{}^d \alpha .$$

Si $a \in K$, g_a se extiende a G_K^S, ya que $s(\alpha)$ y α difieren en una raiz p^α-ésima de 1, para todo s de G_K^S. Por tanto, existe un elemento $\tilde{g}_a$ de $\text{Hom}(G_K^S, \mathbb{Z}/p^\alpha\mathbb{Z})$ tal que $\text{res}(\tilde{g}_a) = g_a$.

Ahora, si g_a es de orden p^α en Hom $(G_{K(\zeta_{p^\alpha})}^{S'}, \mathbb{Z}/p^\alpha\mathbb{Z})$, $\tilde{g}_a$ tiene orden p^α en

$$\text{Hom}\,(G_K^S, \mathbb{Z}/p^\alpha\mathbb{Z}) = H^1(G_K^S, \mathbb{Z}/p^\alpha\mathbb{Z}).$$

Si a es un elemento de $U_S(K)$, es S'-unidad en $K(\zeta_{p^\alpha})$. Tenemos $U_S(K) \simeq V_K(S) \times W_K$, con $V_K(S)$ grupo abeliano libre de rango (#S)-1. Si a es generador de una componente $\mathbb{Z}$ de $V_K(S)$, a tiene orden p^α en

$$U_{K(\zeta_{p^\alpha})}(S')/(U_{K(\zeta_{p^\alpha})}(S') \cap K(\zeta_{p^\alpha})^{*\,p^\alpha}).$$

Los g_a correspondientes son elementos de orden p^α en $H^1(G_{K(\zeta_{p^\alpha})}^{S'}, \mathbb{Z}/p^\alpha\mathbb{Z})$ y los $\tilde{g}_a$ en $H^1(G_K^S, \mathbb{Z}/p^\alpha\mathbb{Z})$. Tenemos pues (#S)-1 elementos de orden p^α independientes en $H^1(G_K^S, \mathbb{Z}/p^\alpha\mathbb{Z})$.#

Utilizando propiedades de grupos abelianos, se obtiene:

Proposición 2.7. Sea s el número de elementos independientes de orden p^α de $H^1(G_K^S, \mathbb{Z}/p^\alpha\mathbb{Z})$. Sea r el p-rango de $H^1(G, \mathbb{Z}/p^\alpha\mathbb{Z})$. Si $r < s$, en el cociente

$$H^1(G_K^S, \mathbb{Z}/p^\alpha\mathbb{Z})/H^1(G, \mathbb{Z}/p^\alpha\mathbb{Z})$$

hay s-r elementos independientes de orden p^α. #

Teorema 2.8. Sea K un cuerpo de números, Θ_K su anillo de enteros, sea S un conjunto finito de primos de Θ_K. Sean L|K una extensión de Galois con grupo G finito, no ramificada fuera de S, A un G-módulo trivial de exponente n. Para cada primo p divisor

de n, sea r_p el p-rango de Hom $(G, \mathbb{Z}/p^{v_p}\mathbb{Z})$, con $v_p = v_p(n)$, valoración de n en p. Suponemos que S contiene los primos que dividen n y los que ramifican en $K(\zeta_n)|K$. Entonces se verifica:

Si, para cada divisor primo p de n, el p-rango a_p de A verifica: $r_p + a_p + 1 < \#S$ ($r_p + a_p < \#S$ si $K \supset \mu_{v_p}$) entonces todo problema de inmersión resoluble sobre (K,S), dado por $L|K$ y una extensión central de A por G tiene solución propia no ramificada fuera de S.

Demostración. Por la proposición 2.6, para cada divisor primo p de $n = \exp A$, hay $(\#S)-1$ elementos de orden p^{v_p} independientes en $H^1(G_K^S, \mathbb{Z}/p^{v_p}\mathbb{Z})$ y, por la proposición 2.7, hay $(\#S)-1-r_p$ elementos de orden p^{v_p} independientes en

$$H^1(G_K^S, \mathbb{Z}/p^{v_p}\mathbb{Z})/H^1(G, \mathbb{Z}/p^{v_p}\mathbb{Z}).$$

Ahora, por la hipótesis $(\#S)-1-r_p > a_p$, aplicando la proposición 2.4, obtenemos que el problema tiene solución propia no ramificada fuera de S. Si $K \supset \mu_{v_p}$, podemos aplicar 2.5. en lugar de 2.6. #

Observación. En el caso en que K contiene las raices p^α-ésimas de 1 y A es $\mathbb{Z}/p^\alpha\mathbb{Z}$, sea L la extensión de Galois de K con grupo G definida por $\varphi: G_K^S \longrightarrow G$, y sea S' el conjunto de primos de Θ_L que contraen a primos de S. La extensión de L correspondiente a la solución impropia ψ_o es $L(\sqrt[p^\alpha]{a})$, con a elemento de L, S'-unidad y tal que $\sqrt[p]{a} \in L$. La solución propia dada

por ψ_o + res x es $L(\sqrt[p^\alpha]{ab})$, donde b es el elemento de $U_K(S)$ correspondiente a x.

Si A es abeliano de exponente n y K contiene las raíces n-ésimas de 1, entonces, si $A = \oplus\ \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ es la descomposición de A en suma directa de grupos cíclicos, la extensión de L correspondiente a ψ_o es compuesta de extensiones $L(\sqrt[p_i^{\alpha_i}]{a_i})$, con a_i elemento de $U_L(S')$. La solución propia es compuesta de extensiones $L(\sqrt[p_i^{\alpha_i}]{a_i\ b_i})$, donde b_i es el elemento de $U_K(S)$ correspondiente al elemento x_i de orden $p_i^{\alpha_i}$ de $H^1(G_K^S, \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$ elegido en la construcción de la solución propia.

El teorema anterior, junto con el 1.20 del capítulo I, nos permite ahora enunciar el siguiente resultado:

Teorema 2.9. Sea L|K una extensión galoisiana de un cuerpo de números K no ramificada fuera de un conjunto S de primos del anillo de enteros Θ_K de K. Sea $G = Gal(L|K)$ y A un G-módulo trivial de exponente n.

Suponemos que se cumplen las siguientes condiciones:

1) S contiene los primos que dividen n y los que ramifican en $K(\zeta_n)|K$.

2) El número h_S de S-clases de Θ_K es primo con n.

3) Para cada divisor primo p de n, se cumple:

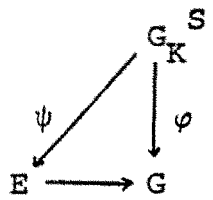
$$r_p + a_p + 1 < \#S\ ,$$

donde a_p = p-rango de A, r_p = p-rango de Hom(G,A).

Entonces todo problema de inmersión resoluble sobre K (es de-

cir sin hipótesis sobre la ramificación de las soluciones) dado por un elemento ε de $H^2(G,A)$ tiene solución propia no ramificada fuera de S. #

Nota 2.10. En el caso de una extensión central no trivial, con núcleo $\mathbb{Z}/p\,\mathbb{Z}$, p primo, todas las soluciones al problema de inmersión son propias. En efecto, si ψ es solución impropia, es conmutativo el diagrama:



y la imagen de ψ es un subgrupo E_o de E distinto del total. Entonces la antiimagen de E_o en $\mathbb{Z}/p\,\mathbb{Z}$ es distinta del total, por tanto 0. E_o es pues isomorfo a G y el isomorfismo de G en E_o es una sección para la extensión, lo cual contradice el que sea no trivial.

§2. PROBLEMAS DE INMERSION CON NUCLEO $\mathbb{Z}/p\,\mathbb{Z}$

En el §1, hemos analizado la variedad de las soluciones para un problema de inmersión dado por una extensión central. Nos interesa ahora estudiar el problema de construcción explícita de soluciones al problema de inmersión en el caso de una extensión con núcleo $\mathbb{Z}/p\,\mathbb{Z}$. Para ello, además de la condición ya vista de que la imagen por el morfismo de inflación del elemento ε de $H^2(G, \mathbb{Z}/p\,\mathbb{Z})$, asociado a la extensión, sea

nula, necesitamos formulaciones alternativas de la resolubilidad del problema de inmersión que introducimos a continuación.

Sea p primo, K un cuerpo de característica distinta de p y que contenga el grupo μ_p de raices p-ésimas de la unidad. Sean $L|K$ una extensión de Galois con grupo G, sea

$$1 \longrightarrow \mathbb{Z}/p\,\mathbb{Z} \longrightarrow E \longrightarrow G \longrightarrow 1$$

una extensión de $\mathbb{Z}/p\,\mathbb{Z}$ por G, central por ser $\mathbb{Z}/p\,\mathbb{Z}$ G-módulo trivial. Suponemos la extensión no trivial y planteamos el problema de inmersión dado por:

$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & & \downarrow \varphi & & \\ 1 & \longrightarrow & \mathbb{Z}/p\,\mathbb{Z} & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

Por 2.10, tenemos que todas las soluciones a este problema de inmersión son propias y, aplicando 2.2, que, dada una solución $L(\sqrt[p]{a})$ todas las soluciones son:

$$L(\sqrt[p]{ra}),$$

con r recorriendo un sistema de representantes de K^*/K^{*p}.

En las dos proposiciones que siguen, recordamos un resultado clásico que da una condición necesaria y suficiente para la existencia de soluciones al problema de inmersión (cf [H], [I]), utilizado también en [MS].

Fijamos desde ahora una raíz primitiva p-ésima ζ_p de 1, y el isomorfismo que determina:

$$\mathbb{Z}/p\,\mathbb{Z} \longrightarrow \mu_p$$

$$n \longmapsto \zeta_p^{\,n}$$

Proposición 2.11. Sea $\gamma \in L^*$. Entonces $L(\sqrt[p]{\gamma})\,|K$ es solución al problema de inmersión:

$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & & \downarrow & & \\ 1 & \longrightarrow & \mathbb{Z}/p\,\mathbb{Z} & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

si y sólo si para cada $s \in G = Gal(L|K)$ se tiene $\gamma^s = b_s^{\,p}\,\gamma$ con $b_s \in L^*$ verificando:

$$\frac{b_s\, b_t^{\,s}}{b_{st}} = \zeta_p^{\,a_{s,t}}$$

donde $a_{s,t}$ es un 2-cociclo de G en $\mathbb{Z}/p\,\mathbb{Z}$ que representa el elemento ε de $H^2(G, \mathbb{Z}/p\,\mathbb{Z})$ que corresponde a la extensión E.

Demostración. Para que $L(\sqrt[p]{\gamma})\,|K$ sea extensión de Galois es condición necesaria y suficiente que $L(\sqrt[p]{\gamma^s})$ sea igual a $L(\sqrt[p]{\gamma})$ para cada s de G o equivalentemente, por teoría de Kummer ([A-T] VI th3) a que $\gamma^s\,\gamma^{-1}$ sea elemento de L^{*p}. Sea $b_s \in L^*$ tal que $\gamma^s = b_s^{\,p}\,.\,\gamma$ para $s \in G$.

Consideramos la sucesión exacta

$$1 \longrightarrow \mathbb{Z}/p\,\mathbb{Z} \simeq Gal(L(\sqrt[p]{\gamma})\,|L) \longrightarrow Gal(L(\sqrt[p]{\gamma})\,|K) \longrightarrow Gal(L|K) \longrightarrow 1,$$

donde el isomorfismo de $\mathbb{Z}/p\,\mathbb{Z}$ en $Gal(L(\sqrt[p]{\gamma})\,|L)$ es:

$$\mathbb{Z}/p\,\mathbb{Z} \xrightarrow{\sim} \mathrm{Gal}(L(\sqrt[p]{\gamma})\,|\,L)$$

$$n \longmapsto h_n, \text{ con } h_n\,(\sqrt[p]{\gamma}) = \zeta_p^{\,n}\ \sqrt[p]{\gamma}\ .$$

Sea $s \in \mathrm{Gal}(L|K)$. Una antiimagen u_s de s en $\mathrm{Gal}(L(\sqrt[p]{\gamma})\,|K)$ queda determinada por $u_s\ (\sqrt[p]{\gamma})$.. Tenemos:

$$[u_s\ (\sqrt[p]{\gamma})\ ]^p = \gamma^s = b_s^{\,p}\ \gamma\ .$$

Elegimos un sistema de representantes u_s de G en Gal $L(\sqrt[p]{\gamma})\,|K)$ poniendo

$$u_s\ (\sqrt[p]{\gamma}) = b_s\ \sqrt[p]{\gamma}\ .$$

Calculemos el 2-cociclo asociado a la extensión a partir de este sistema de representantes. Para s,t de G tenemos:

$$u_s(u_t\ (\sqrt[p]{\gamma})) = u_s(b_t\ \sqrt[p]{\gamma}) = b_t^{\,s}\ b_s\ \sqrt[p]{\gamma}$$

$$u_{st}\ (\sqrt[p]{\gamma}) = b_{st}\ \sqrt[p]{\gamma}\ .$$

Por tanto el 2-cociclo $a_{s,t}$ de G en $\mathbb{Z}/p\,\mathbb{Z}$ viene dado por la relación

$$\frac{b_s\ \ b_t^{\,s}}{b_{st}} = \zeta_p^{\,a_{s,t}}\ .$$

$L(\sqrt[p]{\gamma})\,|\,K$ es pues solución al problema de inmersión si y sólo si se verifica esta relación para un cocido $a_{s,t}$ asociado a la extensión $1 \longrightarrow \mathbb{Z}/p\,\mathbb{Z} \longrightarrow E \longrightarrow G \longrightarrow 1$. #

Con la proposición anterior, hemos obtenido que, para que el problema de inmersión sea resoluble, es condición necesaria

que existan elementos b_s de L^* , para s de G, que verifiquen la relación

$$\frac{b_s \quad b_t^{\,s}}{b_{st}} = \zeta_p^{\,a_{s,t}}$$

Veamos que también es condición suficiente .

Proposición 2.12. Dados elementos b_s de L^*, para cada s de G, verificando la relación:

$$\frac{b_s \quad b_t^{\,s}}{b_{st}} = \zeta_p^{\,a_{s,t}}$$

para cada par de elementos s,t de G, y con $a_{s,t}$ cociclo asociado a la extensión $1 \longrightarrow \mathbb{Z}/p\,\mathbb{Z} \longrightarrow E \longrightarrow G \longrightarrow 1$, existe un elemento γ de L^* verificando $\gamma^s = b_s^{\,p}\,\gamma$, para cada s de G, es decir, tal que $L(\sqrt[p]{\gamma})\,|K$ es solución al problema de inmersión dado por:

$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & & \downarrow & & \\ 1 & \longrightarrow & \mathbb{Z}/p\,\mathbb{Z} & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \end{array} .$$

Demostración. Sea $\gamma = \sum_{s\in G} b_s^{-p}\, x^s$, con x cualquier elemento de L^*. Para cada s de G se verifica.

$$\gamma^s = \Big(\sum_{t\in G} b_t^{-p}\, x^t\Big)^s = \sum_{t\in G} (b_t^{\,s})^{-p}\, x^{st} = \sum_{t\in G} \left(\frac{\zeta_p^{\,a_{s,t}}\, b_{st}}{b_s}\right)^{-p} x^{st} =$$

$$= b_s^{\,p} \sum_{t\in G} b_{st}^{-p}\, x^{st} = b_s^{\,p}\,\gamma .$$

Ahora $s \longmapsto b_s^{-p}$ es cociclo, ya que verifica:

$$\frac{b_s^{-p}\,(b_t^{-p})^s}{b_{st}^{-p}} = (\zeta_p^{\,a_{s,t}})^p = 1 .$$

Por el teorema de independencia de automorfismos ([BO_1] §7 nº 5), existe pues un x tal que γ es no nulo. #

Corolario 2.13. Sea

$$i^*: H^2(G, \mathbb{Z}/p\,\mathbb{Z}) \longrightarrow H^2(G, L^*)$$

el morfismo inducido por $i: \mathbb{Z}/p\,\mathbb{Z} \xrightarrow{\sim} \mu_p \hookrightarrow L^*$, donde el isomorfismo de $\mathbb{Z}/p\,\mathbb{Z}$ en μ_p es el prefijado (por estar μ_p contenido en K*, es G-módulo trivial y por tanto, este isomorfismo es de G-módulos).

