COHOMOLOGÍA GALOISIANA

MARIANO SUÁREZ-ÁLVAREZ

Índice

I. El teorema 90 de Hilbert

Si G y A son grupos, y supongamos que G actúa sobre A por automorfismos de grupos, de manera que tenemos una función

$$(g, a) \in G \times A \longmapsto {}^g a \in A$$

tal que para cada g, $h \in G$ y cada a, $b \in A$ es

$${}^g({}^h a) = {}^{gh} a, \qquad {}^{1_G} a = a, \qquad {}^g e_A = 1_A, \qquad {}^g(a \cdot b) = {}^g a \cdot {}^g b.$$

Decimos que una función $\phi : G \to A$ es un **1-*cociclo de G con valores en A*** si para cada g, $h \in G$ se tiene que

$$\phi(gh) = \phi(g) \cdot {}^g\phi(h),$$

y escribimos $Z^1(G, A)$ al conjunto de todos los 1-cociclos de G con valores en A. Si ϕ, $\psi \in Z^1(G, A)$ son dos 1-cociclos, decimos que ϕ y ψ son ***cohomólogos*** si existe $a \in A$ tal que

$$\phi(g) = a^{-1} \cdot \psi(g) \cdot {}^g a$$

para todo $g \in G$, y en ese caso escribimos $\phi \sim \psi$.

Lema 1. *La relación de cohomología es una relación de equivalencia en el conjunto $Z^1(G, A)$ de los 1-cociclos.*

Date: 22 de agosto, 2014.

Demostración. Que la relación es reflexia es evidente.

Si ϕ, $\psi \in Z^1(G, A)$ son dos 1-cociclos tales que $\phi \sim \psi$, de manera que existe $a \in A$ tal que $\phi(g) = a^{-1} \cdot \psi(g) \cdot {}^g a$ para todo $g \in G$, entonces poniendo $b = a^{-1}$ tenemos que $\psi(g) = b^{-1} \cdot \phi(g) \cdot {}^g b$ para todo $g \in G$, esto eso, que $\psi \sim \phi$.

Finalmente si ϕ, ψ, $\omega \in Z^1(G, A)$ son 1-cociclos tales que $\phi \sim \psi$ y $\psi \sim \omega$, de manera que existen a, $b \in A$ tales que $\phi(g) = a^{-1} \cdot \psi(g) \cdot {}^g a$ y $\psi(g) = b^{-1} \cdot \omega(g) \cdot {}^g b$, entonces $\phi(g) = (ab)^{-1} \cdot \omega(g) \cdot {}^g(ab)$ para todo $g \in G$, esto es, vale que $\phi \sim \omega$. □

En vista de este lema, podemos considerar el conjunto cociente $Z^1(G, A)/\sim$, al que llamamos el ***primer conjunto de cohomología de G con valores en A*** y escribimos $H^1(G, A)$. Es inmediato verificar que la función $\phi : G \to A$ tal que $\phi(g) = 1_A$ para todo $g \in G$ es un 1-cociclo, al que llamamos ***trivial***; en particular, $Z^1(G, A)$ nunca es un conjunto vacío y, en consecuencia, tampoco lo es $H^1(G, A)$. A la clase de equivalencia en $H^1(G, A)$ de este 1-cociclo trivial la denotaremos simplemente 0. Cuando sea ése el único elemento de $H^1(G, A)$ —es decir, cuando todos los 1-cociclos son cohomólogos al 1-cociclo trivial— escribiremos $H^1(G, A) = 0$.

Notemos que un 1-cociclo $\phi : G \to A$ es cohomólogo al 1-cociclo trivial si y solamente si existe $a \in A$ tal que

$$\phi(g) = a^{-1} \cdot {}^g a$$

para todo $g \in G$. La anulación de $H^1(G, A)$ es equivalente a que todos los cociclos sean de esta forma.

El *Teorema 90* de Hilbert describe este conjunto de cohomología en una situación muy especial. Consideremos una extensión de cuerpos E/K finita y galoisiana, y sea $G = \mathsf{Gal}(E/K)$ su grupo de Galois. Para cada $g \in G$ y cada $x \in E$ escribimos ${}^g x = g(x)$. Obtenemos de esta forma una acción

$$(g, x) \in G \times E^\times \longmapsto {}^g x \in E^\times$$

de G sobre el grupo multiplicativo $E^\times$.

Teorema 2 (Teorema 90 de Hilbert)**.** *Si E/K es una extensión galoisiana y finita de grupo de Galois $G = \mathsf{Gal}(E/K)$, entonces $H^1(G, E^\times) = 0$.*

En el caso en que la extensión es cíclica éste es, en un lenguaje moderno, el *Satz 90* del *Zahlbericht* [Hil98] de David Hilbert, y de ahí es que viene el nombre con el que este resultado es universalmente conocido; ese caso era conocido, de todas formas, por Ernst Kummer mucho tiempo antes [Kum55, Kum26]. El caso de una extensión galoisiana arbitraria es debido a Emmy Noether [Noe33].

Demostración. Sea $\phi : G \to E^\times$ un 1-cociclo. El teorema de Dedekind sobre la independencia lineal carácteres [Art59, II.§F. Corollary] nos dice que G, visto como un subconjunto del E-espacio vectorial de las funciones $E^\times \to E$, es linealmente independendiente. En particular, la combinación lineal $\sigma = \sum_{g \in G} \phi(g) g$ es un elemento no nulo de ese espacio vectorial y existe entonces $x \in E^\times$ tal que $\sigma(x) \neq 0$. Pongamos $y = \sigma(x)$.

Si $g \in G$, entonces

$$ {}^g y = {}^g\left(\sum_{h\in G} \phi(h)\cdot {}^h x\right) = \sum_{h\in G} {}^g\phi(h)\cdot {}^{gh}x $$

y, como ϕ es un 1-cociclo, esto es

$$ \begin{aligned} &= \sum_{h\in G} \phi(g)^{-1}\cdot\phi(gh)\cdot {}^{gh}x \\ &= \phi(g)^{-1}\cdot y, \end{aligned} $$

de manera que $\phi(g) = y\cdot {}^g y^{-1}$. Esto nos dice, precisamente, que ϕ es cohomólogo al 1-cociclo trivial. □

Sea, como antes, E/K una extensión galoisiana finita y sea $G = \mathsf{Gal}(E/K)$ su grupo de Galois. Fijemos $n \geq 1$, sea $\mathsf{M}_n(E)$ el E-espacio vectorial de las matrices $n\times n$ con entradas en E y sea $\mathsf{GL}(n,E) \subset \mathsf{M}_n(E)$ el subconjunto de las matrices inversibles; recordemos que $\mathsf{GL}(n,E)$ es un grupo con respecto a la multiplicación matricial.

Lema 3. *Sea E/K una extensión galoisiana finita y sea $G = \mathsf{Gal}(E/K)$ su grupo de Galois.*

(*i*) *El grupo G actúa sobre el grupo $\mathsf{GL}(n,E)$ de manera que para cada $g\in G$ y cada matriz $m = (m_{i,j}) \in \mathsf{GL}(n,E)$ la matriz ${}^g m$ tiene entradas*

$$ ({}^g m)_{i,j} = {}^g m_{i,j} $$

para cada i, $j \in \{1,\dots,n\}$.

(*ii*) *El grupo G actúa sobre el grupo abeliano E^n de manera que para cada $g\in G$ y cada vector $x = (x_1,\dots,x_n)\in E^n$ es ${}^g x = ({}^g x_1,\dots,{}^g x_n)$.*

(*iii*) *Estas acciones de G sobre $\mathsf{GL}(n,E)$ y sobre E son compatibles, en el sentido de que para cada $g\in G$, $u\in\mathsf{GL}(n,E)$ y $x\in E^n$ vale que*

$$ {}^g(m\cdot x) = {}^g m\cdot {}^g x. $$

Demostración. Hacer. □

En la situación del lema, el grupo $\mathsf{GL}(1,E)$ se identifica de manera obvia con el grupo multiplicativo $E^\times$, y es claro que las acciones del grupo de Galois G sobre $\mathsf{GL}(1,E)$ y sobre $E^\times$ se corresponden. Esto muestra que el siguiente resultado es una generalización del Teorema 2:

Teorema 4. *Si E/K es una extensión galoisiana y finita de grupo de Galois $G = \mathsf{Gal}(E/K)$ y $n\geq 1$, entonces $H^1(G,\mathsf{GL}(n,E)) = 0$.*

Demostración. Sea $\phi : G\to\mathsf{GL}(n,E)$ un 1-cociclo de G con valores en $\mathsf{GL}(n,K)$. Consideremos la función $\sigma : E^n\to E^n$ tal que para cada $x\in E^n$ es

$$ \sigma(x) = \sum_{g\in G}\phi(g)\cdot {}^g x $$

y mostremos, para empezar, que

una función E-lineal $\lambda : E^n\to E$ tal que $\lambda\circ\sigma = 0$ se anula idénticamente. (1) {eq:cl-90}

Sea para eso $\lambda : E^n \to E$ una función E-lineal tal que $\lambda \circ \sigma = 0$. Fijemos $x \in E^n$. Para cada $y \in E^\times$ es

$$0 = \lambda(\sigma(yx)) = \sum_{g\in G} \lambda(\phi(g) \cdot {}^g(yx)) = \sum_{g\in G} \lambda(\phi(g) \cdot {}^g x) \cdot {}^g y,$$

y esto nos dice que $\sum_{g\in G} \lambda(\phi(g) \cdot {}^g x)g$ es la función $E^\times \to E$ nula. El teorema de Dedekind sobre la independencia lineal de carácteres implica entonces que $\lambda(\phi(g) \cdot {}^g x) = 0$ para todo $g \in G$. En particular, si $z \in E^n$ podemos tomar $x = \phi(1_G)^{-1} \cdot z$ y $g = 1_G$ en esta igualdad para ver que $\lambda(z) = 0$. Esto prueba (1).

Una consecuencia inmediata de esa observación es que la imagen de la función σ genera a E^n como E-espacio vectorial y, en particular, que existen $x_1, \ldots, x_n \in E^n$ tales que $\{\sigma(x_1), \ldots, \sigma(x_n)\}$ es una base de E^n como E-espacio vectorial. Hay entonces una matriz $m \in \mathsf{GL}(n, E)$ cuyas columnas son, en orden, $x_1, \ldots, x_n$, y podemos considerar $a = \sum_{g\in G} \phi(g) \cdot {}^g m$, que es un elemento de $\mathsf{M}_n(E)$.

Sea $\{e_1, \ldots, e_n\}$ la base estándard de E^n. Si $i \in \{1, \ldots, n\}$ es

$$a \cdot e_i = \sum_{g\in G} \phi(g) \cdot {}^g m \cdot e_i = \sum_{g\in G} \phi(g) \cdot {}^g(m \cdot e_i) = \sum_{g\in G} \phi(g) \cdot {}^g x_i = \sigma(x_i).$$

Así, el conjunto $\{a \cdot e_1, \ldots, a \cdot e_n\}$ es una base de E^n y, en consencuencia, la matriz a es inversible, esto es, pertenece a $\mathsf{GL}(n, E)$.