Entonces el problema de inmersión es resoluble si y sólo si la imagen por i* del elemento ε de $H^2(G, \mathbb{Z}/p\,\mathbb{Z})$ asociado a la extensión es nula.

Demostración. La existencia de elementos b_s de L* tales que $\frac{b_s\, b_t^{\,s}}{b_{st}} = \zeta_p^{\,a_{s,t}}$ equivale a que $(s,t) \longmapsto \zeta_p^{\,a_{s,t}}$ sea coborde de G en L* y $(s,t) \longmapsto \zeta_p^{\,a_{s,t}}$ es cociclo representando $i^*(\varepsilon)$. #

La condición $i^*(\varepsilon) = 0$ puede expresarse también en términos del álgebra producto cruzado. Recordamos a continuación su definición.

Sea K un cuerpo, L|K una extensión de Galois de K con grupo G. Sea

$$1 \longrightarrow L^* \longrightarrow E \longrightarrow G \longrightarrow 1$$

una extensión de L^* por G, de manera que G opere sobre L^* como grupo de Galois de $L|K$.

Consideramos $\mathbb{Z}(E)$, $\mathbb{Z}$-álgebra libre generada por E. Todo elemento de $\mathbb{Z}(E)$ puede escribirse de manera única en la forma:

$$\sum_{e \in E} n_e X_e \quad , \quad n_e \in \mathbb{Z} \ .$$

Sea I el ideal bilátero de $\mathbb{Z}(E)$ generado por

$$X_\lambda + X_\mu - X_{\lambda+\mu} \qquad \text{para } \lambda,\ \mu,\ \lambda+\mu \in L^*$$

$$X_\lambda + X_{-\lambda} \qquad \lambda \in L^* \ .$$

El anillo cociente $A = \mathbb{Z}(E)/I$ contiene L y es una K-álgebra simple central tal que $[A:K] = [L:K]^2$. Estas dos condiciones implican que $A \underset{K}{\otimes} L$ es álgebra de matrices sobre L([S_1]th 10). A se llama *álgebra producto cruzado* de $L|K$ por E.

Sea ahora u_s un sistema de representantes de G en E. Todo elemento de E se escribe en la forma λu_s, con $\lambda \in L^*$, $s \in G$. Podemos escribir cada elemento del álgebra producto cruzado en la forma.

$$\sum_{s \in G} \lambda_s \ u_s, \text{ con } \lambda_s \in L$$

y definir el producto por la regla:

$$(\lambda u_s).(\mu u_t) = \lambda \mu^s \ a_{s,t} \ u_{st} \ ,$$

si $a_{s,t}$ es el 2-cociclo de G en L^* determinado por el sistema de representantes u_s.

Si ε es el elemento de $H^2(G, \mathbb{Z}/p\mathbb{Z})$ asociado a la extensión del problema de inmersión planteado, podemos construir el álgebra producto cruzado asociada a la extensión, dada por el elemento $i^*(\varepsilon)$ de $H^2(G, L^*)$ mediante el 2-cociclo de G en L^*:

$$(s,t) \longmapsto \zeta_p^{a_{s,t}} .$$

Por los resultados de ([S_2] X §5) y ([S_1] §12) tenemos:

Proposición 2.14. Sea L|K una extensión de Galois con grupo G. El conjunto $A_{L|K}$ de clases de equivalencia de K-álgebras simples centrales A, tales que $A \otimes_K L$ es álgebra de matrices sobre L, está en correspondencia 1-1 con el grupo de cohomología $H^2(G, L^*)$. Para un elemento ε de $H^2(G, L^*)$, un representante de la clase de $A_{L|K}$ correspondiente es el álgebra producto cruzado, asociada a la extensión de L^* por G dada por ε. #

Corolario 2.15. El problema de inmersión dado por el elemento ε de $H^2(G, \mathbb{Z}/p\mathbb{Z})$ tiene solución si y sólo si el álgebra producto cruzado asociada a ε es isomorfa a un álgebra de matrices sobre K.

Demostración. La clase nula de $A_{L|K}$ es la de las álgebras de matrices sobre K y por las proposiciones 2.13 y 2.14 el problema de inmersión es resoluble si y sólo si la clase en $A_{L|K}$ del álgebra producto cruzado es la nula.#

Observación. Si $\bar{K}$ es una clausura algebraica de K y G_K es el grupo de galois de $\bar{K}$ sobre K, el grupo $H^2(G_K, \bar{K}^*)$ se obtiene como límite de los $H^2(G, L^*)$, con L recorriendo las extensiones de Galois finitas de K. Por otra parte, para toda K-álgebra simple central A, existe una extensión de Galois finita L de K, tal que $A \underset{K}{\otimes} L$ es álgebra de matrices ([S_2] X §5 prop 7). Por tanto el grupo A_K de clases de equivalencia de K-álgebras simples centrales es reunión de los $A_{L|K}$, para L recorriendo las extensiones de Galois finitas de K. Pasando al límite, se obtiene así el isomorfismo

$$A_K \xrightarrow{\sim} H^2(G_K, \bar{K}^*)$$

que conecta las dos definiciones del grupo de Brauer de K.

Proposición 2.16. El morfismo

$$j^*: H^2(G_K, \mathbb{Z}/p\,\mathbb{Z}) \longrightarrow H^2(G_K, \bar{K}^*),$$

inducido por $j: \mathbb{Z}/p\,\mathbb{Z} \simeq \mu_p \hookrightarrow \bar{K}^*$, es inyectivo y, identificando $H^2(G_K, \mathbb{Z}/p\,\mathbb{Z})$ con su imagen por j^*, se obtiene que $i^*(\varepsilon)$ e inf (ε) coinciden en $H^2(G_K, \bar{K}^*)$, para todo ε de $H^2(G, \mathbb{Z}/p\,\mathbb{Z})$.

Demostración. La sucesión exacta de cohomologia asociada a:

$$1 \longrightarrow \mu_p \longrightarrow \bar{K}^* \longrightarrow \bar{K}^* \longrightarrow 1$$

es:

$$0 = H^1(G_K, \bar{K}^*) \longrightarrow H^2(G_K, \mu_p) \simeq H^2(G_K, \mathbb{Z}/p\,\mathbb{Z}) \xrightarrow{j^*} H^2(G_K, \bar{K}^*),$$

por tanto j^* es inyectiva.

El diagrama:

$$\begin{array}{ccc} H^2(G,\ \mathbb{Z}/p\ \mathbb{Z}) & \xrightarrow{i^*} & H^2(G,\ L^*) \\ \inf \downarrow & & \downarrow \\ H^2(G_K,\ \mathbb{Z}/p\ \mathbb{Z}) & \xrightarrow{j^*} & H^2(G_K,\ \bar{K}^*) \end{array} ,$$

donde la flecha vertical de la derecha es la inclusión de $H^2(G,\ L^*)$ en $H^2(G_K,\ \bar{K}^*)$ ([S_2] X §4 cor.), conmuta. Por tanto, la imagen de inf ε por j^* coincide con $i^*\varepsilon$ en $H^2(G_K,\ \bar{K}^*)$. #

Mediante la proposición 2.16 puede darse una demostración alternativa del corolario 2.13. Sabemos que la resolubilidad del problema de inmersión sobre K dado por la sucesión exacta asociada al elemento ε de $H^2(G,\ \mathbb{Z}/p\ \mathbb{Z})$ equivale a inf $\varepsilon = 0$ en $H^2(G_K,\ \mathbb{Z}/p\ \mathbb{Z})$ (prop. 1.16). Por 2.16, tenemos inf $\varepsilon = 0$ equivalente a $i^*\varepsilon = j^*$ (inf ε) $= 0$ en $H^2(G_K,\ \bar{K}^*)$ y equivalente a $i^*\varepsilon = 0$ en $H^2(G,\ L^*)$.

§3. PROBLEMAS DE INMERSION CON NUCLEO $\mathbb{Z}/2\ \mathbb{Z}$: LA FORMULA DE SERRE

Para ciertas extensiones con núcleo $\mathbb{Z}/2\ \mathbb{Z}$, la obstrucción al problema de inmersión puede expresarse mediante la fórmula de Serre ([S_3]), que recordamos a continuación.

Sea K un cuerpo de característica distinta de 2. Sea F un cuerpo extensión separable de K de grado n. La forma cuadrática traza de la extensión $F|K$, Q_K, definida por:

$$Q_F(x) = Tr_{F|K}(x^2),$$

da a F estructura de espacio cuadrático. El discriminante d_F del espacio cuadrático F coincide con el discriminante de la extensión $F|K$ en K^*/K^{*2}. Sea $w(Q_F)$ el invariante de Hasse-Witt de Q_F. Si, en una base de F sobre K, Q_F toma forma diagonal $(a_1, a_2, \ldots, a_n)$, $w(Q_F)$ es la clase del elemento $\prod_{i<j} (a_i, a_j)$ del grupo de Brauer de K. Por ser $w(Q_F)$ la clase de un álgebra de cuaterniones, es un elemento de la 2-componente $H^2(G_K, \mathbb{Z}/2\mathbb{Z})$ del grupo de Brauer $H^2(G_K, \bar{K}^*)$ de K.

Sea $\bar{K}$ una clausura algebraica separable de K. Sea ϕ el conjunto de K-morfismos de F en $\bar{K}$. Se tiene card $\phi = n$ y G_K opera sobre ϕ. Sea

$$e: G_K \longrightarrow S_n$$

el morfismo obtenido identificando ϕ con $\{1, 2, \ldots, n\}$. La imagen G de e es un grupo isomorfo al grupo de Galois sobre K de la clausura galoisiana L de F. Cuando $F = K[X]/(f)$, con f polinomio separable de grado n, G es el grupo de Galois de f, entendido como grupo de permutaciones de las raíces de f. A partir de ahora, identificamos G con $Gal(L|K)$ y consideramos un elemento s de G tanto automorfismo de L sobre K como permutación de S_n.

Consideramos la extensión central de S_n, con $n \geq 4$,

$$1 \longrightarrow \mathbb{Z}/2\,\mathbb{Z} \longrightarrow \tilde{S}_n \longrightarrow S_n \longrightarrow 1.$$

caracterizada por la propiedad (P) siguiente:

(P): Todo elemento de $\tilde{S}_n$ cuya imagen en S_n es una trasposición (resp. un producto de dos trasposiciones con soportes disjuntos) es de orden 2 (resp. de orden 4).

Sea s_n el elemento de $H^2(S_n, \mathbb{Z}/2\,\mathbb{Z})$ correspondiente a la extensión. Sea $\tilde{G}$ la antiimagen de G en $\tilde{S}_n$. Serre obtiene el resultado siguiente:

Proposición 2.17. ([S_3] th 1). Sea ε el elemento de $H^2(G, \mathbb{Z}/2\,\mathbb{Z})$ asociado a la extensión

$$1 \longrightarrow \mathbb{Z}/2\,\mathbb{Z} \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1,$$

es decir la imagen de s_n en $H^2(G, \mathbb{Z}/2\,\mathbb{Z})$ por el morfismo de restricción:

$$\text{res}: H^2(S_n, \mathbb{Z}/2\,\mathbb{Z}) \longrightarrow H^2(G, \mathbb{Z}/2\,\mathbb{Z}).$$

En $H^2(G_K, \mathbb{Z}/2\,\mathbb{Z})$ se verifica la igualdad:

$$\inf \varepsilon = w(Q_F)\ \mathbb{Q}(2, d_F)$$

donde $(2, d_F)$ es la clase del álgebra de cuaterniones con generadores i, j, tales que $i^2 = 2$, $j^2 = d_F$, $ij = -ji$.#

Veamos ahora que la forma cuadrática traza Q_F es equivalente a la identidad sobre L, es decir, que la forma $Q_F{}^L$, obtenida a partir de Q_F ampliando escalares a L, es equivalente a la forma cuadrática identidad de L^n.

Sea H el subgrupo de G formado por los automorfismos de L

que dejan fijo F. Tenemos $[G:H] = n$. Sea $\phi = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ el conjunto de K-morfismos de F en $\bar{K}$. Identificamos F con $\varphi_1(F)$ y elegimos un sistema de representantes $S = \{s_1, s_2, \ldots, s_n\}$ de G módulo H de manera que:

$$F^{s_i} = \varphi_i(F) \quad , \qquad i = 1, 2, \ldots, n.$$

Sea $(x_1, x_2, \ldots, x_n)$ una base de F sobre K. Si $F = K[X]/(f)$, con f polinomio separable, se tiene $F = K(\Theta)$, para una raiz Θ de f y puede tomarse la base $(1, \Theta, \ldots, \Theta^{n-1})$ de F sobre K. Consideramos la matriz M de $M_n(L)$:

$$M = \begin{bmatrix} x_1^{s_1} & x_2^{s_1} & \ldots & x_n^{s_1} \\ x_1^{s_2} & x_2^{s_2} & \ldots & x_n^{s_2} \\ & \ldots\ldots & & \\ x_1^{s_n} & x_2^{s_n} & \ldots & x_n^{s_n} \end{bmatrix}$$

La matriz M^tM es la matriz de Q_F en la base $(x_1, x_2, \ldots, x_n)$ ya que su elemento (ij) es:

$$\sum_{k=1}^{n} x_i^{s_k} x_j^{s_k} = Tr_{F|K}(x_i x_j).$$

Q_F es pues isomorfa a la identidad sobre L, y el isomorfismo $f: L^n \longrightarrow F \otimes_K L$ de matriz M^{-1} en las bases $(e_1, e_2, \ldots e_n)$, base canónica, de L^n y $(x_1, x_2, \ldots, x_n)$ de $F \otimes_K L$ verifica $Q_F^L(f(x)) = Q_I^L(x)$, donde Q_I^L indica la forma cuadrática identidad de L^n.

Para un isomorfismo f entre L-espacios vectoriales y un

elemento s de G, se define $f^s = s\ f\ s^{-1}$. Si f tiene matriz M, la matriz de f^s en las mismas bases es la matriz M^s obtenida aplicando s a todos los elementos de M.

Sea $\mathcal{C}(L|K)$ el conjunto de clases de equivalencia sobre K de las formas cuadráticas que son equivalentes sobre L a la forma cuadrática identidad Q_I^L. Sea $O(Q_I^L)$ el grupo de transformaciones ortogonales de L^n respecto de Q_I^L. Por el isomorfismo:

$$\mathcal{C}(L|K) \xrightarrow{\sim} H^1(G,\ O(Q_I^L)),$$

a Q_F le corresponde la clase del cociclo $s \longmapsto f^{-1}\ f^s$. ([$S_2$] X §2). Calculemos este cociclo.

Para $s \in G$, la matriz M^s es:

$$M^s = \begin{bmatrix} x_1^{ss_1} & x_2^{ss_1} & \dots & x_n^{ss_1} \\ x_1^{ss_2} & x_2^{ss_2} & \dots & x_n^{ss_2} \\ & \dots\dots & & \\ x_1^{ss_n} & x_2^{ss_n} & \dots & x_n^{ss_n} \end{bmatrix}$$

El elemento $x_j^{ss_i}$ es $x_j^{s_i'}$ si i' es tal que $\varphi_{i'} = \varphi_i^s$, es decir i' = s(i) considerando s elemento de S_n. Entonces, M^s es la matriz obtenida permutando las filas de M de manera que la fila i de M^s es la fila s(i) de M.

Consideramos la matriz $A_s \in M_n(L)$ definida por:

$$a_{s(j),j} = 1 \quad ; \quad a_{ij} = 0 \quad \text{si} \quad i \neq s(j).$$

Al multiplicar cualquier matriz por A_s a la izquierda se produce la permutación de filas contraria a la del paso de M a M^s, por tanto se tiene $A_s\ M^s = M$, o equivalentemente:

$$M\, M^{-s} = A_s\ .$$

El 1-cociclo de G en $O(Q_I^{\,L})$ asociado a Q_F es pues $s \longmapsto p_s$ con p_s transformación ortogonal de matriz A_s en la base canónica $(e_1, e_2, \ldots, e_n)$ de L^n, es decir definido por

$$p_s(e_i) = e_{s(i)} \quad , \quad i = 1, \ldots n\ .$$

Consideramos la inyección $S_n \xhookrightarrow{\text{iny}} O(Q_I^{\,L})$ definida por $e_i \longmapsto e_{\sigma(i)}$ para $\sigma \in S_n$. Entonces la composición:

$$G \hookrightarrow S_n \xrightarrow{\text{iny}} O(Q_I^{\,L})$$

es el cociclo p_s. En el lenguaje de ([S_4] I 5.3), Q_F es la forma cuadrática obtenida de Q_I por torsión galoisiana mediante el 1-cociclo p_s: $G \longrightarrow O(Q_I^{\,L})$.