Si $g \in G$, entonces

$${}^g a = {}^g\left(\sum_{h\in G} \phi(h) \cdot {}^h m\right) = \sum_{h\in G} {}^g\phi(h) \cdot {}^{gh} m$$

y, como ϕ es un 1-cociclo, esto es

$$\begin{aligned} &= \sum_{h\in G} \phi(g)^{-1} \cdot \phi(gh) \cdot {}^{gh} m \\ &= \phi(g)^{-1} \cdot a, \end{aligned}$$

de manera que, $\phi(g) = a \cdot {}^g a^{-1}$. Esto nos dice, precisamente, que ϕ es cohomólogo al 1-cociclo trivial. □

II. Álgebras

§1. Álgebras y morfismos de álgebras

Sea K un cuerpo. Una ***K-álgebra*** es K-espacio vectorial A dotado de una función K-bilineal $\mu_A : A \times A \to A$ que hace del grupo abeliano subyacente a A un anillo unitario. Si $x, y \in A$, escribimos $x \cdot y$ o simplemente xy en lugar de $\mu_A(x, y)$. Usando esta notación, las condiciones que imponemos sobre μ_A son las siguientes:

- la función μ_A es K-bilineal: para todo $x, x', y \in A$ y todo $a \in K$ es

$$\begin{aligned} &(x + x') \cdot y = x \cdot y + x' \cdot y, \\ &y \cdot (x + x') = y \cdot x + y \cdot x', \\ &(ax) \cdot y = a(x \cdot y) = x \cdot ay; \end{aligned}$$

- la función μ_A es asociativa: para todo x, y, $z \in A$ es
$$x \cdot (y \cdot z) = (x \cdot y) \cdot z;$$
- el producto μ_A es unitario: existe un elemento $1_A \in A$ tal que para todo $x \in A$ es
$$x \cdot 1_A = x = 1_A \cdot x.$$

Si A y B son K-álgebras, un ***morfismo de K-álgebras*** es una función K-lineal $f : A \to B$ que es un homomorfismo de anillos unitarios. Explicitamente, esto significa que se tiene

$$\begin{aligned} f(ax + by) &= af(x) + bf(y), \\ f(x \cdot y) &= f(x) \cdot f(y), \\ f(1_A) &= 1_B \end{aligned}$$

cualesquiera sean x, $y \in A$ y a $b \in K$. Si además la función f es biyectiva, decimos que f es un ***isomorfismo de K-álgebras*** y si, más aún, las K-álgebras A y B son la misma, que f es un ***automorfismo de K-álgebras***.

§2. Constantes de estructura

Sea K un cuerpo, sea A una K-álgebra de dimensión finita y sea $\mathscr{B} = (x_i)_{i\in I}$ una base de A como K-espacio vectorial. Si i, $j \in I$, entonces existe una única familia $(\gamma_{i,j}^k)_{k\in I}$ de elementos de K tal que

$$x_i \cdot x_j = \sum_{k\in I} \gamma_{i,j}^k x_j.$$

Llamamos a la familia $C_{\mathscr{B}}(A) = (\gamma_{i,j}^k)_{i,j,k\in I}$ de elementos de K la ***tabla de constantes de estructura*** de A con respecto a la base $\mathscr{B}$.

Esta tabla $C_{\mathscr{B}}(A)$ determina completamente a la función $\mu_A : A \times A \to A$. En efecto, si x, $y \in A$ son dos elementos y $(a^i)_{i\in I}$, $(b^i)_{i\in I}$ son las coordenadas de x e y con respecto a $\mathscr{B}$, de manera que $x = \sum_{i\in I} a^i x_i$ e $y = \sum_{i\in I} b^i x_i$, se tiene que

$$\begin{aligned} \mu_A(x, y) &= \mu_A\Big(\sum_{i\in I} a^i x_i, \sum_{j\in I} b^j x_j\Big) \\ &= \sum_{i,j\in I} a^i b^j \mu_A(x_i, x_j) && \text{ya que } \mu \text{ es } K\text{-bilineal} \\ &= \sum_{i,j,k\in I} a^i b^j \gamma_{i,j}^k x_k \end{aligned}$$

en vista de la definición de las constantes de estructura. Como la multiplicación de un álgebra queda determinada por su tabla de constantes de estructura, es razonable esperar que las condiciones que impusimos sobre aquélla pudan expresarse en términos de ésta —ése es el contenido de la siguiente proposición.

Proposición 5. *Sean K un cuerpo, A un K-espacio vectorial de dimensión finita y $\mathscr{B} = (x_i)_{i\in I}$ una base de A como K-espacio vectorial. Sea $C = (\gamma_{i,j}^k)_{i,j,k\in I}$ una familia de elementos de K indexados por $I \times I \times I$. Entonces existe una multiplicación*

$\mu_A : A \times A \to A$ que hace de A una K-álgebra y tal que $C_{\mathscr{B}}(A) = C$ si y solamente si

- *para cada i, j, $k \in I$ se tiene que*
$$\sum_{l\in I} \gamma_{i,j}^l \gamma_{l,k}^r = \sum_{l\in I} \gamma_{i,l}^r \gamma_{j,k}^l \tag{2}$$ {eq:st-alg:1}
- *y existe una familia $(u^i)_{i\in I}$ de elementos de K tal que*
$$\sum_{i\in I} u^i \gamma_{i,j}^k = \delta_j^k = \sum_{i\in I} u^i \gamma_{j,i}^k. \tag{3}$$ {eq:st-alg:2}
para todo j, $k \in I$.

Demostración. Hacer. □

Dada una K-álgebra A, la tabla $C_{\mathscr{B}}(A)$ de las constantes de estructura de A con respecto a una base $\mathscr{B}$ depende efectivamente de $\mathscr{B}$ y no solamente del álgebra A. Podemos describir esta dependencia de forma precisa:

Proposición 6. *Sea K un cuerpo y sea A una K-álgebra de dimensión finita. Sean $\mathscr{B} = (x_i)_{i\in I}$ y $\mathscr{B}' = (x'_i)_{i\in I}$ dos bases de A como K-espacio vectorial y sea $(c_i^j)_{i,j\in I} \in M_I(K)$ la matriz de cambio de base de $\mathscr{B}$ a $\mathscr{B}'$, de manera que para cada $i \in I$ es $x'_i = \sum_{j\in I} c_i^j x_j$. Si $C_{\mathscr{B}}(A) = (\gamma_{i,j}^k)_{i,j,k\in I}$ y $C_{\mathscr{B}'}(A) = (\gamma_{i,j}'^k)_{i,j,k\in I}$ son las tablas de constantes de estructura de A con respecto a $\mathscr{B}$ y a $\mathscr{B}'$, respectivamente, entonces para cada i, j, $k \in I$ se tiene que*
$$\sum_{r,s\in I} c_i^r c_j^s \gamma_{r,s}^k = \sum_{t\in I} \gamma_{i,j}'^t c_t^k$$

Demostración. Hacer. □

De la misma manera que podemos expresar las condiciones que determinan a un álgebra en términos de sus constantes de estructura, podemos expresar las condiciones que hacen que una función lineal entre dos álgebras sea un morfismo de álgebras en términos de su matriz.

Proposición 7. *Sea K un cuerpo, sean A y B dos K-álgebras de dimensión finita, sean $\mathscr{B}_A = (x_i)_{i\in I}$ y $\mathscr{B}_B = (y_u)_{u\in U}$ bases de A y de B como K-espacios vectoriales. Sean $C_{\mathscr{B}_A}(A) = (\gamma_{i,j}^k)_{i,j,k\in I}$ y $C_{\mathscr{B}_B}(B) = (\eta_{u,v}^w)_{u,v,w\in U}$ las tablas de constantes de estructura de A y de B respecto de $\mathscr{B}_A$ y de $\mathscr{B}_B$, respectivamente, y sean $(r^i)_{i\in I}$ y $(s^j)_{j\in J}$ las coordenadas de 1_A y de 1_B con respecto a $\mathscr{B}_A$ y a $\mathscr{B}_B$, de manera que $1_A = \sum_{i\in I} r^i x_i$ y $1_B = \sum_{u\in U} s^u y_u$. Sea finalmente $f : A \to B$ una función K-lineal y $(f_i^u)_{i\in I, u\in U} \in M_{I,U}(K)$ la matriz de f con respecto a las bases $\mathscr{B}_A$ y $\mathscr{B}_B$, de manera que $f(x_i) = \sum_{u\in U} f_i^u y_u$ para cada $i \in I$. Entonces la función f es un morfismo de K-álgebras si y solamente si*
$$\sum_{u,v\in U} f_i^u f_j^v \eta_{u,v}^w = \sum_{k\in I} \gamma_{i,j}^k f_k^w$$
para cada i, $j \in I$ y cada $w \in U$ y
$$\sum_{i\in U} r^i f_i^u = s^u$$

para cada $u \in U$.

Demostración. Hacer. □

Corolario 8. *Sea K un cuerpo, sean A y B K-álgebras de dimensión finita, sean $\mathscr{B}_A = (x_i)_{i\in I}$ y $\mathscr{B}_b = (y_i)_{i\in I}$ bases de A y de B como K-espacios vectoriales indexadas por el mismo conjunto I, y sean $C_{\mathscr{B}_A}(A)$ y $C_{\mathscr{B}_B}(B)$ las tablas de constantes de estructura de A y de B con respecto a $\mathscr{B}_A$ y a $\mathscr{B}_B$, respectivamente. La función K-lineal $f : A \to B$ tal que $f(x_i) = y_i$ para todo $i \in I$ es un isomorfismo de K-álgebras si y solamente si $C_{\mathscr{B}_A}(A) = C_{\mathscr{B}_B}(B)$.*

Demostración. Hacer. □

§3. Extensión de escalares

Proposición 9. *Sea E/K una extensión de cuerpos, sea A una K-álgebra de dimensión finita, sea $\mathscr{B} = (x_i)_{i\in I}$ una base de A como K-espacio vectorial y sea $C_{\mathscr{B}}(A) = (\gamma_{i,j}^k)_{i,j,k\in I}$ la tabla de constantes de estructura de A con respecto a $\mathscr{B}$. Sea $\bar{\mathscr{B}} = (\bar{x}_i)_{i\in I}$ una familia de símbolos nuevos tales que $\bar{x}_i \neq \bar{x}_j$ si $i, j \in I$ son distintos, y sea $A_{\mathscr{B}}^E$ el E-espacio vectorial que tiene a $\bar{\mathscr{B}}$ como base. Existe una única estructura de E-álgebra sobre $A_{\mathscr{B}}^E$ tal que $C_{\bar{\mathscr{B}}}(A_{\mathscr{B}}^E) = C_{\mathscr{B}}(A)$.*

Notemos que lo que afirma esta proposición tiene sentido: como $K \subseteq E$, la tabla de constantes de estructura $C_{\mathscr{B}}(A)$ es una posible tabla de constantes de estructura de una E-álgebra