En el caso en que d_F sea igual a 1, la imagen de e: $G_K \longrightarrow S_n$ está contenida en el alternado A_n. La restricción de s_n a A_n es el elemento a_n de $H^2(A_n, \mathbb{Z}/2\,\mathbb{Z})$ correspondiente a la extensión central de A_n que escribimos en la forma:

$$1 \longrightarrow \mathbb{Z}/2\,\mathbb{Z} \longrightarrow \tilde{A}_n \longrightarrow A_n \longrightarrow 1\ .$$

En este caso la fórmula de Serre se reduce a:

$$\inf \varepsilon = w(Q_F) \quad \text{en } H^2(G_K, \mathbb{Z}/2\,\mathbb{Z})\ .$$

Al ser $Q_F^{\,L}$ isomorfa a la identidad, su invariante de Hasse-Witt es trivial. Tenemos pues:

$$1 = w(Q_F^{\,L}) = w(Q_F) \underset{K}{\otimes} L,$$

es decir, $w(Q_F)$ está en el subgrupo $H^2(G, L^*)$ del grupo de Bra-

uer de K, correspondiente a las álgebras escindidas por L. De aquí puede deducirse el siguiente resultado.

Proposición 2.18. Sea G la imagen de $e: G_K \longrightarrow A_n$. Sea ε la imagen de a_n por el morfismo de restricción de $H^2(A_n, \mathbb{Z}/2\mathbb{Z})$ en $H^2(G, \mathbb{Z}/2\mathbb{Z})$. Sea

$$i^* : H^2(G, \mathbb{Z}/2\mathbb{Z}) \longrightarrow H^2(G, L^*)$$

el morfismo inducido por $i: \mathbb{Z}/2\mathbb{Z} \simeq \mu_2 \hookrightarrow L^*$. Se verifica:

$$i^*(\varepsilon) = w(Q_F) \quad \text{en } H^2(G, L^*).$$

Demostración. Por 2.16, tenemos que inf ε coincide con $i^*\varepsilon$ en $H^2(G_K, \bar{K}^*)$. Entonces la fórmula de Serre da:

$$i^*(\varepsilon) = w(Q_F) \quad \text{en } H^2(G_K, \bar{K}^*),$$

y por ser ambos elementos de $H^2(G, L^*)$, se tiene la igualdad en $H^2(G, L^*)$. #

CAPITULO III

CONSTRUCCION EXPLICITA DE SOLUCIONES

Sea K un cuerpo de característica distinta de 2. El objetivo de este capítulo es construir explícitamente las soluciones de un problema de inmersión dado por:

$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & & \downarrow e & & \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \tilde{G} & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

donde G es un subgrupo del grupo alternado A_n y $\tilde{G}$ es la antiimagen de G en $\tilde{A}_n$, doble recubrimiento de A_n, con $n \geq 4$. Sea $L|K$ la extensión de Galois correspondiente al epimorfismo e . En el caso en que el problema sea resoluble, sabemos que si $L(\sqrt{\gamma})$ es un cuerpo solución, la solución general es $L(\sqrt{r\gamma})$ con r recorriendo K^*/K^{*2} (cf. 2.2).

Obtenemos una solución γ como coordenada de la norma espinorial de un elemento adecuado del álgebra de Clifford de la forma cuadrática traza Q_F de $F|K$, subextensión separable de grado n de $L|K$ (teorema 3.15). Mediante la fórmula de Serre (cf 2.17), sabemos que la resolubilidad del problema equivale, en este caso, a que el invariante de Hasse-Witt de Q_F sea trivial. Para ha

llar la solución, utilizaremos la construcción del doble recubrimiento $\tilde{A}_n$ de A_n, mediante el grupo de Clifford reducido de la forma cuadrática identidad Q_I, dada por Schur. Usaremos asimismo las relaciones entre las álgebras de Clifford de Q_F y Q_I, que obtendremos previamente.

En el caso en que Q_F es equivalente sobre K a Q_I o, más generalmente, a una forma cuadrática del tipo:

$$Q_q = -(X_1^2 + X_2^2 + \ldots + X_q^2) + X_{q+1}^2 + \ldots + X_n^2 ,$$

damos explícitamente la solución en función de un cambio de base que pase de Q_F a Q_q, o en su caso a Q_I (teoremas 3.17 y 3.24).

§1. EXTENSIONES ESPINORIALES. ESTUDIO DEL PROBLEMA

Dada una forma cuadrática Q sobre un K-espacio vectorial V de dimensión n, se define su *álgebra de Clifford* C(Q) como el cociente del álgebra tensorial de V por el ideal bilátero generado por los elementos $x \otimes x - Q(x)$, con x recorriendo V. C(Q) es una K-álgebra simple central graduada. Indicamos por $C^+(Q)$ la imagen en el cociente de $\bigoplus_{i \text{ par}} T^i(V)$, por $C^-(Q)$ la de $\bigoplus_{i \text{ impar}} T^i(V)$. Se llaman elementos pares de C(Q) a los elementos de $C^+(Q)$, impares a los de $C^-(Q)$. Identificamos el espacio vectorial V con su imagen en C(Q). Si $(e_1, e_2, \ldots, e_n)$ es una base ortogonal de V (respecto de Q) tal que $Q(e_i) = a_i$, $i = 1, \ldots, n$, C(Q) es la K-álgebra generada por $e_1, e_2, \ldots, e_n$ con las relaciones:

$e_i^2 = a_i$, $1 \leq i \leq n$; $e_i e_j = -e_j e_i$, $1 \leq i \neq j \leq n$.

Los elementos $e_1^{\varepsilon_1} e_2^{\varepsilon_2} \ldots e_n^{\varepsilon_n}$, con $\varepsilon_i = 0,1$, forman una base de $C(Q)$ como K-espacio vectorial. La dimensión de $C(Q)$ sobre K es pues 2^n.

Si L es un cuerpo extensión de K y Q^L es la forma cuadrática obtenida a partir de Q ampliando escalares a L, el álgebra de Clifford de Q^L coincide con $C(Q) \underset{K}{\otimes} L$ y la indicaremos por $C_L(Q)$. Identificamos $C(Q)$ con su imagen en $C_L(Q)$ por $x \longmapsto x \otimes 1$. Si L es extensión de Galois de K, con grupo de Galois G, podemos definir una acción de G sobre $C_L(Q) = C(Q) \underset{K}{\otimes} L$, haciendo operar G sobre el segundo factor. La parte fija de $C_L(Q)$ por la acción de G es $C(Q)$ y la acción de G restringe a $C_L^+(Q)$, y a $C_L^-(Q)$.

Si Q, Q' son formas cuadráticas equivalentes sobre K, definidas sobre los espacios vectoriales V, V' respectivamente, un isomorfismo f de V en V' tal que

$$Q'(f(x)) = Q(x) \text{ , para todo } x \text{ de } V,$$

se extiende a un isomorfismo de $C(Q)$ en $C(Q')$. En efecto, para $x \in V$, tendremos: $f(x)^2 = Q'(f(x)) = Q(x) = x^2$.

Sea β: $C(Q) \longrightarrow C(Q)$ el *antiautomorfismo principal* de $C(Q)$, es decir el único antiautomorfismo de $C(Q)$ que deja fijo V. Si $v_1, v_2, \ldots, v_k$ son vectores de V, tenemos:

$$\beta(v_1 v_2 \ldots v_k) = v_k v_{k-1} \ldots v_2 v_1 .$$

Definimos la *norma espinorial* $N(x)$ de un elemento x de $C(Q)$ por:

$$N(x) = \beta(x).x$$

Se llama *grupo de Clifford especial* de Q, $G^+(Q)$, al grupo multiplicativo de los elementos invertibles x de $C^+(Q)$ tales que $x\ V\ x^{-1} = V$.

Para un elemento x de $G^+(Q)$ su norma espinorial N(x) es un elemento de K* y la aplicación:

$$N:\ x \longmapsto N(x)$$

es un morfismo de $G^+(Q)$ en K*. Se llama *grupo de Clifford reducido*, $G_o^+(Q)$, al núcleo del morfismo N.

Proposición 3.1. Sea SO(Q) el grupo de las rotaciones del espacio cuadrático V. Para $x \in G_o^+(Q)$, $v \in V$, definimos $\varphi(x)(v) = x\ v\ x^{-1}$. Entonces φ es un morfismo de $G_o^+(Q)$ en SO(Q) y la sucesión

$$1 \longrightarrow \{\pm 1\} \longrightarrow G_o(Q) \longrightarrow SO(Q)$$

es exacta.

Demostración. Por ([BO_2] §9 nº 5 th.4), φ es morfismo de $G_o^+(Q)$ en SO(Q) y su núcleo está contenido en el centro de C(Q). Un elemento par del centro de C(Q) es del cuerpo K([0] 54:4) y los elementos de K con norma espinorial 1 son ± 1.#

Proposición 3.2. ([S_3] 2.3.lema 1). Sea Q_I la forma cuadrática identidad sobre K^n, con $n \geq 4$. Consideramos A_n incluido en SO(Q) mediante $s \longmapsto p_s$, con $p_s(e_i) = e_{s(i)}$ para $(e_1, e_2, \ldots, e_n)$ base canónica de K^n. Entonces A_n está incluido en la imagen de $\varphi: G_o^+(Q_I) \longrightarrow SO(Q_I)$. Para el elemento (ij)(kl) de A_n, pro-

ducto de las trasposiciones (ij) y (kl), una antiimagen en $G_o(Q)$ es el elemento $\frac{1}{2}(e_i - e_j)(e_k - e_l)$, de orden 4 si i, j, k, l son distintos. Por tanto $\varphi^{-1}(\tilde{A}_n)$ es isomorfo a $\tilde{A}_n$.#

De la construcción de la sucesión exacta:

$$1 \longrightarrow \{\pm 1\} \longrightarrow \tilde{A}_n \longrightarrow A_n \longrightarrow 1,$$

dada por la proposición anterior, se deduce que para G. imagen de e: $G_K \longrightarrow A_n$, podemos considerar $\tilde{G}$ antiimagen de G en $\tilde{A}_n$ como subgrupo de $G_o^+(Q_I)$. Si u_s es un sistema de representantes de G en $\tilde{G}$, los u_s son elementos de $C(Q_I)$ verificando

$$u_s\, e_i\, u_s^{-1} = u_{s(i)} \quad , \quad i = 1, \ldots, n \ ,$$

siendo $(e_1, e_2, \ldots, e_n)$ la base canónica de K^n. Además cada u_s es producto de un número par de factores del tipo $(e_i - e_j)$, y factores $\frac{1}{2}$, por la proposición anterior. De ahora en adelante, consideramos fijado un sistema de representantes u_s, con $u_1 = 1$. Sea $a_{s,t}$ el 2-cóciclo de G en $\{\pm 1\}$ que determina, es decir:

$$a_{s,t} = u_s\, u_t\, u_{st}^{-1} \quad , \quad s, t \in G.$$

Designamos por ε la clase de $a_{s,t}$ en $H^2(G, \{\pm 1\})$.

El grupo de Clifford reducido $G_o^+(Q_I)$ de la forma cuadrática identidad se identifica con el grupo de los espinores, $Spin_n(K)$. Para un subgrupo G del alternado A_n, con $n \geq 4$, si $\tilde{G}$ es su antiimagen en $\tilde{A}_n$, por la proposición 3.2, es conmutativo el diagrama:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \tilde{G} & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & Spin_n(K) & \longrightarrow & SO_{n(K)} & & \end{array}$$

Adoptamos la definición siguiente.

Para un subgrupo G del grupo alternado A_n, con $n \geq 4$, llamaremos *extensión espinorial de* G a la sucesión exacta

$$1 \longrightarrow \{\pm 1\} \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1,$$

donde $\tilde{G}$ es la antiimagen de G en la extensión central $\tilde{A}_n$ de A_n es decir el grupo que hace conmutativo el diagrama anterior.

Consideramos un problema de inmersión dado por una extensión espinorial, sobre un cuerpo K de característica distinta de 2, es decir, dado por un diagrama del tipo:

$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & & \downarrow & e & \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \tilde{G} & \longrightarrow & G & \longrightarrow & 1 \end{array} .$$

Suponemos el problema resoluble, es decir que si ε es el elemento de $H^2(G, \{\pm 1\})$ asociado a la extensión espinorial de G, se verifica $\inf \varepsilon = 0$ en $H^2(G, \{\pm 1\})$ o, equivalentemente, $i^* \varepsilon = 0$ en $H^2(G, L^*)$, siendo $L|K$ la extensión de Galois con grupo G asociada al morfismo $e: G_K \longrightarrow G$ (cf 1.16 y 2.13).

Si $L(\sqrt{\gamma})$ es un cuerpo solución, sabemos, por 2.2, que la solución general será $L(\sqrt{r\gamma})$, con r recorriendo K^*/K^{*2}. Además, por 2.10, si la extensión espinorial de G no es escindida, todas las soluciones son propias. En este caso, $L(\sqrt{r\gamma})$, con r recorriendo K^*/K^{*2}, da todos los cuerpos solución.

En el caso en que K sea un cuerpo de números, sea S el conjunto de primos de Θ_K, anillo de enteros de K, en que ramifica la extensión L|K. Si el número de clases de ideales de Θ_K es impar, sabemos por 1.21, que existe una solución al problema de inmersión no ramificada fuera de $S \cup \{\mathfrak{p} \in \text{Spec } \Theta_K / \mathfrak{p} | 2\}$.

Nos proponemos calcular explícitamente una solución al problema de inmersión considerado. Por 2.11, debemos hallar un elemento γ de L , tal que:

$$\gamma^s = b_s^2 \quad \gamma, \text{ para todo } s \text{ de } G$$

y con b_s de L verificando:

$$b_s \; b_t^s \; b_{st}^{-1} = a_{s,t}$$

donde $a_{s,t}$ es el 2-cociclo de G en $\{\pm 1\}$, determinado por el sistema de representantes u_s de G en $\tilde{G}$, fijado anteriormente. Hallaremos el elemento γ mediante el álgebra de Clifford $C_L(Q_F) = C(Q_F) \underset{K}{\otimes} L$.

Proposición 3.3. El isomorfismo $f: L^n \longrightarrow F \underset{K}{\otimes} L$, con matriz M^{-1} en las bases $(e_1, e_2, \ldots, e_n)$, base canónica, de L^n y $(x_1, x_2, \ldots, x_n)$ de $F \underset{K}{\otimes} L$, introducido en II §3, donde teníamos

$$M = (x_j^{s_i}) \quad \begin{matrix} 1 \leq i \leq n \\ 1 \leq j \leq n \end{matrix} ,$$

extiende a un isomorfismo de $C_L(Q_I)$ en $C_L(Q_F)$.

Demostración. f cumple $Q_I^L(x) = Q_F^L(f(x))$, para todo x de L^n, por tanto extiende a un isomorfismo entre las álgebras de Clifford.#

Indicaremos también por f el isomorfismo de $C_L(Q_I)$ en $C_L(Q_F)$ dado por la proposición anterior, y definimos:

$$v_i = f(e_i) \quad , \quad i = 1,\ldots, n \ .$$

Veamos ahora que también $C(Q_I)$ y $C(Q_F)$ son isomorfas. Más concretamente se verifica el resultado siguiente.

Proposición 3.4. Si $d_F = 1$, y es resoluble el problema de inmersión dado por:

$$\begin{array}{ccccccccc} & & & & & & & & G_K \\ & & & & & & & & \downarrow \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \tilde{G} & \longrightarrow & G & \longrightarrow & 1 \ , \end{array}$$

entonces existe un isomorfismo $C(Q_F) \longrightarrow C(Q_I)$, que transforma $C^+(Q_F)$ en $C^+(Q_I)$ y $C^-(Q_F)$ en $C^-(Q_I)$.

Para la demostración, usaremos el siguiente lema:

Lema 3.5. Sea $C_L^+(Q_I)^*$ el grupo multiplicativo de $C_L^+(Q_I)$. Es un G-módulo y se verifica:

$$H^1(G,\ C_L^+(Q_I)^*) = 0 \ .$$

Demostración. Supongamos primero K infinito. Sea a_s un 1-cociclo de G en $C_L^+(Q_I)^*$. Sea c un elemento cualquiera de $C_L^+(Q_I)^*$. Formamos el elemento

$$b = \sum_{s \in G} a_s \cdot c^s$$

b verifica $b^s = a_s^{-1}\, b$, por tanto, si b es invertible, se tiene $a_s = b^{-s}\, b$, es decir $s \longmapsto a_s$ es coborde. Ahora, por el teorema de independencia algebraica de automorfismos ([BO_1] §10 th 4), puede tomarse c de manera que b sea invertible.

Sea ahora K finito, entonces el grupo de Brauer de K es nulo ([S_2] X §7), es decir, toda K-álgebra simple central es álgebra de matrices sobre K.

Si $n = [F:K]$ es impar, $C_L^+(Q_I)$ es K-álgebra simple central ([LA] V 2.4), por tanto álgebra de matrices y por ([S_2] X prop 3), tenemos $H^1(G, C_L^+(Q_I)^*) = 0$.

Si n es par, y por ser $d_I = 1$, $C_L^+(Q_I)$ es suma directa de 2 K-álgebras simples centrales isomorfas ([LA] V 2.5), por tanto

$$C_L^+(Q_I) \simeq M_{2^{n-2}}(L) \times M_{2^{n-2}}(L),$$

y por ([S_2] X prop. 3), se tiene:

$H^1(G, C_L^+(Q_I)^*) \simeq H^1(G, GL(2^{n-2}, L)) \times H^1(G, GL(2^{n-2}, L)) = 0.\#$

Demostración de 3.4. Sea $f^{-1}: F \underset{K}{\otimes} L \longrightarrow L^n$ el isomorfismo inverso del obtenido en la proposición 3.3. Entonces, se cumple

$$f^{-1} \circ f^s (e_i) = e_{s(i)} \qquad i = 1, \ldots, n$$

(cf cap II §3). Por ser el problema de inmersión resoluble, existen elementos b_s de L^*, tales que

$$\frac{b_s\ b_t^s}{b_{st}} = a_{s,t} \ .$$

Sea u_s el sistema de representantes de G en $\tilde{G}$ fijado anteriormente, sea

$$h_s = b_s^{-1}\ u_s \ .$$

Entonces, $s \longmapsto h_s$ es 1-cociclo de G en $C_L^+(Q_I)^*$ y, por el lema 3.5, es coborde, es decir existe un elemento α de $C_L^+(Q_I)$ tal que

$$h_s = \alpha\ \alpha^{-s} \ .$$

Por tanto tenemos:

$$f^{-1} \circ f^s(e_i) = e_{s(i)} = u_s\ e_i\ u_s^{-1} = h_s\ e_i\ h_s^{-1} = \alpha\alpha^{-s}\ e_i\ \alpha^s\ \alpha^{-1},$$

o equivalentemente

$$f^{-1}\ o\ f^s(x) = \alpha\alpha^{-s}\ x\ \alpha^s\ \alpha^{-1} \ ,$$

para todo x de L^n. Si $y = f^s(x)$, tenemos:

$$\alpha^{-1}\ f^{-1}(y)\ \alpha = \alpha^{-s}\ f^{-s}(y)\ \alpha^s \ .$$

Definimos ahora:

$$\psi(y) = \alpha^{-1}\ f^{-1}(y)\ \alpha \ , \text{ para } y \in F \otimes L \ .$$

Por la igualdad anterior, tenemos $\psi^s = \psi$, para todo s de G. Además se cumple:

$$\psi(y)^2 = \alpha^{-1}\ f^{-1}(y)^2\ \alpha = Q_I(f^{-1}(y)) = Q_F(y) \ ,$$

por tanto, ψ extiende a un morfismo de $C_L(Q_F)$ en $C_L(Q_I)$. Por definición, ψ es composición del isomorfismo f^{-1} y de un auto-

morfismo interior de $C_L(Q_I)$, por tanto es isomorfismo de $C_L(Q_F)$ en $C_L(Q_I)$. Por ser $\psi^s = \psi$, la restricción de ψ a $C(Q_F)$ es un isomorfismo

$$\tilde{\psi} : C(Q_F) \longrightarrow C(Q_I).$$

Además, por ser α un elemento par de $C_L(Q_I)$, $\tilde{\psi}$ transforma $C^+(Q_F)$ en $C^+(Q_I)$ y $C^-(Q_F)$ en $C^-(Q_I)$. #

Observación. La proposición anterior se inspira en un resultado de Springer ([SP] th 4.2). Hemos dado aquí un enunciado relativo a las formas cuadráticas Q_I y Q_F, y en relación al problema de inmersión tal como lo usaremos. Springer define un invariante $a_L(Q, Q_1)$ para dos formas cuadráticas Q y Q_1, definidas sobre un cuerpo K y equivalentes sobre un cuerpo L, extensión de Galois de K. En el caso en que Q sea la forma cuadrática identidad, $a_L(Q, Q_1)$ es el invariante de Hasse-Witt de Q_1, que es elemento de $H^2(G, L^*)$. La hipótesis $a_L(Q, Q_1) = 1$ del teorema de Springer equivale pues por 2.18 a $i^*(\varepsilon) = 0$, es decir a la existencia de los elementos b_s de L^* tales que $b_s\, b_t^s\, b_{st}^{-1} = a_{s,t}$.

Proposición 3.6. El elemento α, definido en la demostración de la proposición anterior, es un elemento invertible de $C_L(Q_I)$, cuya norma espinorial $N(\alpha)$ verifica:

$$N(\alpha)^s = b_s^2\, N(\alpha), \text{ para todo } s \text{ de } G$$

y con $b_s \in L^*$ cumpliendo $b_s\, b_t^s\, b_{st}^{-1} = a_{s,t}$.

Demostración. α cumple $\alpha\alpha^{-s} = b_s^{-1}\, u_s$, por tanto:

$$\beta(\alpha^{-s})\ \beta(\alpha)\ \alpha\ \alpha^{-s} = \beta(\alpha\alpha^{-s})\alpha\alpha^{-s} = b_s^{-2}\ \beta(u_s)\ u_s = b_s^{-2}$$

por ser u_s de $G_o^+(Q_I)$. Tenemos pues:

$$\beta(\alpha).\alpha = b_s^{-2}\ \beta(\alpha^s)\ \alpha^s ,$$

es decir:

$$N(\alpha)^s = b_s^2\ N(\alpha).\#$$

Observación. Si $N(\alpha)$ es un elemento de L^*, entonces $L(\sqrt{N(\alpha)})\,|L$ es solución al problema de inmersión.

Corolario 3.7. Si escribimos el elemento $N(\alpha)$ de la proposición anterior en la base $\{e_1^{\varepsilon_1} e_2^{\varepsilon_2} \dots e_n^{\varepsilon_n}\}_{\varepsilon_i = 0,1}$ de $C_L(Q_I)$, cualquier coordenada λ de $N(\alpha)$ verifica

$$\lambda^s = b_s^{\,2}\ \lambda\ .$$

Por tanto, para λ coordenada no nula de $N(\alpha)$, $L(\sqrt{\lambda})\,|L$ es solución al problema de inmersión.

Demostración. Si $N(\alpha) = \Sigma\ \lambda_{\varepsilon_1 \dots \varepsilon_n}\ e_i^{\varepsilon_1} \dots e_n^{\varepsilon_n}$, tenemos:

$$N(\alpha)^s = \Sigma\ \lambda^s_{\varepsilon_1\varepsilon_2\dots\varepsilon_n}\ e_1^{\varepsilon_1}\ e_2^{\varepsilon_2} \dots e_n^{\varepsilon_n}\ ,$$

por ser e_i de $C(Q_I)$, e igualando coordenadas de $N(\alpha)^s$ y $b_s^2\ N(\alpha)$, se obtiene el resultado.#

Corolario 3.8. Si $f(\alpha)$ es la imagen de α por el isomorfismo f de $C_L(Q_I)$ en $C_L(Q_F)$ y f' es el isomorfismo inverso del isomorfismo $\tilde{\psi}$ obtenido en la proposición 3.4, se verifica:

1) $N(f(\alpha))^s = b_s^2\, N(f(\alpha))$ y $\lambda^s = b_s^2\, \lambda$ para cualquier coordenada λ de $N(f(\alpha))$ en una base de $C(Q_F)$.

2) $f'(e_i) = f(\alpha)\, v_i\, f(\alpha)^{-1}$, $i = 1,2,\ldots, n$.

Demostración. Por ser f isomorfismo entre los espacios vectoriales de $C_L(Q_I)$ y $C_L(Q_F)$, conmuta con los antiautomorfismos principales, por tanto la primera igualdad de 1) se deduce de 3.6. Igual que 3.7, se obtiene la segunda.

Tenemos $\tilde{\psi}(y) = \alpha^{-1}\, f^{-1}(y)\, \alpha$, por definición, por tanto

$$f'(e_i) = f(\alpha\, e_i\, \alpha^{-1}) = f(\alpha)\, v_i\, f(\alpha)^{-1}. \ \#$$

§2 METODO DE RESOLUCION

Obtendremos la solución al problema de inmersión calculando explícitamente un elemento z invertible de $C_L^+(Q_F)$ tal que:

$$e_i \longmapsto z^{-1}\, v_i\, z$$

defina un isomorfismo de $C(Q_I)$ en $C(Q_F)$.

Veamos primero que, a partir del conocimiento explícito de un isomorfismo de $C(Q_I)$ en $C(Q_F)$, que transforme $C^+(Q_I)$ en $C^+(Q_F)$ y $C^-(Q_I)$ en $C^-(Q_F)$, puede calcularse este elemento z.

Lema 3.9. Sean, como antes, f, el isomorfismo de $C_L(Q_I)$ en $C_L(Q_F)$ y $v_i = f(e_i)$, $i = 1, \ldots n$. Sea g un isomorfismo de $C(Q_I)$ en $C(Q_F)$ que transforme $C^+(Q_I)$ en $C^+(Q_F)$ y $C^-(Q_I)$ en $C^-(Q_F)$, y sea $w_i = g(e_i)$, $i = 1,\ldots,n$. Entonces podemos elegir g de manera que el elemento

$$z = \sum_{\varepsilon_1=0,1} v_1^{\varepsilon_1} v_2^{\varepsilon_2} \ldots v_n^{\varepsilon_n} w_n^{\varepsilon_n} \ldots w_2^{\varepsilon_2} w_1^{\varepsilon_1}$$

sea un elemento no nulo de $C_L(Q_F)$.

Demostración. Supongamos que z es igual a 0. Sea $w_1' = - w_1$. Entonces la asignación

$$e_1 \longmapsto w_1' \quad ; \quad e_i \longmapsto w_i \qquad i = 2,\ldots n$$

define un isomorfismo de $C(Q_I)$ en $C(Q_F)$ que transforma $C^+(Q_I)$ en $C^+(Q_F)$ y $C^-(Q_I)$ en $C^-(Q_F)$. Formamos el elemento:

$$z' = \sum_{\varepsilon_i=0,1} v_1^{\varepsilon_1} v_2^{\varepsilon_2} \ldots v_n^{\varepsilon_n} w_n^{\varepsilon_n} \ldots w_2^{\varepsilon_2} w_1^{\varepsilon_1}$$

Entonces se cumple:

$$z - z' = 2\, v_1 \Big(\sum_{\varepsilon_i=0,1} v_2^{\varepsilon_2} \ldots v_n^{\varepsilon_n} w_n^{\varepsilon_n} \ldots w_2^{\varepsilon_2} \Big) w_1 .$$

Si z' es también nulo, por ser v_1 y w_1 invertibles, tenemos:

$$\sum_{\varepsilon_i=0,1} v_2^{\varepsilon_2} \ldots v_n^{\varepsilon_n} w_n^{\varepsilon_n} \ldots w_2^{\varepsilon_2} = 0 .$$

Podemos pues sustituir w_2 por $w_2' = -w_2$ y reiterar el proceso. Llegaríamos a $v_n \cdot w_n = 0$, imposible ya que v_n y w_n son ambos invertibles.

Por tanto, sustituyendo por sus opuestos los elementos w_i que sea necesario, obtenemos un isomorfismo g tal que z es no nulo. #

Observación. z es un elemento par de $C_L(Q_F)$ ya que cada uno de sus sumandos es producto de un número par de elementos impares. (Cada v_i es impar por ser de $L \otimes F$, y cada $w_i = g(e_i)$ lo es ya que g transforma $C^-(Q_I)$ en $C^-(Q_F)$).

Proposición 3.10. Sean f, g, v_i, w_i como en el lema anterior y g elegido de manera que el elemento

$$z = \sum_{\varepsilon_i=0,1} v_1^{\varepsilon_1} v_2^{\varepsilon_2} \dots v_n^{\varepsilon_n} w_n^{\varepsilon_n} \dots w_2^{\varepsilon_2} w_1^{\varepsilon_1}$$

sea no nulo. Entonces z es invertible y verifica:

$$N(z)^s = b_s^2 \; N(z),$$

para todo s de G, con los elementos b_s de L^* cumpliendo:

$$\frac{b_s \, b_t^s}{b_{st}} = a_{s,t} \cdot$$

Para hacer la demostración de 3.10, necesitamos una serie de lemas:

Lema 3.11. z cumple: $v_i \, z = z \, w_i$, para $i = 1,\dots n$.

Demostración. Tenemos:

$$v_i\, v_1^{\varepsilon_1}\ldots v_i^{\varepsilon_i}\ldots v_n^{\varepsilon_n} = (-1)^{\sum_{j<i}\varepsilon_j}\, v_1^{\varepsilon_1}\ldots v_i^{\varepsilon_i+1}\ldots\, v_n^{\varepsilon_n}, \text{con } \varepsilon_i+1\in\mathbb{Z}/2\,\mathbb{Z},$$

$$w_n^{\varepsilon_n}\ldots w_i^{\varepsilon_i}\ldots\, w_1^{\varepsilon_1}\, w_i = (-1)^{\sum_{j<i}\varepsilon_j}\, w_n^{\varepsilon_n}\ldots\, w_i^{\varepsilon_i+1}\ldots\, w_1^{\varepsilon_1}.$$

Por tanto:

$$v_i\, z\, w_i = \sum_{\varepsilon_j=0,1} v_1^{\varepsilon_1}\ldots v_i^{\varepsilon_i+1}\ldots v_n^{\varepsilon_n}\, w_n^{\varepsilon_n}\ldots w_i^{\varepsilon_i+1}\ldots w_1^{\varepsilon_1} = z$$

o equivalentemente $v_i\, z = z\, w_i$ por ser $w_i^2 = 1$.#

Lema 3.12. z es invertible.

Demostración. Por 3.8, tenemos un elemento $f(\alpha)$ de $C_L^+(Q_F)$ invertible y tal que:

$$e_i \longmapsto f(\alpha)\, v_i\, f(\alpha)^{-1}$$

define un isomorfismo f' de $C(Q_I)$ en $C(Q_F)$ que restringe a un isomorfismo de $C^+(Q_I)$ en $C^+(Q_F)$. Sea g el isomorfismo de $C(Q_I)$ en $C(Q_F)$ introducido en el lema 3.9.

Si n es par, $C_L(Q_F)$ es álgebra simple central ([LA] V 2.5), por tanto gf'^{-1} es automorfismo interior, es decir existe un elemento a de $C(Q_F)$ invertible tal que:

$$f'(e_i) = a^{-1}\, g(e_i)\, a = a^{-1}\, w_i\, a.$$

Por tanto tenemos:

$f(\alpha)\, v_i\, f(\alpha)^{-1} = a^{-1}\, w_i\, a$ o bien $a\, f(\alpha)\, v_i = w_i\, a\, f(\alpha)$.