Demostración. Basta que verifiquemos que se cumplen las condiciones de la Proposición 5 y esto es inmediato, ya que $K \subseteq E$. □

Si E/K es una extensión de cuerpos, A una K-álgebra de dimensión finita y $\mathscr{B}$ una base de A como K-espacio vectorial, decimos que la E-álgebra $A_{\mathscr{B}}^E$ construida en este lema se obtiene de A ***por extensión de escalares de K a E con respecto a $\mathscr{B}$***. Esta E-álgebra depende claramente de la base $\mathscr{B}$ usada para construirla, pero cambiar la base no cambia la clase de isomorfismo del álgebra obtenida:

Proposición 10. *Sea E/K una extensión de cuerpos y sea A una K-álgebra de dimensión finita. Si $\mathscr{B}$ y $\mathscr{B}'$ son dos bases de A como K-espacio vectorial, entonces las E-álgebras $A_{\mathscr{B}}^E$ y $A_{\mathscr{B}'}^E$ son isomorfas.*

Demostración. Supongamos que las bases del enunciado del lema son $\mathscr{B} = (x_i)_{i\in I}$ y $\mathscr{B}' = (x_i')_{i\in I}$, que $(c_i^j)_{i,j\in I} \in M_I(K)$ es la matriz de cambio de base de $\mathscr{B}$ a $\mathscr{B}'$, de manera que para cada $i \in I$ es $x_i' = \sum_{j\in I} c_i^j x_j$, y que $C_A(\mathscr{B}) = (\gamma_{i,j}^k)_{i,j,k\in I}$ y $C_A(\mathscr{B}') = (\gamma_{i,j}'^k)_{i,j,k\in I}$ son las tablas de constantes de estructura de A con respecto a $\mathscr{B}$ y a $\mathscr{B}'$, respectivamente. Sean $\bar{\mathscr{B}} = (\bar{x}_i)_{i\in I}$ y $\bar{B}' = (\bar{x}_i')_{i\in I}$ las bases de $A_{\mathscr{B}}^E$ y de $A_{\mathscr{B}'}^E$ usadas para construir estas E-álgebras y sea $f : A_{\mathscr{B}'}^E \to A_{\mathscr{B}}^E$ la función E-lineal tal que para

$$f(\bar{x}_i') = \sum_{j\in I} c_i^k \bar{x}_i$$

para cada $i \in I$. Para probar el lema bastará que mostremos que f es un isomorfismo de E-álgebras.

De la Proposición 6 sabemos que para cada i, j, $k \in I$ es

$$\sum_{r,s\in I} c_i^r c_j^s \gamma_{r,s}^k = \sum_{t\in I} \gamma_{i,j}'^r c_t^k. \tag{4}$$ {eq:wdf:1}

Por otro lado, si $(e^i)_{i\in I}$ y $(e'^i)_{i\in I}$ son las coordenadas de 1_A con respecto a las bases $\mathscr{B}$ y $\mathscr{B}'$, respectivamente, de manera que $1_A = \sum_{i\in I} e^i x_i = \sum_{i\in I} e'^i x_i'$, tenemos que para cada $i \in I$ es

$$\sum_{j\in I} e'^j c_j^i = e^i.$$

En vista de esta ecuación y de (4), la Proposición 7 nos permite concluir que f es un morfismo de E-álgebras. La matriz de f con respecto a las bases $\bar{\mathscr{B}}'$ y $\bar{\mathscr{B}}$ es la matriz $(c_i^j)_{i,j\in I}$ de cambio de base de $\mathscr{B}$ a $\mathscr{B}'$, que tiene determinante no nulo: esto implica que el morfismo f es, de hecho, un isomorfismo. □

Proposición 11. *Sea E/K una extensión de cuerpos, sea A una K-álgebra de dimensión finita, sea $\mathscr{B} = (x_i)_{i\in I}$ una base de A como K-espacio vectorial, sea $A_{\mathscr{B}}^E$ la E-álgebra obtenida por extensión de escalares de K a E con respecto a $\mathscr{B}$ y sea $\bar{\mathscr{B}} = (\bar{x}_i)_{i\in I}$ la base usada para construirla. La función K-lineal $\iota : A \to A_{\mathscr{B}}^E$ tal que $\iota(x_i) = \bar{x}_i$ para cada $i \in I$ es un morfismo inyectivo de K-álgebras.*

Una situación importante en la que podemos describir la extensión de escalares es la siguiente:

Proposición 12. *Sea E/K una extensión de cuerpos, sea $f \in K[X]$ un polinomio no constante y sea $A = K[X]/(f)$. Si $\mathscr{B}$ es una base de A, entonces hay un isomorfismo $A_{\mathscr{B}}^E \cong E[X]/(f)$.*

Demostración. En vista de la Proposición 10 basta probar que tenemos un isomorfismo para alguna base $\mathscr{B}$ de A. Sea $n = \deg f$, sea x la clase de X en A y sea $I = \{0, \dots, n-1\}$, y consideremos la base $\mathscr{B} = (x^i)_{i\in I}$ de A como K-espacio vectorial. Sea $\bar{\mathscr{B}} = (\overline{x^i})_{i\in I}$ es la base usada para construir $A_{\mathscr{B}}^E$ y sea $\iota : A \to A_{\mathscr{B}}^E$ el morfismo de la Proposición 11. Como ι es un morfismo de anillos, tenemos que $\bar{x}^i = \iota(x)^i = \iota(x^i) = \overline{x^i}$ para cada $i \in I$, y esto nos dice que $\bar{x}$ genera a $A_{\mathscr{B}}^E$ como E-álgebra. En particular, el morfismo de E-álgebras $h : E[X] \to A_{\mathscr{B}}^E$ tal que $h(X) = \bar{x}$ es sobreyectivo.

Como $h(f) = f(\bar{x}) = f(\iota(x)) = \iota(f(x)) = 0$, el ideal (f) generado por f en $E[X]$ está contenido en el núcleo de h, de manera que este morfismo induce un morfismo de E-álgebras $h' : E[X]/(f) \to A_{\mathscr{B}}^E$ que es sobreyectivo porque h lo es. Como

$$\dim_E(E[X]/(f)) = \deg f = \dim_E A = \dim_E A_{\mathscr{B}}^E,$$

el morfismo h' tiene que ser también inyectivo, así que es un isomorfismo. □

De la misma forma que podemos extender escalares en un álgebra, podemos hacerlo con morfismos:

Proposición 13. *Sea E/K una extensión de cuerpos, sean A y B dos K-álgebras y sean $\mathscr{B}_A = (x_i)_{i\in I}$ y $\mathscr{B}_B = (y_u)_{u\in U}$ bases de A y de B como K-espacios vectoriales. Sean $\bar{\mathscr{B}}_A = (\bar{x}_i)_{i\in I}$ y $\bar{\mathscr{B}}_B = (\bar{y}_u)_{u\in U}$ las bases de $A^E_{\mathscr{B}_A}$ y de $B^E_{\mathscr{B}_B}$ usadas para construir estas E-álgebras. Si $f : A \to B$ es un morfismo de K-álgebras y $(f_i^u)_{i\in I,u\in I} \in M_{I,U}(K)$ es su matriz con respecto a las bases $\mathscr{B}_A$ y $\mathscr{B}_B$, de manera que $f(x_i) = \sum_{u\in U} f_i^u y_u$ para cada $i \in I$, entonces existe exactamente un morfismo $f^E_{\mathscr{B}_A,\mathscr{B}_B} : A^E_{\mathscr{B}_A} \to B^E_{\mathscr{B}_B}$ de E-álgebras tal que*

$$f^E_{\mathscr{B}_A,\mathscr{B}_B}(\bar{x}_i) = \sum_{u\in U} f_i^i \bar{y}_u$$

para cada $i \in I$.

Demostración. Hacer. □

La extensión de escalares de morfismos interactúa de forma útil con la composición.

Proposición 14. *Sea E/K una extensión de cuerpos.*

(*i*) *Si A es una K-álgebra de dimensión finita y $\mathscr{B}$ es una base de A como K-espacio vectorial, entonces el morfismo*

$$(\mathsf{id}_A)^E_{\mathscr{B},\mathscr{B}} : A^E_{\mathscr{B}} \to A^E_{\mathscr{B}}$$

que se obtiene por extensión de escalares del morfismo identidad

$$\mathsf{id}_A : A \to A$$

de la K-álgebra A, coincide con el morfismo identidad

$$\mathsf{id}_{A^E_{\mathscr{B}}} : A^E_{\mathscr{B}} \to A^E_{\mathscr{B}}$$

de la E-álgebra $A^E_{\mathscr{B}}$.

(*ii*) *Si A, B y C son K-álgebras de dimensión finita, $\mathscr{B}_A$, $\mathscr{B}_B$ y $\mathscr{B}_C$ son bases de A, de B y de C como K-espacios vectoriales, y $f : A \to B$ y $g : B \to C$ son morfismos de K-álgebras, entonces el morfismo de E-álgebras*

$$(g \circ f)^E_{\mathscr{B}_A,\mathscr{B}_C} : A^E_{\mathscr{B}_A} \to C^E_{\mathscr{B}_C}$$

coincide con la composición

$$g^E_{\mathscr{B}_B,\mathscr{B}_C} \circ f^E_{\mathscr{B}_A,\mathscr{B}_B} : A^E_{\mathscr{B}_A} \to C^E_{\mathscr{B}_C}.$$

Demostración. Hacer. □

Un corolario inmediato de esta última proposición es el siguiente:

Corolario 15. *Sea E/K una extensión de cuerpos, sean A y B dos K-álgebras de dimensión finita y sean $\mathscr{B}_A$ y $\mathscr{B}_B$ bases de A y de B como K-espacios vectoriales. Si $f : A \to B$ es un isomorfismo de K-álgebras, entonces el morfismo $f^E_{\mathscr{B}_A,\mathscr{B}_B} : A^E_{\mathscr{B}_A} \to B^E_{\mathscr{B}_B}$ obtenido por extensión de escalares de K a E es un isomorfismo de E-álgebras.*

Demostración. Sea $g : B \to A$ el isomorfismo de K-álgebras inverso de f y sea $g^E_{\mathscr{B}_B,\mathscr{B}_A} : B^E_{\mathscr{B}_B} \to A^E_{\mathscr{B}_A}$ el morfismo de E-álgebras obtenido de g por extensión de escalares. Entonces

$$\begin{aligned} g^E_{\mathscr{B}_B,\mathscr{B}_A} \circ f^E_{\mathscr{B}_A,\mathscr{B}_B} &= (g \circ f)^E_{\mathscr{B}_A,\mathscr{B}_A} && \text{por la parte } (ii) \text{ de la Proposición 14} \\ &= (\mathsf{id}_A)^E_{\mathscr{B}_A,\mathscr{B}_B} && \text{porque } f \text{ y } g \text{ son inversos} \\ &= \mathsf{id}_{A^E_{\mathscr{B}_A}} && \text{por la parte } (i) \text{ de la Proposición 14} \end{aligned}$$

y, de manera similar, $f^E_{\mathscr{B}_A,\mathscr{B}_B} \circ g^E_{\mathscr{B}_B,\mathscr{B}_A} = \mathsf{id}_{B^E_{\mathscr{B}_B}}$. Esto nos dice que losmorfismos de E-álgebras $f^E_{\mathscr{B}_A,\mathscr{B}_B}$ y $g^E_{\mathscr{B}_B,\mathscr{B}_A}$ son isomorfismos inversos. □

§4. Formas de un álgebra

Si E/K es una extensión de cuerpos y A es una E-álgebra, decimos que una K-álgebra $\mathcal{A}$ es una ***K-forma*** de A si existe una base $\mathscr{B}$ de $\mathcal{A}$ como K-espacio vectorial tal que hay un isomorfismo de E-álgebras $A \cong \mathcal{A}^E_{\mathscr{B}}$. De acuerdo a la Proposición 10, si es éste el caso entonces de hecho hay un isomorfismo de E-álgebras $\mathcal{A}^E_{\mathscr{B}'} \cong A$ para *toda* base $\mathscr{B}'$ de $\mathcal{A}$ como K-espacio vectorial.