Por el lema 3.11, se tiene $v_i\ z = z\ w_i$. De las dos igualdades se obtiene:

$$v_i\ z\ a\ f(\alpha)\ v_i = z\ w_i^2\ a\ f(\alpha) = z\ a\ f(\alpha),$$

es decir el elemento z a f(α) está en el centro de $C_L(Q_F)$, por tanto en L. Tenemos pues

$$z = b\ [a\ f(\alpha)]^{-1} \quad \text{con } b \in L\ .$$

Hemos tomado g de manera que z sea no nulo, por tanto b es no nulo, y z invertible.

Supongamos ahora que n es impar. Entonces ([LA] V 2.4) $C_L^+(Q_F^i)$ es álgebra simple central. Por restringir f' y g a isomorfismos entre las partes pares de las álgebras, la restricción de gf'^{-1} a $C_L^+(Q_F)$ es automorfismo interior. A partir de aquí, la demostración es igual que en el caso n par, sustituyendo $C_L(Q_F)$ por $C_L^+(Q_F)$ y v_i, w_i por $v_i\ v_j$, $w_i\ w_j$, respectivamente. #

Lema 3.13. Sea $m_s = f(u_s)$, donde u_s es un sistema de representantes de G en $\tilde{G}$, y consideramos los u_s como elementos de $C(Q_I)$. Entonces se verifica:

$$v_i\ m_s^{-1}\ z^s = m_s^{-1}\ z^s\ w_i\ ,$$

para todo s de G y todo i = 1,..., n .

Demostración. Aplicando s a: $v_i\ z = z\ w_i$ (3.11) obtenemos : $v_i^s\ z^s = z^s\ w_i$, por ser w_i de $C(Q_F)$, y por tanto :

$$m_s^{-1}\, z^s\, w_i = (m_s^{-1}\, v_i^{\,s}\, m_s)\, m_s^{-1}\, z^s .$$

Calculamos $v_i^{\,s}$. Por definición, tenemos $v_i = f(e_i)$, con f isomorfismo de matriz M^{-1} en las bases $(e_i, e_2, \ldots e_n)$ y $(x_1, x_2, \ldots x_n)$, por tanto:

$$v_j = \sum_{i=1}^{n} c_{ij}\, x_i \ , \text{ con } (c_{ij}) = C = M^{-1}.$$

La matriz $M = (m_{ij})$ verificaba $m_{ij}^{\,s} = m_{s(i)j}$, por tanto su inversa C verifica $c_{ij}^{\,s} = c_{is(j)}$. Tenemos pues:

$$v_j^{\,s} = \sum_{i=1}^{n} c_{ij}^{\,s}\, x_i = \sum_{i=1}^{n} c_{is(j)}\, x_i = v_{s(j)}.$$

Ahora los elementos m_s verifican:

$$m_s\, m_t = a_{s,t}\, m_{st} \ ; \quad m_1 = 1 \quad ; \quad m_s\, v_i\, m_s^{-1} = v_{s(i)}$$

a partir de las relaciones análogas de u_s y e_i. Por tanto:

$$m_s^{-1} = a_{s,s^{-1}}\, m_{s^{-1}} \ ,$$

y se tiene:

$$m_s^{-1}\, v_i^{\,s}\, m_s = m_{s^{-1}}\, v_{s(i)}\, m_{s^{-1}}^{-1} = v_i \ .$$

Obtenemos pues:

$$m_s^{-1}\, z^s\, w_i = (m_s^{-1}\, v_i^{\,s}\, m_s)\, m_s^{-1}\, z^s = v_i\, m_s^{-1}\, z^s. \ \#$$

Lema 3.14. $m_s^{-1}\, z^s\, z^{-1}$ es un elemento de L^* y $b_s = m_s^{-1}\, z^s\, z^{-1}$ verifica:

$$\frac{b_s\, b_t^{\,s}}{b_{st}} = a_{s,t}\,,$$

para todo par s,t de elementos de G, con $a_{s,t}$ cociclo asociado a la extensión:

$$1 \longrightarrow \{\pm 1\} \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1$$

determinado por el sistema de representantes u_s fijado.

Demostración. De las dos igualdades:

$$v_i\, m_s^{-1}\, z^s = m_s^{-1}\, z^s\, w_i \qquad (3.13)$$

$$v_i\, z = z\, w_i \qquad (3.11)$$

se deduce $v_i\, m_s^{-1}\, z^s\, z^{-1}\, v_i^{-1} = m_s^{-1}\, z^s\, z^{-1}$, por tanto $b_s = m_s^{-1}\, z^s\, z^{-1}$ es del centro de $C_L(Q_F)$; además es par (por ser z y m_s pares) y por tanto de L ([0] 54:4).

Ahora, para cada elemento invertible z de $C_L(Q_F)$, se verifica la identidad:

$$(zz^{-s})\,(zz^{-t})^s\,(zz^{-st})^{-1} = 1.$$

Sustituyendo zz^{-s} por $b_s^{-1}\, m_s^{-1}$, etc, obtenemos:

$$b_s^{-1}\, m_s^{-1}\,(b_t^{-1}\, m_t^{-1})^s\,(b_{st}^{-1}\, m_{st}^{-1})^{-1} = 1$$

y de aquí:

$$b_s\, b_t^{\,s}\, b_{st}^{-1} = m_s^{-1}\, m_t^{-s}\, m_{st}.$$

Calculamos $m_t^{\,s}$. Hemos elegido el sistema de representantes u_s de G en $\tilde{G}$ de manera que cada u_s sea producto de un número par

de términos $(e_i - e_j)$ y factores $\frac{1}{2}$. Entonces, $m_s = f(u_s)$ es producto de un número par de términos $(v_i - v_j)$ y factores $\frac{1}{2}$.
De la igualdad:

$$m_s \, v_i \, m_s^{-1} = v_{s(i)} = v_i^{\,s}$$

(demostración de 3.13), se deduce pues:

$$m_s \, m_t \, m_s^{-1} = m_t^{\,s} .$$

Tenemos así:

$$b_s \, b_t^{\,s} \, b_{st}^{-1} = m_s^{-1} \, m_t^{-s} \, m_{st} = m_s^{-1} \, m_s \, m_t^{-1} \, m_s^{-1} \, m_{st} = a_{s,t} \, m_{st}^{-1} \, m_{st} = a_{s,t} .\#$$

Demostración de 3.10. Por 3.14, tenemos $z^s \, z^{-1} = b_s \, m_s$. Tomando normas espinoriales obtenemos:

$$\beta(z^s \, z^{-1}) \; z^s \, z^{-1} = b_s^{\,2} \quad \beta(m_s) \; m_s = b_s^{\,2} ,$$

ya que tenemos $N(u_s) = 1$ y por ser $m_s = f(u_s)$ y f extendido de un isomorfismo entre los espacios vectoriales, $N(m_s) = 1$. Ahora, el miembro de la izquierda es:

$$\beta(z^{-1}) \; \beta(z^s) \; z^s \, z^{-1} = \beta(z^{-1}) \; N(z)^s \, z^{-1} .$$

Tenemos pues: $\beta(z^{-1}) \; N(z)^s \, z^{-1} = b_s^{\,2}$ y por tanto:

$$N(z)^s = b_s^{\,2} \; \beta(z) \; z = b_s^{\,2} \; N(z) . \#$$

Teorema 3.15. Sea f el isomorfismo de $C_L(Q_I)$ en $C_L(Q_F)$, obtenido por extensión del morfismo de L^n en $F \underset{K}{\otimes} L$ con matriz M^{-1}. Sea $(e_1, e_2, \ldots, e_n)$ la base canónica de L^n, $v_i = f(e_i)$, $i = 1,2,\ldots,n$. Si es resoluble el problema de inmersión dado por $\tilde{G} \longrightarrow G \simeq Gal(L|K)$,

con $\tilde{G}$ extensión espinorial de G, entonces existe un isomorfismo g de $C(Q_I)$ en $C(Q_F)$, que transforma $C^+(Q_I)$ en $C^+(Q_F)$ y $C^-(Q_I)$ en $C^-(Q_F)$ y tal que, definiendo $w_i = g(e_i)$, $i = 1,\ldots, n$, el elemento de $C_L^+(Q_F)$:

$$z = \sum_{\varepsilon_i=0,1} v_1^{\varepsilon_1} v_2^{\varepsilon_2} \ldots v_n^{\varepsilon_n} w_n^{\varepsilon_n} \ldots w_2^{\varepsilon_2} w_1^{\varepsilon_1}$$

sea no nulo.

La solución general del problema de inmersión es:

$$L\ (\sqrt{r\gamma})$$

con $r \in K^*$ y γ cualquier coordenada no nula de la norma espinorial $N(z)$ de z en la base $\{w_1^{\varepsilon_1} w_2^{\varepsilon_2} \ldots w_n^{\varepsilon_n}\}_{\varepsilon_i=0,1}$ de $C_L(Q_F)$ (o en cualquier base de $C_L(Q_F)$ invariante por G).

Demostración. Por la proposición 3.4, existe un isomorfismo g de $C(Q_I)$ en $C(Q_F)$ que transforma $C^+(Q_I)$ en $C^+(Q_F)$ y $C^-(Q_I)$ en $C^-(Q_F)$. Por el lema 3.9, puede modificarse g para obtener z no nulo. Basta ahora igualar las coordenadas de los dos miembros de la igualdad $N(z)^s = b_s^2\ N(z)$, obtenida en 3.10, teniendo en cuenta que los w_i son invariantes por G. #

Observación. Si es trivial la extensión:

$$1 \longrightarrow \{\pm 1\} \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1$$

podemos tomar el sistema de representantes u_s de G en $\tilde{G}$ tal que el cociclo que determine sea $a_{s,t} = 1$, para todo par s,t de G. Entonces si $b_s \in L^*$ verifican $b_s\ b_t^s = a_{s,t}\ b_{st}$, $s \longmapsto b_s$ es

coborde, por tanto se tiene:

$$b_s = a^s\ a^{-1}$$

para un elemento a de L*. El elemento z verifica entonces:

$$N(z)^s = (a^s\ a^{-1})^2\ N(z)$$

o, equivalentemente,

$$(a^{-2}\ N(z))^s = a^{-2}\ N(z),$$

es decir $a^{-2}\ N(z)$ es un elemento invariante por G y por tanto de $C(Q_F)$. Una coordenada γ no nula de $N(z)$, en una base de $C(Q_F)$, será entonces de la forma:

$$\gamma = a^2.\ \gamma_o,\ \text{con}\ \ \gamma_o \in K^*.$$

El teorema 3.15 da pues la solución general al problema de inmersión también en este caso.

Veamos ahora como se obtiene un isomorfismo de $C(Q_I)$ en $C(Q_F)$, que transforme $C^+(Q_I)$ en $C^+(Q_F)$ y $C^-(Q_I)$ en $C^-(Q_F)$, en el caso en que Q_F sea equivalente sobre K a una forma cuadrática de la forma:

$$-(X_1^2 + X_2^2 +\ldots+ X_q^2) + X_{q+1}^2 +\ldots+ X_n^2\ .$$

Analizamos primero el caso en que Q_F es equivalente sobre K a la forma cuadrática identidad Q_I.

§3. SOLUCION EN EL CASO EN QUE Q_F ES EQUIVALENTE SOBRE K A LA IDENTIDAD.

Si Q_F es equivalente a la forma cuadrática identidad Q_I sobre K, tenemos:

$$d_F = d(Q_I) = 1 \qquad y \qquad w(Q_F) = w(Q_I) = 1,$$

por tanto el problema de inmersión es resoluble.

Sea $(x_1, x_2, \ldots, x_n)$ una base de F sobre K, T la matriz de la forma cuadrática traza Q_F en esta base, M la matriz introducida en el cap. II §3 tal que:

$$M^t M = T \ .$$

Suponemos que Q_F es equivalente sobre K a Q_I, por tanto existe una matriz P invertible de $M_n(K)$ tal que:

$$P^t T P = I \ .$$

Entonces el isomorfismo g de K^n en F, con matriz P en las bases $(e_1, e_2, \ldots, e_n)$, base canónica de K^n, y $(x_1, x_2, \ldots, x_n)$ de F, verifica $Q_F(g(x)) = Q_I(x)$ para todo x de K^n y por tanto se extiende a un isomorfismo g de $C(Q_I)$ en $C(Q_F)$.

Sea $w_i = g(e_i)$, $i = 1, \ldots, n$. Los w_i son vectores de F que en $C(Q_F)$ verifican las relaciones:

$$w_i^2 = 1 \quad , \quad 1 \le i \le n \quad ; \quad w_i w_j = -w_j w_i \ , \ 1 \le i \ne j \le n \ .$$

Formamos el elemento de $C_L(Q_F)$:

$$z = \sum_{\varepsilon_i = 0,1} v_1^{\varepsilon_1} v_2^{\varepsilon_2} \ldots v_n^{\varepsilon_n} w_n^{\varepsilon_n} \ldots w_2^{\varepsilon_2} w_1^{\varepsilon_1} \ .$$

Hemos visto que, cambiando si es necesario algunos de los vectores w_j por sus opuestos, el elemento z es no nulo. En este caso los elementos w_j están definidos por:

$$w_j = \sum_{i=1}^{n} p_{ij}\, x_i \quad , \quad j = 1, \ldots, n \, .$$

El cambio de w_j por $-w_j$ equivale pues a cambiar el signo de los elementos de la columna j de la matriz P. Puede comprobarse directamente que dicho cambio no modifica la igualdad.

$$P^t \, T \, P = I \, .$$

Suponemos que hemos cambiado en la matriz P los signos de los elementos de tantas columnas como haya sido necesario para obtener z no nulo. Realizados estos cambios, veremos que, en este caso, N(z) es un elemento de L^* y puede calcularse explícitamente en función de las matrices P y M.

Proposición 3.16. Sea $z = \sum_{\varepsilon_i = 0,1} v_1^{\varepsilon_1} v_2^{\varepsilon_2} \ldots v_n^{\varepsilon_n} w_n^{\varepsilon_n} \ldots w_2^{\varepsilon_2} w_1^{\varepsilon_1}$.

Se verifica

$$N(z) = 2^n \det (MP + I) \, .$$

Demostración. Tenemos $v_i z = z w_i$, por tanto, $\beta(z)\, v_i = w_i\, \beta(z)$, ya que v_i y w_i están en el espacio vectorial de $C_L(Q_F)$. Entonces se cumple:

$$\beta(z)\, z = \beta(z)\, v_i^2\, z = w_i \;\; \beta(z)\, z\, w_i \, .$$

$N(z) = \beta(z)\ z$ es pues elemento par del centro de $C_L(Q_F)$ y es por tanto de L. ([0] 54:4).

Calculamos ahora N(z):

$$\beta(z)\ z = \sum_{\varepsilon_i=0,1} w_1^{\varepsilon_1} w_2^{\varepsilon_2} \dots w_n^{\varepsilon_n} v_n^{\varepsilon_n} \dots v_2^{\varepsilon_2} v_1^{\varepsilon_1}\ z$$

$$= \sum_{\varepsilon_i=0,1} w_1^{\varepsilon_1} w_2^{\varepsilon_2} \dots w_n^{\varepsilon_n}\ z\ w_n^{\varepsilon_n} \dots w_2^{\varepsilon_2} w_1^{\varepsilon_1}\ .$$

Cada sumando tiene la misma componente en L que z, por tanto:

$$\beta(z)\ z = 2^n.(\text{componente en L de } z)\ .$$

Calculamos ahora la componente en L de z. Tenemos:

$$z = \sum_{\varepsilon_i=0,1} v_1^{\varepsilon_1} v_2^{\varepsilon_2} \dots v_n^{\varepsilon_n} w_n^{\varepsilon_n} \dots w_2^{\varepsilon_2} w_1^{\varepsilon_1}$$

$$= \sum_{i_1<i_2<\dots<i_k} v_{i_1} v_{i_2} \dots v_{i_k} w_{i_k} \dots w_{i_2} w_{i_1}\ .$$

Por otra parte, tenemos:

$$w_j = \sum_{i=1}^{n} d_{ij} v_i \quad , \text{ con } (d_{ij}) = D = M P\ .$$

Calculamos la componente en L de cada sumando de z.

$v_{i_1} v_{i_2} \dots v_{i_k} w_{i_k} \dots w_{i_2} w_{i_1}$ tiene componente en L igual a la coordenada según $v_{i_1} v_{i_2} \dots v_{i_k}$ de $w_{i_1} w_{i_2} \dots w_{i_k}$.

$$w_{i_1} w_{i_2} \dots w_{i_k} = \left(\sum_{\ell=1}^{n} d_{\ell i_1} v_\ell\right)\left(\sum_{\ell=1}^{n} d_{\ell i_2} v_\ell\right) \dots \left(\sum_{\ell=1}^{n} d_{\ell i_k} v_\ell\right)$$

tiene coordenada según $v_{i_1}\ v_{i_2} \ldots v_{i_k}$ igual a:

$$\Sigma\ sg(\sigma)\ d_{\sigma(i_1)i_1}\ d_{\sigma(i_2)i_2} \cdots d_{\sigma(i_k)i_k}\ ,$$

donde σ recorre las permutaciones de los índices $i_1, i_2, \ldots i_k$ y $sg(\sigma)$ es el signo de la permutación. Es pues el menor principal de la matriz D formado por las filas y columnas de índices $i_1, i_2, \ldots i_k$.

La componente de z en L es pues la suma de todos los menores principales de la matriz MP más 1 (el sumando con todos los ε_i nulos), es decir el polinomio característico de MP valorado en -1, igual a det (MP + I). #

Teorema 3.17. Sea $(x_1, x_2, \ldots, x_n)$ una base de F sobre K. Sean $s_1, s_2, \ldots, s_n$ elementos de G tales que $F^{s_1} = F$; $F^{s_2}, \ldots, F^{s_n}$ sean todos los conjugados de F. Sea M la matriz de $M_n(L)$ definida por:

$$M = (x_j^{s_i}) \quad \begin{matrix} 1 \leq i \leq n \\ 1 \leq j \leq n \end{matrix} .$$

Sea T la matriz de Q_F, forma cuadrática traza de F|K, en la base $(x_1, x_2, \ldots, x_n)$.

Si Q_F es equivalente a la identidad sobre K, y $P \in M_n(K)$ verifica $P^t\ T\ P = I$, entonces la solución general al problema de inmersión dado por $\tilde{G} \longrightarrow G = Gal\ (L|K)$ es:

$$L(\sqrt{r\gamma}),\ \text{con}\ \ \gamma = \det(MP + I)\ \ \text{y}\ \ r \in K^* .$$

Demostración. En este caso, por ser N(z) de L^*, N(z) es solución al problema de inmersión (por 3.10 y 2.11). γ difiere de N(z) en un elemento de K^* (ya que K tiene característica distinta de 2) por tanto, por 2.2, es también solución y se tiene la solución general. #

Veamos ahora en que casos se verifica la hipótesis de que Q_F sea equivalente a la identidad sobre K, supuesto $d_F = 1$ y el problema de inmersión resoluble.

Proposición 3.18. Si $d_F = 1$, para n = 4 ó 5, son equivalentes:
a) El problema de inmersión es resoluble.
b) La forma cuadrática traza Q_F es equivalente a la identidad sobre K.

Por tanto, en este caso, la solución viene dada por el teorema 3.17.

Demostración. Por ([S_3] 3.2), el problema de inmersión es resoluble, es decir $w(Q_F) = (2, d_F)$, si y sólo si se tiene:
para n = 4, Q_F equivalente a $X_1^2 + X_2^2 + 2X_3^2 + 2d_F X_4^2$ sobre K,
para n = 5, Q_F equivalente a $X_1^2 + X_2^2 + X_3^2 + 2X_4^2 + 2d_F X_5^2$ sobre K.

Si $d_F = 1$, teniendo en cuenta que $2X_1^2 + 2X_2^2$ es equivalente a $Y_1^2 + Y_2^2$, mediante el cambio $Y_1 = X_1 + X_2$, $Y_2 = X_1 - X_2$, se obtiene, en los dos casos, Q_F equivalente a la identidad sobre K. #

Ejemplo. Sea K, como siempre, un cuerpo de característica distinta de 2. Sea L una extensión bicuadrática de K que escribimos $L = K(x_1, x_2, x_3)$ con $x_i^2 = a_i \in K^*$, $i = 1, 2, 3$, y $x_1 x_2 x_3 = 1$. $L|K$ es extensión de Galois con grupo $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Un elemento primitivo de la extensión es $\Theta = x_1 + x_2$ y el polinomio que da la extensión es:

$$f(X) = X^4 - 2(a_1 + a_2) X^2 + (a_1 + a_2)^2 + 4 a_1 a_2 .$$

Tenemos $G = \{g_1, g_2, g_3, g_4\}$ donde g_1 es la identidad y los restantes están definidas por:

$$g_2: \begin{matrix} x_1 \longmapsto -x_1 \\ x_2 \longmapsto x_2 \end{matrix} \qquad g_3: \begin{matrix} x_1 \longmapsto x_1 \\ x_2 \longmapsto -x_2 \end{matrix} \qquad g_4: \begin{matrix} x_1 \longmapsto -x_1 \\ x_2 \longmapsto -x_2 \end{matrix}$$

Ordenamos las 4 raices del polinomio f:

$$\Theta_1 = \Theta,\ \Theta_2 = g_2(\Theta) = -x_1 + x_2,\ \Theta_3 = g_3(\Theta) = x_1 - x_2,\ \Theta_4 = g_4(\Theta) = -x_1 - x_2 .$$

Tenemos que g_2, g_3, g_4 producen sobre los índices de las raices Θ_1, Θ_2, Θ_3, Θ_4 las permutaciones (12)(34), (13)(24), (14)(23) respectivamente. Obtenemos así la inclusión de G en A_4 y la antiimagen $\tilde{G}$ de G en $\tilde{A}_4$ es el grupo de los cuaterniones (cf [S_3]3.2).

En este caso, tenemos F = L. Sea Q_F la forma traza de $F|K$. En la base $(1, x_1, x_2, x_3)$, Q_F tiene matriz diagonal:

$$T = \begin{bmatrix} 4 & & & \\ & 4a_1 & & \\ & & 4a_2 & \\ & & & 4a_3 \end{bmatrix}$$

La matriz M de $M_4(L)$ tal que $M^t M = T$ es:

$$M = \begin{bmatrix} 1 & x_1 & x_2 & x_3 \\ 1 & -x_1 & x_2 & -x_3 \\ 1 & x_1 & -x_2 & -x_3 \\ 1 & -x_1 & -x_2 & x_3 \end{bmatrix}$$

Por la proposición 3.18, el problema de inmersión:

$$\begin{array}{ccccccccc} & & & & & & & & G_K \\ & & & & & & & & \downarrow \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \tilde{G} & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

tiene solución si y sólo si Q_F es equivalente sobre K a la identidad, es decir si existe una matriz P de $M_4(K)$, invertible tal que $P^t\ T\ P = I$. Entonces la solución es $\gamma = \det(MP + I)$.

Calculamos ahora la solución de modo a lograr de ella una expresión sencilla. Consideramos la matriz diagonal:

$$W = \begin{bmatrix} 1 & & & \\ & x_1 & & \\ & & x_2 & \\ & & & x_3 \end{bmatrix}$$

W verifica:

$$W^t\ W = \begin{bmatrix} 1 & & & \\ & a_1 & & \\ & & a_2 & \\ & & & a_3 \end{bmatrix}$$

Por tanto 2W verifica $(2W)^t\ (2W) = T$. Las matrices M y 2W difieren pues en una matriz ortogonal. Calculando $M(2W)^{-1}$ se obtiene:

$$M(2W)^{-1} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

Indicaremos esta matriz por Ω.

Sea ahora

$$\bar{P} = \begin{bmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{bmatrix}$$

una matriz con coeficientes en K, de determinante 1, y verificando

$$\bar{P}^t \begin{bmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{bmatrix} \bar{P} = I.$$

Sea P la matriz de $M_4(K)$ definida por

$$2\ P\ \Omega = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & & & \\ 0 & & \bar{P} & \\ 0 & & & \end{bmatrix}$$

Se cumple:

$$(2\ P\ \Omega)^t \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & a_2 & 0 \\ 0 & 0 & 0 & a_3 \end{bmatrix} (2\ P\ \Omega) = I,$$

y por tanto: $(P\ \Omega)^t\ T\ P\ \Omega = I$, lo cual implica

$$P^t\ T\ P = (\Omega^{-1})^t\ \Omega^{-1} = I\ .$$

El elemento $\gamma = \det\ (MP + I)$ es pues solución al problema de inmersión. Ahora tenemos:

$$\det(MP + I) = \det\ (P^{-1}(PM + I)P) = \det\ (PM + I)$$

y, para la matriz PM, se cumple: $PM = P(\Omega\ 2\ W) = 2\ P\ \Omega\ W$, por tanto:

$$PM = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p_{11} & p_{12} & p_{13} \\ 0 & p_{21} & p_{22} & p_{23} \\ 0 & p_{31} & p_{32} & p_{33} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & x_1 & 0 & 0 \\ 0 & 0 & x_2 & 0 \\ 0 & 0 & 0 & x_3 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p_{11}\,x_1 & p_{12}\,x_2 & p_{13}\,x_3 \\ 0 & p_{21}\,x_1 & p_{22}\,x_2 & p_{23}\,x_3 \\ 0 & p_{31}\,x_1 & p_{32}\,x_2 & p_{33}\,x_3 \end{bmatrix}$$

El determinante de PM + I es pues igual a

$$2 \det \left[\begin{bmatrix} p_{11} x_1 & p_{12} x_2 & p_{13} x_3 \\ p_{21} x_1 & p_{22} x_2 & p_{23} x_3 \\ p_{31} x_1 & p_{32} x_2 & p_{33} x_3 \end{bmatrix} + I \right] =$$

$$= 2 \left[1 + p_{11} x_1 + p_{22} x_2 + p_{33} x_3 + \begin{vmatrix} p_{11} x_1 & p_{12} x_2 \\ p_{21} x_1 & p_{22} x_2 \end{vmatrix} + \right.$$

$$\left. + \begin{vmatrix} p_{11} x_1 & p_{13} x_3 \\ p_{31} x_1 & p_{33} x_3 \end{vmatrix} + \begin{vmatrix} p_{21} x_2 & p_{23} x_3 \\ p_{32} x_2 & p_{33} x_3 \end{vmatrix} + \begin{vmatrix} p_{11} x_1 & p_{12} x_2 & p_{13} x_3 \\ p_{21} x_1 & p_{22} x_2 & p_{23} x_3 \\ p_{31} x_1 & p_{32} x_2 & p_{33} x_3 \end{vmatrix} \right].$$

El último sumando es $(\det \bar{P})(x_1\ x_2\ x_3) = 1$. Ahora, la matriz $\bar{P}$ verifica:

$$\bar{P}^t \begin{bmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{bmatrix} \bar{P} = I, \text{ y por tanto } \bar{P}^{-1} = \bar{P}^t \begin{bmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{bmatrix},$$

igualando los elementos de la diagonal de las dos matrices, obtenemos:

$$p_{11}\ a_1 = \begin{vmatrix} p_{22} & p_{23} \\ p_{32} & p_{33} \end{vmatrix}, \quad p_{22}\ a_2 = \begin{vmatrix} p_{11} & p_{13} \\ p_{31} & p_{33} \end{vmatrix}, \quad p_{33}\ a_3 = \begin{vmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{vmatrix},$$

y por tanto:

$$\begin{vmatrix} p_{11}\,x_1 & p_{12}\,x_2 \\ p_{21}\,x_1 & p_{22}\,x_2 \end{vmatrix} = x_1\,x_2 \begin{vmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{vmatrix} = x_1\,x_2\,p_{33}\,a_3 =$$

$$= (x_1\,x_2\,x_3)\,p_{33}\,x_3 = p_{33}\,x_3$$

y del mismo modo:

$$\begin{vmatrix} p_{11}\,x_1 & p_{13}\,x_3 \\ p_{31}\,x_1 & p_{33}\,x_3 \end{vmatrix} = p_{22}\,x_2 \quad ; \quad \begin{vmatrix} p_{22}\,x_2 & p_{23}\,x_3 \\ p_{32}\,x_2 & p_{33}\,x_3 \end{vmatrix} = p_{11}\,x_1$$

Obtenemos así:

$$\det (PM + I) = 2(1 + p_{11}\,x_1 + p_{22}\,x_2 + p_{33}\,x_3 + p_{33}\,x_3 + p_{22}\,x_2 + p_{11}\,x_1 + 1)$$

$$= 4(1 + p_{11}\,x_1 + p_{22}\,x_2 + p_{33}\,x_3)\,.$$

Una solución al problema de inmersión es pues:

$$\gamma = 1 + p_{11}\,x_1 + p_{22}\,x_2 + p_{33}\,x_3$$

Observación. El ejemplo anterior fue resuelto por Witt ([W] VI). En su trabajo demuestra que, para que el problema de inmersión sea resoluble, es condición necesaria y suficiente que la forma cuadrática $\sum_{i=1}^{3} a_i\,X_i^2$ sea equivalente a la identidad sobre K, es decir que exista una matriz $\bar{P}$ con coeficientes en K.

$$\bar{P} = \begin{bmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{bmatrix}$$

tal que

$$\bar{P}^t \begin{bmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{bmatrix} \bar{P} = I,$$

y que, en el caso en que el problema sea resoluble, la solución viene dada por el elemento

$$\gamma = 1 + p_{11} x_1 + p_{22} x_2 + p_{33} x_3 .$$

La fórmula de Serre (2.14) generaliza la primera parte del resultado de Witt. Hemos generalizado aquí la segunda parte dando así respuesta a la observación de Serre ([S_3] 3.2).

Para llegar a la solución, Witt utiliza la equivalencia entre la resolubilidad del problema y el que el álgebra producto cruzado sea isomorfa a un álgebra de matrices sobre K (2.15). Para la extensión de grupos estudiada por Witt, el álgebra producto cruzado es producto tensorial de dos álgebras de cuaterniones. Witt obtiene la solución como norma de un elemento C del álgebra Q_L obtenida a partir de una de estas álgebras, ampliando escalares a L. Puede verse que Q_L es subálgebra de $C_L^+(Q_I) \simeq C_L^+(Q_F)$ y que, para el elemento C, coinciden su norma en el álgebra de cuaterniones con su norma espinorial.

Caso K = Q

Analizamos ahora, en el caso en que K es el cuerpo Q de los racionales, cuando se verifica la condición de que Q_F sea equivalente a la identidad sobre Q. Suponemos $d_F = 1$ y $w(Q_F) = 1$, por

tanto el discriminante y el invariante de Hasse-Witt coinciden para Q_F y la identidad. Las dos formas son pues equivalentes si y sólo si la signatura de Q_F es $(n,0)$. Definimos enteros r_1, $r_2 \geq 0$ por la relación:

$$\mathbb{R} \otimes F \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

es decir r_1 es el número de inmersiones reales de F, $2r_2$ el de inmersiones complejas. Tenemos $[F:Q] = n = r_1 + 2r_2$ y la signatura de Q_F es $(r_1 + r_2, r_2)$.

Por tanto Q_F es equivalente a la identidad sobre Q si y sólo si $F|Q$ es totalmente real.