Lema 16. *Sea E/K una extensión de cuerpos. Sean n, $m \geq 0$, $M \in \mathsf{M}_{n,m}(K)$ una matriz de n por m con entradas en K y $b \in K^n$ un vector columna.*

(i) Si existe $x \in E^m$ tal que $Mx = b$, entonces existe $y \in K^m$ tal que $My = b$.

(ii) Si existe un único $x \in E^m$ tal que $Mx = b$, entonces $x \in K^m$.

Demostración. Sea $M' = \begin{pmatrix} M & b \end{pmatrix}$ la matriz de n por $m+1$ cuyas primeras m columnas son las de M y cuya última columna es el vector b.

(i) Sean $X^1, \ldots, X^m$ variables distintas y sea $X = (X^1, \ldots, X^m)$. Como existe $x \in E^m$ tal que $Mx = b$, el sistema de n ecuaciones lineales no homogéneas $MX = b$ con coeficientes en E admite soluciones en E^m, así que es compatible y el rango de la matriz M coincide con el de la matriz extendida M' o, equivalentemente, el tamaño del menor cuadrado más grande de M con determinante no nulo coincide con el tamaño del menor cuadrado más grande de M' con determinante no nulo.

Como tanto M como b tienen todas sus entradas en K, podemos considerer el sistema de n ecuaciones $MX = b$ pero ahora buscando soluciones *en* K^m. El sistema es compatible porque M y M' tienen el mismo rango —ya que la anulación de los determinantes de los menores de estas matrices es independiente del cuerpo en el que busquemos las soluciones del sistema— y esto prueba lo que queremos.

(ii) Esta afirmación sigue inmediatamente de la primera, ya que $K^m \subseteq E^m$. □

Proposición 17. *Sea E/K una extensión de cuerpos y sea A una E-álgebra de dimensión finita. Existe una K-forma de A si y solamente si existe una base $\mathscr{B}$ de A como E-espacio vectorial tal que la tabla $C_{\mathscr{B}}(A)$ de constantes de estructura de A con respecto a $\mathscr{B}$ tiene todas sus entradas en K.*

Demostración. Supongamos primero que existe una base $\mathscr{B} = (x_i)_{i \in I}$ de A como E-espacio vectorial tal que todas las entradas de $C_{\mathscr{B}}(A) = (\gamma^k_{i,j})_{i,j,k \in I}$ están en K. Sea $n = \mathsf{dim}_E A$ y sea $(u^i)_{i \in I}$ la familia de coordenadas de 1_A en la base $\mathscr{B}$, de

manera que $1_A = \sum_{i\in I} u^i x_i$. En principio, sólo sabemos que $u^i \in E$ para cada $i \in I$. Sin embargo, de acuerdo a la Proposición 5, para cada j, $k \in I$ se tiene que

$$\sum_{i\in I} u^i \gamma_{i,j}^k = \sum_{i\in I} u^i \gamma_{j,i}^k = \delta_j^k,$$

y esto significa que la familia $(u^i)_{i\in I}$ es una solución de un sistema de $2n^2$ ecuaciones lineales no homogéneas con coeficientes en K: como ese sistema tiene exactamente una solución, el Lema 16 nos dice que, de hecho, $u^i \in K$ para cada $i \in I$.

Fijemos una familia $\mathscr{B}' = (y_i)_{i\in I}$ de símbolos nuevos tales que $y_i \neq y_j$ si $i \neq j$ y sea $\mathcal{A}$ el K-espacio vectorial que tiene a $\mathscr{B}'$ como base. Como A es una E-álgebra, sabemos que la tabla $(\gamma_{i,j}^k)_{i,j,k\in I}$ y el vector $(u^i)_{i\in I}$ satisfacen las ecuaciones (2) y (3) de la Proposición 5. Como además tienen sus entradas en K, esa misma proposición nos dice que hay una estructura de K-álgebra sobre $\mathcal{A}$ tal que $C_{\mathscr{B}'}(\mathcal{A}) = C_{\mathscr{B}}(A)$.

Consideremos ahora el álgebra $\mathcal{A}^E_{\mathscr{B}'}$ obtenida por extensión de escalares de K a E a partir de $\mathcal{A}$ con respecto a la base $\mathscr{B}'$ y sea $\bar{\mathscr{B}}' = (\bar{y}_i)_{i\in I}$ la base de $\mathcal{A}^E_{\mathscr{B}'}$ usada en su construcción. Sea $f : \mathcal{A}^E_{\mathscr{B}'} \to A$ la función E-lineal tal que $f(\bar{y}_i) = x_i$ para todo $i \in I$. Como $(\bar{y}_i)_{i\in I}$ y $(x_i)_{i\in I}$ son bases del dominio y del codominio de f, respectivamente, es claro que f es un isomorfismo de E-espacios vectoriales y, más aún, de acuerdo al Corolario 8 se trata de un isomorfismo de E-álgebras, ya que $C_{\bar{\mathscr{B}}'}(\mathcal{A}^E_{\mathscr{B}'}) = C_{\mathscr{B}}(A)$. Así, vemos que $\mathcal{A}$ es una K-forma de A.

Recíprocamente, supongamos que la E-álgebra A posee una K-forma $\mathcal{A}$. Sea $\mathscr{B}' = (y_i)_{i\in I}$ una base de $\mathcal{A}$ como K-espacio vectorial, sea $\bar{\mathscr{B}}' = (\bar{y}_i)_{i\in I}$ la base de $\mathcal{A}^E_{\mathscr{B}'}$ como E-espacio vectorial usada para construir esta E-álgebra y sea $f : \mathcal{A}^E_{\mathscr{B}'} \to A$ un isomorfismo de E-álgebras. Si para cada $i \in I$ ponemos $x_i = f(\bar{y}_i)$, entonces $\mathscr{B} = (x_i)_{i\in I}$ es una base y, de acuerdo al Corolario 8, es $C_{\mathscr{B}}(A) = C_{\bar{\mathscr{B}}'}(\mathcal{A}^E_{\mathscr{B}'})$. En particular, la tabla de constantes de estructura de A con respecto a la base $\mathscr{B}$ tiene todas sus entradas en K. □

La siguiente observación es útil:

Lema 18. *Sea E/K una extensión de cuerpos y sea A una E-álgebra de dimensión finita y positiva. Si A posee una base $\mathscr{B}$ como E-espacio vectorial tal que la tabla de constantes de estructura $C_{\mathscr{B}}(A)$ tiene todas sus entradas en K, entonces tiene una base $\mathscr{B}'$ con la misma propiedad y que incluye a 1_A.*

Demostración. Hacer. □

Si E/K es una extensión de cuerpos, no toda E-álgebra admite una K-forma. Veamos un ejemplo de esto.

Ejemplo 1. Supongamos que A/K es una extensión de cuerpos cíclica de grado 4. Existen α, $\beta \in A$ tales que $A = K(\alpha)$ y $E = K(\beta)$ es el único subcuerpo de A que contiene a K y tal que $[E : K] = 2$. Supongamos que la E-álgebra A tiene una K-forma $\mathcal{A}$. De acuerdo a la Proposición 17 y el Lema 18, existe entonces una base $\mathscr{B}$ de A como E-espacio vectorial de la forma $\{1, x\}$ tal que la tabla de constantes de estructura de A con respecto a $\mathscr{B}$ tiene todas sus entradas en K. En particular, existen a, $b \in K$ tales que $x^2 = ax + b$. El cuerpo $K(x)$ es entonces una

extensión cuadrática de K contenida en A, así que debe ser $K(x) = E$ y esto es imposible porque 1 y x son linealmente independientes sobre E.

Un ejemplo concreto puede obtenerse considerando el cuerpo A de descomposición del polinomio $f(X) = X^4 + 4X^2 + 2 \in \mathbb{Q}[X]$ sobre $\mathbb{Q}$. En efecto, es fácil verificar que si $\alpha \in \mathbb{C}$ es una raíz de f, entonces $A = \mathbb{Q}(\alpha)$ es una extensión cuártica cíclica de $\mathbb{Q}$.

Por otro lado, cuando un álgebra posee formas sobre un subcuerpo de su cuerpo de base, puede ser que tenga muchas no isomorfas entre sí.

Ejemplo 2. Consideremos la extensión de cuerpos $\mathbb{C}/\mathbb{Q}$ y la $\mathbb{C}$-álgebra $A = \mathbb{C} \times \mathbb{C}$. Si $n \geq 2$ es un número entero libre de cuadrados y ponermos $x = \sqrt{n}$, entonces $\mathcal{A} = \mathbb{Q}(x)$ es una $\mathbb{Q}$-álgebra que es una forma de A sobre $\mathbb{Q}$. En efecto, $\mathscr{B} = \{1, x\}$ es una base de $\mathcal{A}$ como $\mathbb{Q}$-espacio vectorial, así que la $\mathbb{C}$-álgebra $\mathcal{A}^{\mathbb{C}}_{\mathscr{B}}$ tiene una base $\bar{\mathscr{B}} = \{\bar{1}, \bar{x}\}$ tal que $\bar{1}$ es la identidad y $\bar{x}^2 = n$. Se sigue de esto que hay un morfismo de $\mathbb{C}$-álgebras $f : \mathbb{C}[X] \to \mathcal{A}^{\mathbb{C}}_{\mathscr{B}}$ tal que $f(X) = \bar{x}$, que este homomorfismo es sobreyectivo, y que su núcleo contiene al ideal $(X^2 - n)$. Así, tenemos un morfismo sobreyectivo de $\mathbb{C}$-álgebras $F : \mathbb{C}[X]/(X^2 - n) \to \mathcal{A}^{\mathbb{C}}_{\mathscr{B}}$. Como $X^2 - n = (X - i\sqrt{n})(X + i\sqrt{n})$ y los dos factores son coprimos en $\mathbb{C}[X]$, el teorema chino del resto nos dice que hay un isomorfismo de $\mathbb{C}$-álgebras

$$\frac{\mathbb{C}[X]}{(X^2 - n)} \cong \frac{\mathbb{C}[X]}{(X - i\sqrt{n})} \times \frac{\mathbb{C}[X]}{(X + i\sqrt{n})}.$$

Finalmente, como $\mathbb{C}[X]/(X - \lambda)$ es isomorfa como $\mathbb{C}$-álgebra con $\mathbb{C}$ cualquiera sea $\lambda \in \mathbb{C}$, vemos que $\mathcal{A}^{\mathbb{C}}_{\mathscr{B}} \cong A$, como dijimos.