§4. SOLUCION EN EL CASO EN QUE Q_F ES ISOMORFA SOBRE K A LA FORMA $-(X_1^2 + \ldots + X_q^2) + X_{q+1}^2 + \ldots + X_n^2$

Sea Q_q la forma cuadrática:

$$Q_q = -(X_1^2 + X_2^2 + \ldots + X_q^2) + X_{q+1}^2 + \ldots + X_n^2 .$$

El discriminante de Q_q es $(-1)^q$. Su invariante de Hasse-Witt es:

$$w(Q_q) = (-1, -1) \otimes \overset{\frac{q(q-1)}{2}}{\ldots} \otimes (-1, -1).$$

Tenemos $(-1, -1) \otimes (-1, -1) \simeq (1, -1)$ y $(-1, -1) \neq 1$, por tanto $w(Q_q) = 1$ si y sólo si $\frac{q(q-1)}{2}$ es par, es decir $q \equiv 0$ ó $1 \bmod 4$. Q_F equivalente a Q_q sobre K implica que las dos formas cuadráticas tienen mismo discriminante y mismo invariante de Hasse-Witt. Nos situamos en el caso en que d_F es 1, por tanto el problema

de inmersión es resoluble si y sólo si $w(Q_F) = 1$. Las condiciones $d(Q_q) = 1$ y $w(Q_q) = 1$ se cumplen si y sólo si $q \equiv 0 \pmod 4$. Tenemos pues:

$$Q_F \overset{K}{\sim} -(X_1^2 + \ldots + X_q^2) + X_{q+1}^2 + \ldots + X_n^2 \text{ , con } q \equiv 0 \quad (4).$$

Veamos como puede construirse en este caso un K-isomorfismo de $C(Q_I)$ en $C(Q_F)$.

Si Q_F es equivalente a Q_q sobre K, existe una matriz P invertible de $M_n(K)$, tal que:

$$P^t \, T \, P = S_q,$$

dónde T es, como antes, la matriz de Q_F en una base $(x_1, x_2, \ldots x_n)$ de $F|K$ y S_q es la matriz diagonal (s_{ij}) con

$$s_{ii} = -1 \text{ , } 1 \leq i \leq q \text{ ; } s_{ii} = +1 \text{ , } q+1 \leq i \leq n .$$

Entonces el isomorfismo $K^n \longrightarrow F$ con matriz P en las bases $(e_1, e_2, \ldots, e_n)$, base canónica de K^n, y $(x_1, x_2, \ldots, x_n)$ de F, extiende a un isomorfismo:

$$C(Q_q) \xrightarrow{\sim} C(Q_F) .$$

Sea t_i, $i = 1, \ldots n$, la imagen de e_i por dicho isomorfismo. Los t_i son vectores de F que, en $C(Q_F)$, verifican las relaciones:

$$t_j^2 = -1 \text{ , } 1 \leq j \leq q \text{ ; } t_j^2 = +1 \text{ , } q+1 \leq j \leq n,$$

$$t_i t_j = -t_j t_i \text{ , } 1 \leq i \neq j \leq n .$$

Veamos ahora como se construyen elementos w_i, $i = 1, \ldots, n$ en $C(Q_F)$ tales que $g(e_i) = w_i$ defina un isomorfismo de $C(Q_I)$ en

$C(Q_F)$, que transforme $C^+(Q_I)$ en $C^+(Q_F)$ y $C^-(Q_I)$ en $C^-(Q_F)$.

Proposición 3.19. Sean $t_1, t_2, \ldots t_n$ los elementos de $C(Q_F)$ definidos arriba. Tenemos $q \equiv 0 \pmod 4$. Cambiamos los índices de los t_j con $1 \leq j \leq q$ en la forma siguiente

$$t_j^i = t_{4i+j} \quad , \quad i = 0, \ldots \frac{q}{4} - 1 \quad , \quad j = 1, 2, 3, 4$$

y definimos:

$$w_1^i = t_2^i\, t_3^i\, t_4^i$$

$$w_2^i = t_1^i\, t_3^i\, t_4^i$$

$$w_3^i = t_1^i\, t_2^i\, t_4^i$$

$$w_4^i = t_1^i\, t_2^i\, t_3^i \quad , \quad i = 0, \ldots, \frac{q}{4} - 1 .$$

Entonces se verifica:

$$(w_j^i)^2 = +1 \qquad j = 1, \ldots, 4 \qquad i = 0, \ldots, \frac{q}{4} - 1$$

$$w_1^i\, w_2^i = t_1^i\, t_2^i \qquad w_1^i\, w_3^i = -t_1^i\, t_3^i \qquad w_1^i\, w_4^i = t_1^i\, t_4^i$$

$$w_2^i\, w_3^i = -t_2^i\, t_3^i \qquad w_2^i\, w_4^i = -t_2^i\, t_4^i \qquad w_3^i\, w_4^i = t_3^i\, t_4^i$$

Definimos ahora w_i, $1 \leq i \leq n$, por:

$$w_{4i+j} = w_j^i \qquad i = 0, \ldots \frac{q}{4} - 1 \qquad j = 1, 2, 3, 4$$

$$w_k = t_k \qquad k = q+1, \ldots, n$$

Los elementos $w_1, w_2, \ldots, w_n$ cumplen:

$w_i^2 = +1 \quad , \quad 1 \leq i \leq n \quad ; \quad w_i\, w_j = -w_j\, w_i \quad , \quad 1 \leq i \neq j \leq n .$

Se define un isomorfismo g de $C(Q_I)$ en $C(Q_F)$ que transforma $C^+(Q_I)$ en $C^+(Q_F)$ y $C^-(Q_I)$ en $C^-(Q_F)$, mediante:

$$g(e_i) = w_i \quad , \quad i = 1,\ldots, n .$$

Demostración. Basta utilizar las reglas de producto de los t_i para obtener la primera parte de la proposición.

Los elementos e_i de $C(Q_I)$ y w_i de $C(Q_F)$ se multiplican con las mismas reglas, por tanto:

$$e_i \longmapsto w_i$$

define un morfismo.$(t_1, t_2,\ldots, t_n)$ es base del espacio vectorial de $C(Q_F)$, por tanto los t_i generan $C(Q_F)$. Además se verifica:

$$w_1^i\, w_2^i\, w_3^i = - t_4^i$$

$$w_1^i\, w_2^i\, w_4^i = - t_3^i$$

$$w_1^i\, w_3^i\, w_4^i = - t_2^i$$

$$w_2^i\, w_3^i\, w_4^i = - t_1^i \quad , \quad i = 0,\ldots,\frac{g}{4}$$

Por tanto los elementos w_i, $i = 1,\ldots, n$, geñeran $C(Q_F)$ y el morfismo:

$$C(Q_I) \longrightarrow C(Q_F)$$

$$e_i \longmapsto w_i$$

es isomorfismo.

Tenemos la relación $w_i\, w_j = \pm\, t_i\, t_j$ para todo par de elementos $i \neq j$ entre 1 y n, por tanto $C^+(Q_I)$ y $C^+(Q_F)$ se corresponden por el isomorfismo. Por ser cada w_i igual a t_i o a un producto de tres t's, el isomorfismo transforma $C^-(Q_I)$ en $C^-(Q_F)$. #

Observación. Por el isomorfismo obtenido en la proposición anterior no se corresponden los espacios vectoriales, $<e_1,e_2,\ldots,e_n>$ de $C(Q_I)$ y $<t_1,t_2,\ldots,t_n>$ de $C(Q_F)$. Si fuera así, tendríamos para $x \in K^n$:

$$Q_F\ (g(x)) = g(x)^2 = x^2 = Q_I(x)$$

y las formas cuadráticas Q_I y Q_F serían equivalentes sobre K.

Formamos ahora el elemento de $C_L(Q_F)$:

$$z = \sum_{\varepsilon_i=0,1} v_1^{\varepsilon_1}\, v_2^{\varepsilon_2} \ldots\, v_n^{\varepsilon_n}\, w_n^{\varepsilon_n} \ldots\, w_2^{\varepsilon_2}\, w_1^{\varepsilon_1}\ .$$

Por lo visto anteriormente, podemos suponer que z es no nulo, cambiando eventualmente alguno de los w_j por sus opuestos. En este caso si es $q + 1 \leq j \leq n$, tenemos

$$w_j = t_j = \sum_{i=1}^{n} p_{ij}\, x_i\ .$$

Por tanto cambiar w_j por $-w_j$ equivale a cambiar de signo los elementos de la columna j de la matriz P. Si es $1 \leq j \leq q$, poniendo $w_j^i = w_{4i+j}$, tenemos las relaciones (demostración de 3.19):

$$t_4^i = - w_1^i\, w_2^i\, w_3^i \quad ; \quad t_3^i = - w_1^i\, w_2^i\, w_4^i \quad ;$$

$$t_2^i = - w_1^i\, w_3^i\, w_4^i \quad ; \quad t_1^i = - w_2^i\, w_3^i\, w_4^i \quad .$$

Por tanto cambiar w_j por $-w_j$ para $1 \leq j \leq q$, equivale a cambiar 3 vectores t por sus opuestos, por tanto el signo de los elementos de 3 columnas de la matriz P.

Supuestos hechos en la matriz P los cambios necesarios para tener z no nulo, veremos que también en este caso puede calcularse explícitamente una solución al problema de inmersión en términos de las matrices M y P. Para ello calculamos primero la norma espinorial de z.

Proposición 3.20. El elemento N(z) es de la forma:

$$N(z) = 2^n \cdot \gamma \cdot w_1\, w_2 \cdots w_q$$

donde γ es la componente en L del elemento $z\, w_q\, w_{q-1} \cdots w_1$ de $C_L(Q_F)$.

Demostración. Veamos primero que $N(z)\, w_q \ldots w_1$ es un elemento de L.

Aplicando β, antiàutomorfismo principal de $C_L(Q_F)$, a la relación $v_1\, z = z\, w_i$ (3.11), se obtiene $\beta(z)\, v_i = \beta(w_i)\, \beta(z)$. Se cumple pues:

$$N(z) = \beta(z)\, z = \beta(w_i)\, \beta(z)\, z\, w_i = \beta(w_i)\, N(z)\, w_i \quad ,$$

o equivalentemente

$$\beta(w_i)\, N(z) = N(z)\, w_i \quad ,$$

para $i = 1, \ldots, n$.

Si es $i \leq q$, w_i es producto de 3 vectores del espacio vectorial de $C_L(Q_F)$, por tanto es $\beta(w_i) = -w_i$ y se tiene:

$$N(z)\ w_q \ldots w_1\ w_i = N(z)(-1)^{q-1}\ w_i\ w_q \ldots w_1 = (-1)^{q-1}\ \beta(w_i)\ N(z)\ w_q \ldots w_1$$

$$= (-1)^q\ w_i\ N(z)\ w_q \ldots w_1 = w_i\ N(z)\ w_q \ldots w_1 .$$

Si es $i > q$, $w_i = t_i$ es del espacio vectorial de $C_L(Q_F)$, por tanto es $\beta(w_i) = w_i$ y se tiene:

$$N(z)\ w_q \ldots w_1\ w_i = N(z)(-1)^q\ w_i\ w_q \ldots w_1 = w_i\ N(z)\ w_q \ldots w_1 .$$

$N(z)\ w_q \ldots w_1$ es pues un elemento par del centro de $C_L(Q_F)$ y es por tanto de L ([0] 54:4).

Veamos ahora que se cumple $N(z)\ w_q \ldots w_1 = 2^n\ \gamma$, con γ componente en L del elemento $z\ w_q \ldots w_1$.

Tenemos:

$$\beta(z)\ z\ w_q \ldots w_1 = (\Sigma\ \beta(w_1)^{\varepsilon_1} \ldots \beta(w_n)^{\varepsilon_n}\ v_n^{\varepsilon_n} \ldots v_1^{\varepsilon_1})\, z\ w_q \ldots w_1 .$$

Utilizando (3.11), la expresión anterior es igual a:

$$\Sigma\ \beta(w_1)^{\varepsilon_1} \ldots \beta(w_n)^{\varepsilon_n}\ z\ w_n^{\varepsilon_n} \ldots\ w_1^{\varepsilon_1}\ w_q \ \ldots\ w_1 \ .$$

Usando las reglas de producto de los w_i, y la expresión de $\beta(w_i)$, queda:

$$\Sigma\ \beta(w_1)^{\varepsilon_1}\ldots\beta(w_n)^{\varepsilon_n}\ z\ w_q\ldots w_1\ w_n^{\varepsilon_n}\ldots w_1^{\varepsilon_1}.(-1)^{\sum_{i=1}^{q}\ \sum_{j\neq i}\varepsilon_j}$$

$$= \Sigma(-1)^{\sum_{i=1}^{q}\varepsilon_i}\ w_1^{\varepsilon_1}\ldots w_n^{\varepsilon_n}\ (z\ w_q\ldots w_1)\ w_n^{\varepsilon_n}\ldots w_1^{\varepsilon_1}(-1)^{\sum_{i=1}^{q}\ \sum_{j\neq i}\varepsilon_j}$$

$$= \Sigma(-1)^{q\ \sum_{j=1}^{q}\varepsilon_j}\ w_1^{\varepsilon_1}\ldots w_n^{\varepsilon_n}\ (z\ w_q\ldots w_1)\ w_n^{\varepsilon_n}\ldots\ w_1^{\varepsilon_1}$$

$$= \Sigma\ w_1^{\varepsilon_1}\ldots w_n^{\varepsilon_n}\ (z\ w_q\ldots w_1)\ w_n^{\varepsilon_n}\ldots w_1^{\varepsilon_1}\ .$$

Cada sumando de la última expresión tiene la misma componente en L que el elemento $z\ w_q\ldots w_1$. Obtenemos pues:

$$N(z)\ w_q\ldots w_1 = 2^n\ \gamma\ ,$$

con γ componente de $z\ w_q\ldots w_1$ en L o equivalentemente:

$$N(z) = 2^n\ \gamma\ w_1\ldots w_q\ .\ \#$$

Proposición 3.21. La componente γ de $z\ w_q\ w_{q-1}\ldots w_1$ en L puede expresarse en la forma siguiente:

$$\gamma = \sum_{C}\ (-1)^{\delta(C)}\ \det C,$$

donde C recorre un subconjunto de submatrices k x k, con $n-q \leq k \leq n$, de la matriz MP + J, con:

$$J = \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix} \begin{matrix} q \\ n-q \end{matrix}$$

Dicho subconjunto comprende todas las submatrices cuadradas C de MP + J que contienen la submatriz de MP + J formada por las n - q últimas filas y columnas y que cumplen las siguientes reglas respecto de los índices 1 a q.

1) El número de valores de i entre 0 y $\frac{q}{4} - 1$ tales que en C no aparece ninguna de las 4 filas de índices 4i+1 a 4i+4 de MP + J coincide con el número de valores de i entre 0 y $\frac{q}{4} - 1$ tales que en C aparecen las 4 filas de índices 4i+1 a 4i+4.

2) Para cada valor de i = 0,...$\frac{q}{4} - 1$, los índices de columnas de MP + J tomadas para formar C, comprendidos entre 4i+1 y 4i+4, quedan determinados por los de filas en la forma siguiente:

a) Si entre los índices de fila figura exactamente un valor entre 4i+1 y 4i+4, entre los de columna figura el mismo.

b) Si entre los índices de fila figuran dos valores entre 4i+1 y 4i+4, entre las dos columnas figuran los otros dos valores comprendidos entre 4i+1 y 4i+4.

c) Si entre los índices de fila figuran tres valores entre 4i+1 y 4i+4, entre los de columna figuran los mismos.

d) Si entre los índices de fila no figura ningún valor (resp. figuran todos los valores) entre 4i+1 y 4i+4, entre los de columna figuran todos (resp. no figura ninguno).

En cuanto a $\delta(C)$, se tiene:

$$\delta(C) = \sum_{i=0}^{\frac{q}{4}-1} \delta_C(i)$$

donde $\delta_C(i) = 0$ en los casos a) y d) y en el caso b) si además los índices de fila son $4i+j_1$ y $4i+j_2$ con $(j_1, j_2) = (1,2)$, $(2,3)$ ó $(3,4)$ y $\delta_C(1) = +1$ en todos los demás casos.

Para la demostración de la proposición utilizaremos los dos lemas siguientes:

Lema 3.22. La componente en L del elemento de $C_L(Q_F)$:

$$v_{i_1} v_{i_2} \cdots v_{i_k} t_{j_\ell} \cdots t_{j_2} t_{j_1}$$

con $i_1 < i_2 < \cdots < i_k$, $j_1 < j_2 < \cdots < j_\ell$ es igual a 0 si $k \neq \ell$ y es igual al menor de filas $i_1, i_2, \ldots, i_k$ y columnas $j_1, j_2, \ldots, j_k$ de la matriz MP si $k = \ell$.