Así, para cada entero $n \geq 2$ libre de cuadrados la $\mathbb{Q}$-álgebra $\mathbb{Q}(\sqrt{n})$ es una $\mathbb{Q}$-forma de la $\mathbb{C}$-álgebra $\mathbb{C} \times \mathbb{C}$, y es fácil verificar que $\mathbb{Q}(\sqrt{n})$ y $\mathbb{Q}(\sqrt{m})$ son $\mathbb{Q}$-álgebras no isomorfas si $n \neq m$. Por otro lado, es inmediato verificar que la $\mathbb{Q}$-álgebra $\mathbb{Q} \times \mathbb{Q}$ también es una $\mathbb{Q}$-forma de $\mathbb{C} \times \mathbb{C}$ y que no es isomorfa a ninguna de las anteriores.

§5. Formas torcidas de un álgebra

Sea E/K una extensión de cuerpos. Decimos que dos K-álgebras A y A' son ***E-isomorfas***, o que A' es una ***forma torcida de A con respecto a la extensión E/K***, si hay bases $\mathscr{B}$ y $\mathscr{B}'$ de A y de A' en tanto K-espacios vectoriales tales que las E-álgebras $A^E_{\mathscr{B}}$ y $A'^E_{\mathscr{B}'}$ son isomorfas como E-álgebras. De acuerdo a la Proposición 10, esta condición depende solamente de A y de A' y no de las bases $\mathscr{B}$ y $\mathscr{B}'$ elegidas, así que esto tiene sentido.

Por otro lado, si A, A' y A'' son K-álgebras tales que A y A' son E-isomorfas y A' y A'' son isomorfas como K-álgebras, entonces A y A'' son E-isomorfas. Esto implica que el hecho de que dos K-álgebras A y A' sean E-isomorfas depende solamente de las clases de isomorfismo de A y de A'. Si A es una K-álgebra, podemos en consecuencia considerar el conjunto $T_{E/K}(A)$ de las clases de isomorfismo de K-álgebras que son E-isomorfas a A.

Nos proponemos obtener una descripción del conjunto $T_{E/K}(A)$ en el caso en que la extensión E/K es galoisiana.

Proposición 19. *Sea E/K una extensión finita y galoisiana de cuerpos y sea $G = \mathsf{Gal}(E/K)$ su grupo de Galois. Sea A es una K-álgebra de dimensión finita, sea $\mathscr{B} = (x_i)_{i\in I}$ una base de A como K-espacio vectorial y sea $\bar{\mathscr{B}} = (\bar{x}_i)_{i\in I}$ la base de $A^E_{\mathscr{B}}$ usada para construir esta E-álgebra. Hay una única acción del grupo G sobre $A^E_{\mathscr{B}}$ por automorfismos de K-álgebra tal que*

- *el morfismo canónico $\eta : E \to A^E_{\mathscr{B}}$ es G-equivariante y*
- *para cada $g \in G$ y cada $i \in I$ es ${}^g\bar{x}_i = \bar{x}_i$.*

Demostración. Supongamos que tenemos una acción de G sobre $A^E_{\mathscr{B}}$ que satisface esas dos condiciones. Si $g \in G$ y $x \in A^E_{\mathscr{B}}$, de manera que existe $(u^i)_{i\in I}$ tal que $x = \sum_{i\in I} u^i\bar{x}_i$, entonces

$$ {}^g x = \sum_{i\in I} {}^g(u^i\bar{x}_i) = \sum_{i\in I} {}^g(\eta(u^i)\bar{x}_i) = \sum_{i\in I} {}^g\eta(u^i)\cdot {}^g\bar{x}_i $$

y aquellas dos condiciones nos dicen que esto es

$$ = \sum_{i\in I} \eta({}^g u^i)\cdot \bar{x}_i = \sum_{i\in I} {}^g u^i\bar{x}_i. $$

Vemos así que hay a lo sumo una acción de G sobre $A^E_{\mathscr{B}}$ que satisface las condiciones del enunciado y, de hecho, nos dice que si existe una entonces es tal que

$$ {}^g\Big(\sum_{i\in I} u^i\bar{x}_i\Big) = \sum_{i\in I} {}^g u^i\bar{x}_i. $$

Como

$$ {}^g x = {}^{1_G}\Big(\sum_{i\in I} u^i\bar{x}_i\Big) = \sum_{i\in I} {}^{1_G}u^i\bar{x}_i = \sum_{i\in I} u^i\bar{x}_i = x, $$

y

$$ \begin{aligned} {}^g({}^h x) = {}^g\Big({}^h\Big(\sum_{i\in I} u^i\bar{x}_i\Big)\Big) = {}^g\Big(\sum_{i\in I} {}^h u^i\bar{x}_i\Big) = \sum_{i\in I} {}^g({}^h u^i)\bar{x}_i = \sum_{i\in I} {}^{gh}u^i\bar{x}_i \\ = {}^{gh}\Big(\sum_{i\in I} u^i\bar{x}_i\Big) = {}^{gh}x \end{aligned} $$

para cada g, $h \in G$, esto efectivamente define una acción de G sobre $A^E_{\mathscr{B}}$. Si $v \in K$, entonces

$$ \begin{aligned} {}^g(vx) = {}^g\Big(v\sum_{i\in I} u^i\bar{x}_i\Big) = {}^g\Big(\sum_{i\in I} vu^i\bar{x}_i\Big) = \sum_{i\in I} {}^g(vu^i)\bar{x}_i = \sum_{i\in I} v\,{}^g(u^i)\bar{x}_i \\ = v\sum_{i\in I} {}^g(u^i)\bar{x}_i = v\,{}^g\Big(\sum_{i\in I} u^i\bar{x}_i\Big) = v\,{}^g x, \end{aligned} $$

así que esta acción es K-lineal. Finalmente, si $\mathscr{B} = (\gamma^k_{i,j})_{i,j,k\in I}$ es la tabla de constantes de estructura de A con respecto a la base $\mathscr{B}$ e $y = \sum_{i\in I} v^i\bar{x}_i$ es otro

elemento de $A^E_{\mathscr{B}}$, entonces

$$\begin{aligned}{}^g(xy) &= {}^g\Big(\sum_{i\in I} u^i\bar{x}_u \cdot \sum_{j\in I} v^j\bar{x}_j\Big) = {}^g\Big(\sum_{i,j\in I} u^iv^j\bar{x}_i\cdot\bar{x}_j\Big)\\ &= {}^g\Big(\sum_{k\in I}\Big(\sum_{i,j,k\in I} u^iv^j\gamma^k_{i,j}\Big)\bar{x}_k\Big) = \sum_{k\in I}{}^g\Big(\sum_{i,j,k\in I} u^iv^j\gamma^k_{i,j}\Big)\bar{x}_k\\ &= \sum_{k\in I}\Big(\sum_{i,j,k\in I}{}^g(u^iv^j\gamma^k_{i,j})\Big)\bar{x}_k = \sum_{k\in I}\Big(\sum_{i,j,k\in I}{}^gu^i\,{}^gv^j\,\gamma^k_{i,j}\Big)\bar{x}_k\end{aligned}$$

y

$$\begin{aligned}{}^gx\cdot{}^gy &= {}^g\Big(\sum_{i\in I}u^i\bar{x}_i\Big){}^g\Big(\sum_{j\in I}v^i\bar{x}_i\Big) = \sum_{i\in I}{}^gu^i\bar{x}_i\cdot\sum_{j\in I}{}^gv^i\bar{x}_i\\ &= \sum_{i,j\in I}{}^gu^i\,{}^gv^i\bar{x}_i\cdot\bar{x}_j = \sum_{i,j,k\in I}{}^gu^i\,{}^gv^i\gamma^k_{i,j}\bar{x}_k,\end{aligned}$$

de manera que ${}^g(xy) = {}^gx\,{}^gy$, y la acción es por morfismos de anillos. □

Es importante observar que —salvo en el caso en que la extensión E/K es trivial— la acción del grupo G sobre $A^E_{\mathscr{B}}$ construida en la Proposición 19 *no* es por automorfismos de E-álgebras.

Proposición 20. *Sea E/K una extensión finita y galoisiana de cuerpos y sea $G = \mathsf{Gal}(E/K)$ su grupo de Galois. Sean A y A' dos K-álgebras de dimensión finita que son E-isomorfas, sean $\mathscr{B}$ y $\mathscr{B}'$ bases de A y de A' como K-espacios vectoriales, y sea $f : A^E_{\mathscr{B}} \to A'^E_{\mathscr{B}'}$ un morfismo de E-álgebras. Para cada $g \in G$ consideremos la función $\alpha_A(g) : x \in A^E_{\mathscr{B}} \mapsto {}^gx \in A^E_{\mathscr{B}}$ y similarmente para A'.*

(*i*) *Para cada $g \in G$, la aplicación ${}^gf$ dada por la composición*

$$A^E_{\mathscr{B}} \xrightarrow{\alpha_A(g^{-1})} A^E_{\mathscr{B}} \xrightarrow{\quad f\quad} A'^E_{\mathscr{B}'} \xrightarrow{\alpha_{A'}(g)} A'^E_{\mathscr{B}'}$$

es un morfismo de E-álgebras.

(*ii*) *Esto determina una acción de G sobre $\mathsf{hom}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}}, A'^E_{\mathscr{B}'})$,*

$$(g,f) \in G\times\mathsf{hom}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}}, A'^E_{\mathscr{B}'}) \longmapsto {}^gf \in \mathsf{hom}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}}, A'^E_{\mathscr{B}'}).$$

Así, es ${}^1{}_Gf = f$ y ${}^h({}^gf) = {}^{hg}f$ si $f \in \mathsf{hom}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}}, A'^E_{\mathscr{B}'})$ y g, $h \in G$.

(*iii*) *Si A'' es otra K-álgebra, $\mathscr{B}''$ es una base de A'' como K-espacio vectorial y $f' : A'^E_{\mathscr{B}'} \to A''^E_{\mathscr{B}''}$ es un isomorfismo de E-álgebras, entonces*

$${}^g(f'\circ f) = {}^gf'\circ{}^gf.$$

(*iv*) *Finalmente, si $\mathsf{id}_{A^E_B} : A^E_{\mathscr{B}} \to A^E_{\mathscr{B}}$ es el morfismo identidad, entonces*

$${}^g(\mathsf{id}_{A^E_B}) = \mathsf{id}_{A^E_B}.$$

Demostración. Supongamos que $\mathscr{B} = (x_i)_{i\in I}$ y $\mathscr{B}' = (x'_u)_{u\in U}$, y sean $\bar{\mathscr{B}} = (\bar{x}_i)_{i\in I}$ y $\bar{\mathscr{B}}' = (\bar{x}'_u)_{u\in U}$ las bases usadas para construir las E-álgebras $A^E_{\mathscr{B}}$ y $A'^E_{\mathscr{B}'}$. Sea, por otro lado, $(f^u_i)_{i\in I,u\in U}$ la matriz de f con respecto a las bases $\bar{\mathscr{B}}$ y $\bar{\mathscr{B}}'$.

Como G actúa sobre $A^E_{\mathscr{B}}$ y sobre $A'^E_{\mathscr{B}'}$ por automofismos de K-álgebra y f es un morfismo de E-álgebras, la composición $\alpha_{A'}(g)\circ f\circ\alpha_A(g^{-1})$ es un morfismo

de K-álgebras. Resta ver que es E-lineal. Si $x = \sum_{i\in I} u^i \bar{x}_i$ es un elemento de $A^E_{\mathscr{B}}$ y $v \in E$, tenemos que

$$\begin{aligned}
{}^g f(vx) &= {}^g\left(f\left({}^{g^{-1}}\Big(\sum_{i\in I} vu^i\bar{x}_i\Big)\right)\right) = {}^g\left(f\left(\sum_{i\in I} {}^{g^{-1}}v\,{}^{g^{-1}}u^i\bar{x}_i\right)\right)\\
&= {}^g\left(f\left(\sum_{i\in I} {}^{g^{-1}}v\,{}^{g^{-1}}u^i\bar{x}_i\right)\right) = {}^g\left(\sum_{i,j\in I} {}^{g^{-1}}v\,{}^{g^{-1}}u^i f_i^j\bar{x}'_i\right)\\
&= \sum_{i,j\in I} vu^{i\,g} f_i^j\bar{x}'_i = v\sum_{i,j\in I} u^{i\,g} f_i^j\bar{x}'_i.
\end{aligned}$$

Notemos que este mismo cálculo pero hecho con $v = 1$ muestra que

$${}^g f(x) = \sum_{i,j\in I} u^{i\,g} f_i^j\bar{x}'_i,$$

así que ${}^g f(vx) = v^g f(x)$. Vemos así que ${}^g f$ es E-lineal; esto prueba (i).

Si $f \in \mathsf{hom}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}}, A'^E_{\mathscr{B}'})$ y g, $h \in G$, entonces

$${}^{1_G} f = \alpha_{A'}(1_G)\circ f\circ\alpha_A(1_G^{-1}) = \mathsf{id}_{A'^E_{\mathscr{B}'}}\circ f\circ \mathsf{id}_{A^E_{\mathscr{B}}} = f$$

y

$$\begin{aligned}
{}^g({}^h f) &= {}^g(\alpha_{A'}(h)\circ f\circ\alpha_A(h^{-1}))\\
&= \alpha_{A'}(g)\circ\alpha_{A'}(h)\circ f\circ\alpha_A(h^{-1})\circ\alpha_A(g^{-1})\\
&= \alpha_{A'}(gh)\circ f\circ\alpha_A((gh)^{-1})\\
&= {}^{gh} f,
\end{aligned}$$

de manera que tenemos una acción de G sobre $\mathsf{hom}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}}, A'^E_{\mathscr{B}'})$, como se afirma en (ii). Finalmente, en la situación de (iii) tenemos que para cada $g \in G$

$$\begin{aligned}
{}^g(f'\circ f) &= \alpha_{A''}(g)\circ f'\circ f\circ\alpha_A(g^{-1})\\
&= \alpha_{A''}(g)\circ f'\circ\alpha_{A'}(g^{-1})\circ\alpha_{A'}(g)\circ f\circ\alpha_A(g^{-1})\\
&= {}^g f'\circ {}^g f.
\end{aligned}$$

y

$${}^g(\mathsf{id}_{A^E_{\mathscr{B}}}) = \alpha_A(g)\circ\mathsf{id}_{A^E_{\mathscr{B}}}\circ\alpha_A(g^{-1}) = \alpha_A(g)\circ\alpha_A(g^{-1}) = \mathsf{id}_{A^E_{\mathscr{B}}},$$

así que (iii) y (iv) valen. □

Corolario 21. *Sea E/K una extensión finita y galoisiana de cuerpos de grupo de Galois $G = \mathsf{Gal}(E/K)$. Sea A una K-álgebra de dimensión finita, sea $\mathscr{B}$ una base de A como K-espacio vectorial y sea $\mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})$ el grupo de automorfismos de $A^E_{\mathscr{B}}$ como E-álgebra.*

(i) Hay una acción de G sobre $\mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})$ por automorfismos de grupos dada por

$$(g, f) \in G\times\mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}}) \longmapsto {}^g f \in \mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}}).$$

(*ii*) *Sean* $n = \dim_K E$ *e* $I = \{1, \dots, n\}$ *y supongamos que* $\mathscr{B} = (x_i)_{i\in I}$ *y que* $\bar{\mathscr{B}} = (\bar{x}_i)_{i\in I}$ *es la base de* $A^E_{\mathscr{B}}$ *como* E*-espacio vectorial usada para construir esta álgebra. Hay un morfismo de grupos*

$$m_{\mathscr{B}} : \mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}}) \to \mathsf{GL}(n, E)$$

tal que si $f \in \mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})$ *y* $m_{\mathscr{B}}(f) = (f^j_i)_{i,j\in I}$*, es* $f(\bar{x}_i) = \sum_{j\in I} f^j_i \bar{x}_j$ *para cada* $i \in I$*. Más aún, este morfismo es* G*-equivariante con respecto a las acciones de* G *sobre* $\mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})$ *y sobre* $\mathsf{GL}(n, E)$ *definidas en la parte* (*i*) *y en el Lema 3, respectivamente.*

Demostración. Hacer. □

En general, si E/K es una extensión, un morfismo de E-álgebras obtenidas por extensión de escalares de K-álgebras no proviene de la extensión de escalares de un morfismo de K-álgebras. La siguiente proposición da una condición suficiente para que sea ése el caso cuando la extensión de cuerpos es galoisiana.

Proposición 22. *Sea* E/K *una extensión finita y galoisiana y sea* $G = \mathsf{Gal}(E/K)$ *su grupo de Galois. Sean* A *y* A' *dos* K*-álgebras de dimensión finita, sean* $\mathscr{B}$ *y* $\mathscr{B}'$ *bases de* A *y de* A' *como* K*-espacios vectoriales y supongamos que* $f : A^E_{\mathscr{B}} \to A'^E_{\mathscr{B}'}$ *es un isomorfismo de* E*-álgebras.*

(*i*) *Si para cada* $g \in G$ *es* ${}^g f = f$*, entonces existe un isomorfismo* $F : A \to A'$ *de* K*-álgebras tal que* $F^E_{\mathscr{B},\mathscr{B}'} = f$*.*

(*ii*) *Si además* f *es un isomorfismo de* E*-álgebras, entonces* F *es un isomorfismo de* K*-álgebras.*

Demostración. Hacer. □

Proposición 23. *Sea* E/K *una extensión finita y galoisiana de cuerpos y sea* $G = \mathsf{Gal}(E/K)$ *su grupo de Galois. Sean* A *y* A' *dos* K*-álgebras de dimensión finita que son* E*-isomorfas, sean* $\mathscr{B}$ *y* $\mathscr{B}'$ *bases de* A *y de* A' *como* K*-espacios vectoriales, y sea* $f : A^E_{\mathscr{B}} \to A'^E_{\mathscr{B}'}$ *un isomorfismo de* E*-álgebras. La función* $\phi_f : G \to \mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})$ *tal que para cada* $g \in G$ *es*

$$\phi_f(g) = f^{-1} \circ {}^g f$$

es un 1*-cociclo de* G *con valores en* $\mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})$*, esto es, para cada* $g, h \in G$ *vale que*

$$\phi_f(g) \circ {}^g\phi_f(h) = \phi_f(gh).$$

Si $f' : A^E_{\mathscr{B}} \to A'^E_{\mathscr{B}'}$ *es otro isomorfismo de* E*-álgebras y ponemos* $u = f'^{-1} \circ f$*, entonces vale que*

$$\phi_f(g) = u^{-1} \circ \phi_{f'}(g) \circ {}^g u$$

para cada $g \in G$*. Así, los* 1*-cociclos* ϕ_f *y* $\phi_{f'}$ *son cohomólogos.*

Demostración. Hacer. □

Proposición 24. *Sea E/K una extensión finita y galoisiana de cuerpos y sea $G = \mathsf{Gal}(E/K)$ su grupo de Galois. Sea A una K-álgebra de dimensión finita, sea $\mathscr{B}$ una base de A como K-espacio vectorial y sea $\mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})$ el grupo de automorfismos de la E-álgebra $A^E_{\mathscr{B}}$ dotado de la acción de G descripta en el Corolario 21. Si $\mathfrak{a} \in T_{E/K}(A)$ es la clase de isomorfismo de una forma torcida A' de A, $\mathscr{B}'$ una base de A' como K-espacio vectorial y $f : A^E_{\mathscr{B}} \to A'^E_{\mathscr{B}'}$ un isomorfismo de E-álgebras, entonces la función $\phi_f : G \to \mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})$ construida en la Proposición 23 es un 1-cociclo de G con valores en $\mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})$ y su clase de cohomología $[\phi_f] \in H^1(G, \mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}}))$ depende solamente de $\mathfrak{a}$ y no del álgebra A' ni del isomorfismo f elegido. En particular, podemos escribirla $\chi(\mathfrak{a})$. Esto define una función*

$$\chi : \mathfrak{a} \in T_{E/K}(A) \longmapsto \chi(\mathfrak{a}) \in H^1(G, \mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})).$$

Demostración. Hacer. □

Teorema 25. *Sea E/K una extensión finita y galoisiana de cuerpos de grupo de Galois $G = \mathsf{Gal}(E/K)$. Sea A una K-álgebra de dimensión finita, sea $\mathscr{B}$ una base de A como K-espacio vectorial y sea $\mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})$ el grupo de automorfismos de la E-álgebra $A^E_{\mathscr{B}}$ dotado de la acción de G descripta en el Corolario 21. La función*

$$\chi : T_{E/K}(A) \to\in H^1(G, \mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}}))$$

construida en la Proposición 24 es una biyección.

Si A' es una forma torcida de A con respecto a la extensión E/K y $[A']$ es su clase de isomorfismo, llamamos a $\chi([A'])$ la ***clase característica*** de A'.