Demostración. Por definición de los vectores v_i y t_j, tenemos:

$$t_j = \sum_{i=1}^{n} d_{ij} v_i \quad , \quad \text{con} \quad (d_{ij}) = D = MP \quad ;$$

$$v_j = \sum_{i=1}^{n} d'_{ij} t_i \quad , \quad \text{con} \quad (d'_{ij}) = D' = D^{-1}.$$

Si $k > \ell$, sustituyendo cada t_j por su expresión en la base $(v_1, \ldots, v_n)$, en $v_{i_1} v_{i_2} \cdots v_{i_k} t_{j_\ell} \cdots t_{j_2} t_{j_1}$ y desarrollando, se obtiene que en cada sumando figura un producto de al menos $k - \ell$ v_i's distintos. Por tanto, este elemento no tiene componente en L. Si es $k < \ell$, se obtiene el resultado en forma análoga escribiendo los v_i en función de los t_j.

Si es $k = \ell$, el elemento $v_{i_1} v_{i_2} \cdots v_{i_k} t_{j_k} \cdots t_{j_2} t_{j_1}$ es igual a:

$$v_{i_1} v_{i_2} \ldots v_{i_k} \left(\sum_{i=1}^{n} d_{ij_k} v_i\right) \ldots \left(\sum_{i=1}^{n} d_{ij_2} v_i\right) \left(\sum_{i=1}^{n} d_{ij_1} v_i\right)$$

y su componente en L es:

$$\sum_{\sigma \in S_k} d_{i_{\sigma(1)} j_1} d_{i_{\sigma(2)} j_2} \ldots d_{i_{\sigma(k)} j_k} v_{i_1} v_{i_2} \ldots v_{i_k} v_{i_{\sigma(k)}} \ldots v_{i_{\sigma(2)}} v_{i_{\sigma(1)}}$$

$$= \sum_{\sigma \in S_k} (-1)^{sg(\sigma)} d_{i_{\sigma(1)} j_1} d_{i_{\sigma(2)} j_2} \cdots d_{i_{\sigma(k)} j_k},$$

es pues el menor de filas $i_1, i_2, \ldots, i_k$ y columnas $j_1, j_2, \ldots j_k$ de la matriz $D = MP$. #

Lema 3.23. Si M es una matriz n x n con coeficientes en un cuerpo L y J_k la matriz

$$J_k = \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix} \begin{matrix} k \\ n-k \end{matrix}$$

el determinante de la matriz $M + J_k$ es igual a la suma de los menores principales de M que contienen las k primeras filas y columnas de M.

Demostración. Se hace por recurrencia sobre n - k, utilizando propiedades elementales de los determinantes. #

Demostración de 3.21. Tenemos:

$$z\, w_q \ldots w_1 = \sum_{\varepsilon_i = 0,1} v_1^{\varepsilon_1} \ldots v_n^{\varepsilon_n} w_n^{\varepsilon_n} \ldots w_1^{\varepsilon_1} w_q \ldots w_1$$

$$= \sum_{\varepsilon_i = 0,1} v_1^{\varepsilon_1} \ldots v_n^{\varepsilon_n} w_n^{\varepsilon_n} \ldots w_{q+1}^{\varepsilon_{q+1}} w_q^{\varepsilon_q + 1} \ldots w_1^{\varepsilon_1 + 1} (-1)^{\frac{q(q-1)}{2}}$$

con $\varepsilon_i + 1 \in \mathbb{Z}/2\mathbb{Z}$ y, por ser $q \equiv 0\ (4)$, es $(-1)^{\frac{q(q-1)}{2}} = 1$.

Utilizando la definición de los w_i a partir de los t_i dada en la proposición 3.19, obtenemos que el elemento $z\, w_q \ldots w_1$ es suma de términos del tipo:

$$v_{i_1} \ldots v_{i_k} \Big(\sum_{q+1 \le j_1 < \ldots < j_\ell \le n} v_{j_1} \ldots v_{j_\ell}\, t_{j_\ell} \ldots t_{j_1} \Big)\, t_{i'_{k'}} \ldots t_{i'_1}$$

con $1 \le i_1 < \ldots < i_k \le q$ y $1 \le i'_1 < \ldots < i'_{k'} \le q$. Si $k = k'$, la componente en L de este término es, por el lema 3.22, igual a la suma, para $q+1 \le j_1 < \ldots < j_\ell \le n$, de los menores de filas $i_1, \ldots i_k, j_1, \ldots j_\ell$ y columnas $i'_1, \ldots i'_k, j_1, \ldots j_\ell$ de la matriz MP. Si J es la matriz.

$$J = \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix} \begin{matrix} q \\ n-q \end{matrix}$$

esta suma es igual al determinante de la submatriz de MP + J formada por las filas $i_1, \ldots i_k, q+1, \ldots n$ y columnas $i'_1, \ldots i'_k, q+1, \ldots, n$, por el lema 3.23.

Veamos ahora cuales son los términos con $k = k'$. Para ello calculamos $w_q^{\varepsilon_q + 1} \ldots w_1^{\varepsilon_1 + 1}$ en función de los vectores t, para los distintos valores de $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_q$. Teniendo en cuenta la definición de los w (prop. 3.19) se obtiene que el elemento

$w_4^{\varepsilon_4+1} \; w_3^{\varepsilon_3+1} \; w_2^{\varepsilon_2+1} \; w_1^{\varepsilon_1+1}$ es igual a:

a) t_j, si j es el único elemento de {1,2,3,4} con $\varepsilon_j = 1$.

b) $\pm \, t_{j_4} \, t_{j_3}$, si es $\varepsilon_j = 1$ para dos valores $j_1 < j_2$ de j en {1,2,3,4}, siendo $j_3 < j_4$ y $\{j_1, j_2, j_3, j_4\} = \{1,2,3,4\}$. El signo es + si $(j_1, j_2) = (1,2)$, (2,3) ó (3,4), - en los demás casos.

c) $- \, t_{j_3} \, t_{j_2} \, t_{j_1}$ si es $\varepsilon_j = 1$ para tres valores $j_1 < j_2 < j_3$ de j en {1,2,3,4}.

d) $t_4 \, t_3 \, t_2 \, t_1$ si es $\varepsilon_j = 0$ para todo j = 1,2,3,4.

e) 1 si es $\varepsilon_j = 1$ para todo j = 1,2,3,4.

Son válidos los mismos resultados sustituyendo cada j = 1,2,3,4 por $4i+j$ para $i = 1, \ldots, \frac{q}{4} - 1$.

A partir de aquí, viendo cuando es el elemento $w_q^{\varepsilon_q+1} \ldots w_1^{\varepsilon_1+1}$ producto de un número de vectores t igual a $\sum_{i=1}^{q} \varepsilon_i$, se obtiene el resultado enunciado en la proposición respecto a las reglas de formación de las matrices C. Observando en que casos aparece un signo -, se deduce el valor de $\delta_C(i)$. #

Podemos ahora dar explícitamente la solución del problema de inmersión en función de la matriz MP.

Teorema 3.24. Sea $(x_1, x_2, \ldots, x_n)$ una base de F sobre K. Sean $s_1, s_2, \ldots, s_n$ elemento de G tales que $F^{s_1} = F, F^{s_2}, \ldots, F^{s_n}$ sean todos los conjugados de F y sea M la matriz de $M_n(L)$ definida por:

$$M = (x_j^{s_i}) \quad 1 \leq i \leq n$$
$$1 \leq j \leq n$$

Sea T la matriz de Q_F, forma cuadrática traza de $F|K$, en la base $(x_1, x_2, \ldots, x_n)$.

Si Q_F es equivalente sobre K a la forma cuadrática

$$Q_q = -(X_1^2 + X_2^2 + \ldots + X_q^2) + X_{q+1}^2 + \ldots + X_n^2, \text{ con } q \equiv 0 \ (4),$$

sea $P \in M_n(K)$ tal que $P^t T P = S_q$, dónde $S_q = (s_{ij})$ con:

$s_{ii} = -1$, $i = 1, \ldots, q$; $s_{ii} = +1$, $i = q+1, \ldots, n$; $s_{ij} = 0$, $i \neq j$ y elegida tal que el elemento z de $C_L(Q_F)$ sea no nulo.

Entonces la solución general al problema de inmersión dado por $\tilde{G} \longrightarrow G = Gal(L|K)$ es:

$$L\ (\sqrt{r\gamma})$$

donde $r \in K^*$ y γ es el elemento de L^* dado por:

$$\gamma = \sum_C (-1)^{\delta(C)} \det C \ ,$$

dónde el subconjunto de submatrices de la matriz $MP + J$ recorrido por C y el valor de $\delta(C)$ son los determinados en la proposición 3.22.

Demostración. Por ser z no nulo, es invertible (3.10) y por tanto N(z) es no nula. Teniendo en cuenta que es:

$$N(z) = 2^n \gamma w_1 w_2 \ldots w_q$$

(3.20), el elemento $2^n \gamma$ es la única coordenada no nula de N(z)

en la base $\{w_1^{\varepsilon_1}, w_2^{\varepsilon_2} \ldots w_n^{\varepsilon_n}\}_{\varepsilon_i=0,1}$ de $C_L(Q_F)$. Por 3.15, $2^n\gamma$, y por tanto γ, da una solución al problema de inmersión y la solución general es:

$$L(\sqrt{r\gamma}), \quad \text{con } r \in K^*. \ \#$$

Obsérvese que si q es 0, la expresión del elemento γ dada en 3.24 se reduce a un único sumando igual a det (MP + I). El teorema 3.24 generaliza pues el 3.17 que daba la solución en el caso en que Q_F es equivalente a la identidad sobre K.

Caso K = Q.

Veamos ahora que, en el caso en que K es el cuerpo Q de los racionales, el teorema 3.24 da en todos los casos la solución al problema de inmersión.

En efecto, sean r_1, $r_2 \geq 0$ tales que $\mathbb{R} \otimes E \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Entonces ([$S_3$] 3.4), son equivalentes:

a) $d_F = 1$ y el problema de inmersión es resoluble.

b) $r_2 \equiv 0 \pmod 4$ y Q_F equivalente sobre Q a Q_{r_2}, siendo

$$Q_{r_2} = -(X_1^2 + X_2^2 + \ldots + X_{r_2}^2) + X_{r_2+1}^2 + \ldots + X_n^2 .$$

Por tanto, si nos situamos en el caso $d_F = 1$, un problema de inmersión:

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow Q & & \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \tilde{G} & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

es resoluble si y sólo si Q_F es equivalente sobre Q a la forma:

$$Q_{r_2} = -(X_1^2 + X_2^2 + \ldots + X_{r_2}^2) + X_{r_2+1}^2 + \ldots + X_n^2$$

con $r_2 \equiv 0 \pmod 4$. Por tanto, la solución viene dada explícitamente por el teorema 3.24.

Ejemplo.

Para el grupo de Mathieu M_{12}, Matzat y Zeh dan una realización sobre Q, especializando en valores enteros $t \equiv 1 \pmod{66}$ una realización de M_{12} sobre Q(T) dada por un polinomio irreducible de grado 12, de discriminante un cuadrado ([MA-Z]).

Haciendo operar M_{12} sobre las 12 raices del polinomio, obtenemos pues un morfismo:

$$e: M_{12} \longrightarrow A_{12} .$$

Sea Θ una raíz del polinomio en una clausura algebraica $\bar{Q}$ de Q. Sea $F = Q(\Theta)$. Sea Q_F la forma traza de F sobre Q.

Tenemos $w(Q_F) = 1$ para t cumpliendo $t \geq -197$, $t \equiv 1 \pmod 4$ y $d_1(t) = 5^{15}\, t^2 - 2^{22}\, 3^{18}$ primo. Además, se tiene entonces $r_1(t) = 4$ ([B-LL-V]).

Tenemos pues $12 = r_1 + 2r_2$ y $r_1 = 4$, por tanto $r_2 = 4$ y Q_F es equivalente sobre Q a la forma:

$$Q_4 = -(X_1^2 + X_2^2 + X_3^2 + X_4^2) + X_5^2 + \ldots + X_{12}^2 .$$

Si T es la matriz de Q_F en la base $(1, \Theta, \ldots, \Theta^{11})$ de F sobre Q y $\Theta_1 = \Theta, \Theta_2, \ldots, \Theta_{12}$ son las 12 raíces del polinomio, sea M la matriz dada por:

$$M = (\theta_i^j)_{1 \leq i \leq 12}$$
$$0 \leq j \leq 11 .$$

Sea P una matriz de cambio de Q_F a Q_4 sobre Q.

Aplicando el teorema 3.24, se obtiene el elemento γ que da la solución al problema de inmersión como suma de los determinantes de 14 submatrices de la matriz MP + J afectados de los signos correspondientes.

BIBLIOGRAFIA

A-T - E. Artin, J. Tate; Class Field Theory. Benjamin, 1967.

B-LL-V - P. Bayer, P. Llorente, N. Vila; $\tilde{M}_{12}$ comme groupe de Galois sur Q. C.R. Acad. Sc. Paris. t. 303, I,7 (1986), 277-280.

BO_1 - N. Bourbaki; Elements de Mathématique, Algèbre Chap 5. Hermann, 1967.

BO_2 - N. Bourbaki; Elements de Mathématique, Algèbre Cap 9. Hermann, 1959.

G-D - A. Grothendieck, J.A. Dieudonné; Elements de Géométrie Algébrique I. Springer, 1971.

G - Séminaire de Géométrie Algébrique du Bois Marie 1960/61. SGA 1; Revêtements Etales et Groupe Fondamental. Springer, 1971.

GO - L.J. Goldstein; Analitic Number Theory. Prentice-Hall, 1971.

H - H. Hasse; Existenz und Mannigfaltigkeit abelscher Algebren mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers. Math. Nach. I(1948), 40-61.

HA - R. Hartshorne; Algebraic Geometry. Springer, 1977.

HO - K. Höchsmann; Zum Einbettungsproblem. J. Crelle, 229 (1962), 81-106.

I - M. Ikeda; Zur Existenz eigentlicher galoischer Körper beim Einbettungsproblem für galoische Algebren. Abh. Math. Sem. Univ. Hamburg, 24 (1960), 126-131.

L - S. Lang; Rapport sur la Cohomologie des Groupes. Benjamin, 1966.

LA - T.Y. Lam; The Algebraic Theory of Quadratic Forms. Benjamin, 1973.

M - J.S. Milne; Etale Cohomology. Princeton, 1980.

MA-Z - B.M. Matzat, A. Zeh; Realisierung der Mathieugruppen M_{11} und M_{12} als Galoisgruppen über Q. J. Number Theory 23(1986), 195-202.

MS - R. Massy; Formules de construction de p-extensions galoisiennes. C.R. Acad. Sc. Paris, t. 303, I, 13(1986), 591-594.

N_1 - J. Neukirch; Etaltopologie, Etale Garben. Universität Regensburg, 1975-76.

N_2 - J. Neukirch; Uber das Einbettungsproblem der algebraischen Zahlentheorie. Invent. math. 21 (1973), 59-116.

N_3 - J. Neukirch; Einbettungsprobleme mit lokale Vorgabe. J. Crelle 259 (1973), 1-47.

O - O.T. O'Meara; Introduction to Quadratic Forms. Springer, 1973.

S_1 - J.P. Serre; Aplications algébriques de la cohomologie des groupes. Séminaire H. Cartan, E.N.S., 1950-51.

S_2 - J.P. Serre; Local Fields. Springer, 1979.

S_3 - J.P. Serre; L'invariant de Witt de la forme $Tr(x^2)$. Comment. Math. Helvetici 59 (1984), 651-676.

S_4 - J.P. Serre; Cohomologie Galoisienne. Springer, 1986.

SP - T.A. Springer; On the equivalence of Quadratic Forms. Proc. Neder. Acad. Sc. 62 (1959), 241-253.

T - G. Tamme; Einführung in die étale Kohomologie. Mathematisches Institut der Universität Göttinger, 1975-76.

W - E. Witt; Konstruktion von Körpern zu vorgegebener Gruppe der Ordnung p^f. J. Crelle 174 (1936), 237-245.