Demostración. Supongamos primero que A' y A'' son dos K-álgebras, que $\mathscr{B}'$ y $\mathscr{B}''$ son bases de A' y de A'' como K-espacios vectoriales, que $f : A^E_{\mathscr{B}} \to A'^E_{\mathscr{B}'}$ y $f' : A^E_{\mathscr{B}} \to A''^E_{\mathscr{B}''}$ son isomorfismos de E-álgebras, y que los 1-cociclos correspondientes ϕ_f, $\phi_{f'} : G \to \mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})$ son cohomólogos, de manera que existe $u \in \mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})$ tal que para cada $g \in G$ es

$$\phi_f(g) = u^{-1} \circ \phi_{f'}(g) \circ {}^g u$$

o, equivalentemente,

$$f' \circ u \circ f^{-1} = {}^g(f' \circ u \circ f^{-1}).$$

Esto significa precisamente que la función $f' \circ u \circ f^{-1} : A'^E_{\mathscr{B}'} \to A''^E_{\mathscr{B}''}$, que es un isomorfismo de E-álgebras, satisface las condiciones de la Proposición 22 y, entonces, que existe un isomorfismo $F : A' \to A''$ de K-álgebras tal que $F^E_{\mathscr{B}',\mathscr{B}''} = f' \circ u \circ f^{-1}$. En particular, las K-álgebras A' y A'' son isomorfas. Esto prueba que la función χ del enunciado es inyectiva.

Veamos ahora que se trata de una suryección. Sea $\phi : G \to \mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})$ un 1-cociclo de G con valores en $\mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})$. Sea $n = \mathsf{dim}_K A$, supongamos que es $\mathscr{B} = (x_i)_{i\in I}$ con $I = \{1, \dots, n\}$, sea $C_{\mathscr{B}}(A) = (\gamma^k_{i,j})_{i,j,k\in I}$ la tabla de constantes de estructura de A con respecto a $\mathscr{B}$, y sea $1_A = \sum_{i\in I} e^i x_i$ la expresión del elemento identidad de A en la base $\mathscr{B}$. Sea finalmente $\bar{\mathscr{B}} = (\bar{x}_i)_{i\in I}$ la base de $A^E_{\mathscr{B}}$ como E-espacio vectorial usada para construir esta álgebra.

Sea $m_{\mathscr{B}} : \mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}}) \to \mathsf{GL}(n, E)$ el morfismo de grupos de la parte (ii) del Corolario 21. Como ϕ es un 1-cociclo con valores en $\mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})$, es inmediato verificar que la composición $m \circ \phi : G \to \mathsf{GL}(n, E)$ es un 1-cociclo con valores en $\mathsf{GL}(n, E)$. De acuerdo al Teorema 4, sabemos que $H^1(G, \mathsf{GL}(n, K)) = 0$ y, entonces, que existe $u = (u_i^j)_{i,j\in I} \in \mathsf{GL}(n, E)$ tal que para todo $g \in G$ es

$$m_{\mathscr{B}}(\phi(g)) = u^{-1} \cdot {}^g u.$$

Esto nos dice que para cada $g \in G$ es

$${}^g u = u \cdot m_{\mathscr{B}}(\phi(g)), \qquad {}^g u^{-1} = m_{\mathscr{B}}(\phi(g))^{-1} \cdot u^{-1}. \tag{5}$$ {eq:gu}

Si ponemos $u^{-1} = (\hat{u}_i^j)_{i,j\in I}$ y, para cada $g \in G$,

$$m_{\mathscr{B}}(\phi(g)) = (g_i^j)_{i,j\in I}, \qquad m_{\mathscr{B}}(\phi(g))^{-1} = (\hat{g}_i^j)_{i,j\in I}$$

las ecuaciones (5) implican que

$${}^g u_i^j = \sum_{k\in I} u_i^k g_k^j, \qquad {}^g \hat{u}_i^j = \sum_{k\in I} \hat{g}_i^k \hat{u}_k^j. \tag{6}$$ {eq:guv}

Por otro lado, como $\phi(g)$ es un automorfismo de la E-álgebra $A^E_{\mathscr{B}}$, para cada i, j, k tenemos que

$$\sum_{i,j,k\in I} \gamma_{i,j}^k g_r^i g_s^j \hat{g}_k^t = \gamma_{r,s}^t \tag{7}$$ {eq:mor}

y

$$\sum_{k\in I} e^k \hat{g}_k^i = e^i. \tag{8}$$ {eq:mor:1}

Para cada i, j, $k \in I$ consideremos el elemento de E

$$\eta_{i,j}^k = \sum_{r,s,t\in I} \gamma_{r,s}^t u_i^r u_j^s \hat{u}_t^k. \tag{9}$$ {eq:eta}

Si $g \in G$, entonces

$${}^g \eta_{i,j}^k = {}^g\Big(\sum_{r,s,t\in I} \gamma_{r,s}^t u_i^r u_j^s \hat{u}_t^k \Big)$$

que, ya que las constantes de estructura de A están en K, es igual a

$$\sum_{r,s,t\in I} \gamma_{r,s}^t \cdot {}^g u_i^r \cdot {}^g u_j^s \cdot {}^g \hat{u}_t^k.$$

En vista de (6), podemos reescribir esto como

$$\sum_{\substack{r,s,t\in I\\ p,l,m\in I}} \gamma_{r,s}^t \cdot u_i^p g_p^r \cdot u_j^l g_l^s \cdot \hat{g}_t^m \hat{u}_m^k = \sum_{\substack{r,s,t\in I\\ p,l,m\in I}} \gamma_{r,s}^t g_p^r g_l^s \hat{g}_t^m \cdot u_i^p u_j^l \hat{u}_m^k$$

que, gracias a las igualdades (7), es lo mismo que

$$\sum_{\substack{r,s,t\in I\\ p,l,m\in I}} \gamma_{p,l}^m u_i^p u_j^l \hat{u}_m^k = \eta_{j,k}^k.$$

Así, la tabla $(\eta_{i,j}^k)_{i,j,k\in I}$ tiene todas sus entradas en el cuerpo fijo E^G, que es precisamente K.

Sea $\mathscr{B}' = (y_i)_{i\in I}$ un nuevo conjunto de símbolos tales que $y_i \neq y_j$ si $i \neq j$, y sea A' el K-espacio vectorial que tiene a $\mathscr{B}'$ como base. Hay una función K-bilineal $\mu_{A'} : A' \times A' \to A'$ tal que $\mu_{A'}(y_i, y_j) = \sum_{k\in I} \eta_{i,j}^k y_k$ para toda elección de i, $j \in I$. Veamos que esto hace de A' una K-álgebra asociativa.

Si i, j, l, $m \in I$, entonces

$$\sum_{k\in I} \eta_{i,j}^k \eta_{k,l}^m = \sum_{\substack{r,s,t\in I\\ a,b,c\in I}} \gamma_{r,s}^t u_i^r u_j^s \hat{u}_t^k \gamma_{a,b}^c u_k^a u_l^b \hat{u}_c^m$$

y, como $\hat{u}_t^k u_k^a = \delta_t^a$, esto es lo mismo que

$$= \sum_{\substack{r,s,t\in I\\ b,c\in I}} \gamma_{r,s}^t u_i^r u_j^s \gamma_{t,b}^c u_l^b \hat{u}_c^m = \sum_{\substack{r,s\in I\\ b,c\in I}} \left(\sum_{t\in I} \gamma_{r,s}^t \gamma_{t,b}^c \right) u_i^r u_j^s u_l^b \hat{u}_c^m \quad (10) \quad \{\text{eq:ass-1}\}$$

Por otro lado, procediendo de la misma forma vemos que

$$\sum_{k\in I} \eta_{i,k}^m \eta_{j,l}^k = \sum_{\substack{r,s,t\in I\\ a,b,c\in I}} \gamma_{r,s}^t u_i^r u_k^s \hat{u}_t^m \gamma_{a,b}^c u_j^a u_l^b \hat{u}_c^k = \sum_{\substack{r,s,t\in I\\ a,b\in I}} \gamma_{r,s}^t u_i^r \hat{u}_t^m \gamma_{a,b}^s u_j^a u_l^b$$

$$= \sum_{\substack{r,t\in I\\ a,b\in I}} \left(\sum_{s\in I} \gamma_{r,s}^t \gamma_{a,b}^s \right) u_i^r u_j^a u_l^b \hat{u}_t^m. \quad (11) \quad \{\text{eq:ass-2}\}$$

Como la tabla $(\gamma_{i,j}^k)_{i,j,k}$ de constantes de estructura de A satisface la ecuación 2 de la Proposición 5, es inmediato ver que las expresiones (10) y (11) son iguales. Esto implica que la multiplicación $\mu_{A'}$ es asociativa.

Por otro lado, para cada $i \in I$ ponemos $h^i = \sum_{j\in I} e^j \hat{u}_j^i$. Si $g \in G$, entonces

$${}^g h^i = {}^g\Big(\sum_{j\in I} e^j \hat{u}_j^i \Big) = \sum_{j\in G} {}^g e^j \cdot {}^g \hat{u}_j^i$$

y, como $e^j \in K$ para cada $j \in I$ y usando (6), esto es

$$\sum_{j,k\in G} e^j \cdot (g^{-1})_i^k \hat{u}_k^i$$

que, en vista de la ecuación (8), es simplemente

$$\sum_{k\in I} e^k \hat{u}_k^i = h^i.$$

Así, tenemos que $h^i \in E^G = K$ para cada $i \in I$ y podemos, entonces, considerar el elemento $1_{A'} = \sum_{i\in i} h^i y_i$ de A', que resulta ser una identidad para $\mu_{A'}$: en efecto, si $i \in I$ tenemos que

$$\mu_{A'}(1_{A'}, y_i) = \sum_{j\in I} h^j \mu_{A'}(y_j, y_i) = \sum_{j,k\in I} h^j \eta_{j,i}^k y_k = \sum_{\substack{j,k,l\in I\\ r,s,t\in I}} e^l \hat{u}_l^j \gamma_{r,s}^t u_j^r u_i^s \hat{u}_t^k y_k$$

$$= \sum_{\substack{j,k,l\in I\\ s,t\in I}} e^l \gamma_{l,s}^t u_i^s \hat{u}_t^k y_k = \sum_{\substack{j,k\in I\\ s\in I}} u_i^s \hat{u}_s^k y_k = \sum_{\substack{j,k\in I\\ s\in I}} \delta_i^k y_k = y_i.$$

porque $e^l \gamma_{l,s}^t = \delta_s^t$ y, de manera similar, que $\mu_{A'}(y_i, 1_{A'}) = y_i$.

Sea ahora $\bar{\mathscr{B}}' = (\bar{y}_i)_{i\in I}$ la base de $A'^E_{\mathscr{B}'}$ usada para construir esta E-álgebra y consideremos la función E lineal $f : A^E_{\mathscr{B}} \to A'^E_{\mathscr{B}'}$ tal que $f(\bar{x}_i) = \sum_{j\in I} \hat{u}_i^j \bar{y}_j$; la matriz de f con respecto a las bases $\bar{\mathscr{B}}$ y $\bar{\mathscr{B}}'$ de su dominio y su codominio es precisamente u^{-1}, un elemento de $\mathsf{GL}(n, E)$, así que f es un isomorfismo de E-espacios vectoriales. Si i, $j \in I$, es

$$f(\bar{x}_i \cdot \bar{x}_j) = \sum_{k\in I} \gamma_{i,j}^k f(\bar{x}_k) = \sum_{k,m\in I} \gamma_{i,j}^k \hat{u}_k^m \bar{y}_m$$

y

$$f(\bar{x}_i) \cdot f(\bar{x}_j) = \sum_{k,l\in I} \hat{u}_i^k \hat{u}_j^l \, \bar{y}_k \cdot \bar{y}_l = \sum_{k,l,m\in I} \hat{u}_i^k \hat{u}_j^l \eta_{k,l}^m \bar{y}_m,$$

y esas dos expresiones son iguales porque de la ecuación (9) que define a $\eta_{i,j}^k$ se deduce inmediatamente que

$$\sum_{i,j\in I} \eta_{i,j}^k \hat{u}_r^i \hat{u}_s^j = \sum_{r,s,t\in I} \gamma_{r,s}^t \hat{u}_t^k.$$

Vemos así que f es un isomorfismo de E-álgebras.

Sea finalmente $\phi_f : G \to \mathsf{Aut}_{E\text{-}\mathsf{alg}}(A^E_{\mathscr{B}})$ el 1-cociclo que corresponde al isomorfismo f como en la Proposición 23, de manera que para cada $g \in G$ es $\phi_f(g) = f^{-1} \circ {}^g f$.

Terminar. □

§6. Algunos ejemplos

Sea K un cuerpo, sea $n \geq 1$ y consideremos la K-álgebra

$$K^n = K \times \cdots \times K.$$

Nos proponemos describir sus formas torcidas. Pongamos $I = \{1, \ldots, n\}$ y para cada $i \in I$ sea $e_i = (0, \ldots, 1, \ldots, 0)$, con el 1 en la posición i-ésima. La familia $\mathscr{B} = (e_i)_{i\in I}$ es una base de K^n como K-espacio vectorial y la tabla de constantes de estructura $C_{\mathscr{B}}(K^n) = (\gamma_{i,j,k})_{i,j,k\in I}$ tiene

$$\gamma_{i,j}^k = \begin{cases} 1, & \text{si } i = j = k; \\ 0, & \text{en cualquier otro caso.} \end{cases}$$

Proposición 26. *Sea E/K una extensión de cuerpos, sea $(K^n)^E_{\mathscr{B}}$ el álgebra obtenida de K^n por extensión de escalares de K a E con respecto a la base $\mathscr{B}$ y sea $\bar{\mathscr{B}} = (\bar{e}_i)_{i\in I}$ la base usada para construirla.*

(*i*) *Hay un isomorfismo de E-álgebras $(K^n)^E_{\mathscr{B}} \cong E^n$.*

(*ii*) *Hay un isomorfismo de grupos $\alpha : S_n \to \mathsf{Aut}_{E\text{-}\mathsf{alg}}((K^n)^E_{\mathscr{B}})$ tal que*

$$\alpha(\pi)(\bar{e}_i) = \bar{e}_{\pi(i)}$$

para cada $\pi \in S_n$ y cada $i \in \{1, \ldots, n\}$.

(*iii*) *Si la extensión E/K es galoisiana y finita y $G = \mathsf{Gal}(E/K)$ es su grupo de Galois, la acción de G sobre $\mathsf{Aut}_{E\text{-}\mathsf{alg}}((K^n)^E_{\mathscr{B}})$ es trivial.*

Demostración. Hacer. □

Consideremos, por simplicidad, el isomorfismo α de la segunda parte de esta proposición como una identificación. Para describir las formas torcidas del álgebra K^n con respecto a una extensión galoisiana E/K de grupo de Galois $G = \mathsf{Gal}(E/K)$ tenemos que calcular $H^1(G, S_n)$. Como la acción de G sobre S_n es trivial, el siguiente resutado hace precisamente eso.

Proposición 27. *Sea G un grupo y sea A un grupo sobre el que G actúa de manera trivial.*

(*i*) *Una función $\phi : G \to A$ es un 1-cociclo si y solamente si es un morfismo de grupos. Así, $Z^1(G, A) = \mathsf{hom}_{\mathsf{Grp}}(G, A)$.*

(*ii*) *Dos morfismos de grupos ϕ, $\psi : G \to A$ son cohomólogos en tanto 1-cociclos si y solamente si son conjugados, esto es, si existe un elemento $a \in A$ tal que $\phi(g) = a^{-1}\psi(g)a$ para cada $g \in G$.*

(*iii*) *Es $H^1(G, A) = \mathsf{hom}_{\mathsf{Grp}}(G, A)/\mathsf{conj}$, el conjunto de clases de equivalencia de morfismos de grupos $G \to A$ bajo la relación de conjugación conj.*

Demostración. Hacer. □

Como consecuencia de esta proposición, si E/K es una extensión galoisiana y finita, tenemos una biyección $T_{E/K}(K^n) \cong \mathsf{hom}_{\mathsf{Grp}}(G, S_n)/\mathsf{conj}$. Así, a cada clase de conjugación de morfismos de grupos $G \to S_n$ corresponde una clase de isomorfismo de formas torcidas del álgebra K^n y esta correspondencia es biyectiva.

Proposición 28. *Sea E/K una extensión galoisiana y finita, sea $G = \mathsf{Gal}(E/K)$ su grupo de Galois e identifiquemos a $\mathsf{Aut}_{E\text{-}\mathsf{alg}}(E^n)$ con S_n, con su acción trivial de G. Si $\phi : G \to S_n$ es un morfismo de grupos cuya imagen es un subgrupo transitivo de S_n y $N = \{g \in G : \phi(g)(1) = 1\}$, que es un subgrupo de G, entonces el subcuerpo E^N de E es una forma torcida de K^n con respecto a E/K y su clase característica $\chi([E^N]) \in H^1(G, S_n)$ es la clase de cohomología $[\phi]$.*

Demostración. (*i*) Como E^N/K es una extensión finita y separable, el teorema del elemento primitivo nos dice que existe $\alpha \in E^N$ tal que $E^N = K(\alpha)$. El grado de esta extensión es

$$[E^N : K] = [G : N] = [\phi(G) : \phi(N)] = n,$$

ya que $\phi(G)$ actúa transitivamente sobre $I = \{1, \ldots, n\}$ y el estabilizador de 1 en $\phi(G)$ es precisamente $\phi(N)$. Sea $f \in K[X]$ el polinomio minimal de α sobre K, de manera que hay un isomorfismo de K-álgebras $K(\alpha) \cong K[X]/(f)$ y $\deg f = n$. Como f es irreducible y tiene una raíz en E, que es una extensión normal y separable de K, las tiene todas y son simples.

Para cada $i \in I$ existe $g_i \in G$ tal que $\phi(g_i)(1) = i$, y podemos elegir $g_1 = 1_G$. El conjunto $\{g_1, \ldots, g_n\}$ es un sistema completo de representantes para las coclases izquierdas de N en G, de manera que $G = \bigsqcup_{i=1}^n g_i N$, y esto implica que las raíces de f son $\alpha = g_1\alpha$, $g_2\alpha$, …, $g_n\alpha$.

Se sigue de la Proposición 12 que si $\mathscr{B}$ es una base de E^N como K-espacio vectorial, entonces hay un isomorfismo $(E^N)^E_{\mathscr{B}} \cong E[X]/(f)$ de E-álgebras. Ahora bien, como la extensión E/K es normal y separable, el polinomio $f \in K[X]$ es separable y tiene todas sus raíces en E; así, existen α_1, …, $\alpha_n \in E$ distintos dos a

dos tales que $f(X) = \prod_{i=1}^{N}(X - \alpha_i)$. El teorema chino del resto nos dice entonces que

$$\frac{E[X]}{(f)} = \frac{E[X]}{\prod_{i=1}^{n}(X-\alpha_i)} \cong \frac{E[X]}{(X-\alpha_1)} \times \cdots \times \frac{E[X]}{(X-\alpha_n)} \cong E^n.$$

Así, la K-álgebra E^N es una forma torcida de K^n con repecto a E/K y podemos considerar su clase de isomorfsmo $[E^N]$ en $T_{E/K}(K^n)$.

□

Proposición 29. *Sea E/K una extensión galoisiana y finita, sea $G = \mathsf{Gal}(E/K)$ su grupo de Galois y sea $S_n = \mathsf{Aut}_{E\text{-}\mathsf{alg}}(E^n)$ con su acción trivial de G . Si $\phi : G \to S_n$ es un morfismo de grupos, existen $r \geq 1$, $n_1, \ldots, n_r \geq 1$ y un morfismo de grupos $\psi : G \to S_{n_1} \times \cdots \times S_{n_r}$ tal que tales que $n = n_1 + \cdots + n_r$,*

- *la composición de ψ con la inclusión estándar $S_{n_1} \times \cdots \times S_{n_r} \to S_n$ es conjugada a ϕ, y*
- *para cada $j \in \{1, \ldots, r\}$ la composición $\pi_j \circ \psi : G \to S_{n_j}$ de ψ con la proyección j-ésima $\pi_j : S_{n_1} \times \cdots \times S_{n_r} \to S_{n_j}$ tiene imagen transitiva.*

Si para cada $j \in \{1, \ldots, r\}$ ponemos $N_j = \{g \in G : \pi_j(\psi(g))(1) = 1\}$, entonces la K-álgebra $E^{N_1} \times \cdots \times E^{N_r}$ es una forma torcida de K^n con respecto a la extensión E/K y su clase característica en $H^1(G, S_n)$ es la clase de cohomología $[\phi]$.

Referencias

[Art59] Emil Artin, *Galois theory*, Edited and supplemented with a section on applications by Arthur N. Milgram. Second edition, with additions and revisions. Fifth reprinting. Notre Dame Mathematical Lectures, No. 2, University of Notre Dame Press, South Bend, Ind., 1959. MR0265324 (42 #234)

[Hil98] David Hilbert, *The theory of algebraic number fields*, Springer-Verlag, Berlin, 1998. Translated from the German and with a preface by Iain T. Adamson; With an introduction by Franz Lemmermeyer and Norbert Schappacher. MR1646901 (99j:01027)

[Kum55] Ernst Eduard Kummer, *Über eine besondere Art, aus complexen Einheiten gebildeter Ausdrücke*, J. Reine Angew. Math. **50** (1855), 212–232, available at http://resolver.sub.uni-goettingen.de/purl?GDZPPN002148927.

[Kum26] ———, *Zwei neue Beweise der allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist*, J. Reine Angew. Math. **50** (1826), 10–40, available at http://gdz.sub.uni-goettingen.de/index.php?id=11&PPN=GDZPPN002159929&L=1.

[Noe33] Emmy Noether, *Der Hauptgeschlechtssatz für relativ-galoissche Zahlkörper*, Math. Ann. **108** (1933), 411–419, available at http://gdz.sub.uni-goettingen.de/index.php?id=11&PPN=PPN235181684_0108&DMDID=DMDLOG_0030&L=1.

[Ser62] Jean-Pierre Serre, *Corps locaux*, Publications de l'Institut de Mathématique de l'Université de Nancago, VIII, Actualités Sci. Indust., No. 1296. Hermann, Paris, 1962 (French). MR0150130 (27 #133)