EL GRUPO DE BRAUER DE UN CUERPO

MARIANO SUÁREZ-ÁLVAREZ

Índice

Fecha: 12 de noviembre, 2014; compilado: 9 de mayo de 2015.

§1. El producto tensorial de espacios vectoriales

¶ Fijemos en toda esta sección un cuerpo $\Bbbk$. Todos los espacios vectoriales que consideramos son $\Bbbk$-espacios vectoriales.

¶ Si V es un espacio vectorial, escribimos V^* a su espacio dual. Si $S \subseteq V$, denotamos $S^\circ \subseteq V^*$ al conjunto de elementos de V^* que se anulan en todos los elementos de S.

Si $\mathscr{B} = (v_i)_{i \in I}$ es una base de V, escribimos $\mathscr{B}^* = (\hat{v}_i)_{i \in I}$ a la familia de elementos de V^* determinada por la condición de que sea $\hat{v}_i(v_j) = \delta_{i,j}$ para cada i, $j \in I$. Si V tiene dimensión finita, entonces $\mathscr{B}^*$ es una base de V^*, a la que llamamos la ***base dual*** de $\mathscr{B}$. En este caso se tiene que para cada $v \in V$ es $v = \sum_{i \in I} \hat{v}_i(v) v_i$.

¶ Si V, W, U son espacios vectoriales, entonces una ***función bilineal*** es una función $f : V \times W \to U$ tal que

$$f(av + bv', w) = af(v, w) + bf(v', w),$$
$$f(v, aw + bw') = af(v, w) + bf(v, w')$$

para cada v, $v' \in V$, w, $w' \in W$ y a, $b \in \Bbbk$. Escribimos $\mathsf{Bil}(V, W; U)$ al conjunto de todas las funciones bilineales $V \times W \to U$; se trata de un subespacio del espacio vectorial de todas las funciones $V \times W \to U$.

Una forma de construir funciones bilineales, enteramente análoga a la forma usual de construir funciones lineales fijando sus valores en una base, es la siguiente:

Lema 1.1. *Sean V, W y U espacios vectoriales y sean $(v_i)_{i \in I}$ y $(w_j)_{j \in J}$ bases de V y de W, respectivamente. Si $(u_{i,j})_{i \in I, j \in J}$ es una familia de elementos de U indexada por $I \times J$, existe exactamente una función bilineal $f : V \times W \to U$ tal que $f(v_i, w_j) = u_{i,j}$ para cada $i \in I$ y cada $j \in J$.*

Demostración. Definimos la función $f : V \times W \to U$ de la siguiente manera. Si $v \in V$ y $w \in W$, existen familias de escalares $(a_i)_{i \in I}$ y $(b_j)_{j \in J}$ tales que $a_i = 0$ para casi todo $i \in I$, $b_j = 0$ para casi todo $j \in J$, $v = \sum_{i \in I} a_i v_u$ y $w = \sum_{j \in J} b_j w_j$. Ponemos entonces

$$f(v, w) = \sum_{i \in I, j \in J} a_i b_j u_{i,j}.$$

Notemos que esto tiene sentido porque hay un número finito de términos no nulos. Es inmediato verificar que la función f así definida es bilineal: esto establece la afirmación sobre existencia del enunciado.

Para ver la uniciadad, alcanza con que mostremos que si $g : V \times W \to U$ es una función bilineal tal que $g(v_i, w_j) = 0$ para cada $i \in I$ y cada $j \in J$, entonces $g = 0$. Pero si g satisface esa condición y $v \in V$ y $w \in W$, existen como antes familias de escalares $(a_i)_{i \in I}$ y $(b_j)_{j \in J}$ tales que $a_i = 0$ para casi todo $i \in I$, $b_j = 0$ para casi todo $j \in J$, $v = \sum_{i \in I} a_i v_u$ y $w = \sum_{j \in J} b_j w_j$, y

$$g(v, w) = \sum_{i \in I, j \in J} a_i b_j g(v_i, w_j) = 0.$$

Esto prueba lo que queremos. □

¶ Si V y W son dos espacios vectoriales, decimos que un par (T, ϕ) en el que T es un espacio vectorial y $\phi : V \times W \to T$ es una función bilineal es un ***producto tensorial para V y W*** si para cada función bilineal $f : V \times W \to U$ con valores es un espacio vectorial U existe exactamente una función lineal $\bar{f} : T \to U$ tal que conmuta el diagrama

$$\begin{tikzcd} & T \arrow[d, "\bar{f}"] \\ U \times V \arrow[ur, "\phi"] \arrow[r, "f"'] & V \end{tikzcd}$$

{prop:otimes:uniq}

Proposición 1.2. *Si V y W son espacios vectoriales y (T, ϕ) y (T', ϕ') son productos tensoriales para V y W, entonces hay un único isomorfismo $f : T \to T'$ que have conmutar el diagrama*

$$\begin{tikzcd} & T \arrow[d, "f"] \\ U \times V \arrow[ur, "\phi"] \arrow[r, "\phi'"'] & T' \end{tikzcd}$$

Demostración. Como (T, ϕ) y (T', ϕ') son productos tensoriales para V y W y $\phi' : V \times W \to T'$ y $\phi : V \times W \to T$ son funciones bilineales, tenemos funciones lineales $\bar{\phi}' : T \to T'$ y $\bar{\phi} : T' \to T$ tales que $\bar{\phi}' \circ \phi = \phi'$ y $\bar{\phi} \circ \phi' = \phi$.

Se sigue de esto que

$$\bar{\phi} \circ \bar{\phi}' \circ \phi = \bar{\phi} \circ \phi' = \phi,$$

y entonces si la flecha punteada en el siguiente diagrama es $\bar{\phi} \circ \bar{\phi}'$ el diagrama conmuta

$$\begin{tikzcd} & T' \arrow[d, dotted] \\ U \times V \arrow[ur, "\phi'"] \arrow[r, "\phi'"'] & T' \end{tikzcd}$$

Como el diagrama también conmuta si la flecha punteada es $\mathsf{id}_{T'}$, vemos que $\bar{\phi} \circ \bar{\phi}' = \mathsf{id}_{T'}$. Procediendo de la misma forma, podemos concluir que también $\bar{\phi}' \circ \bar{\phi} = \mathsf{id}_T$. Así, las funciones $\bar{\phi}$ y $\bar{\phi}'$ son isomorfismos inversos. Basta entonces poner $f = \bar{\phi}'$ para probar la proposición. □

{prop:otimes:exist}

Proposición 1.3. *Si V y W son espacios vectoriales, entonces existe un producto tensorial (T, ϕ) para V y W.* □

Dejaremos la prueba de esta proposición para más adelante —más que nada porque todo lo que sigue depende solamente de la existencia y no de los detalles de la demostración.

¶ Si V y W son espacios vectoriales, la Proposición 1.3 nos dice que existe un producto tensorial (T, ϕ) para V y W. Escribimos $V \otimes W$ en lugar de T y para cada $v \in V$ y cada $u \in U$ escribimos $v \otimes w$ al elemento $\phi(v, w)$ de T; de esta forma no necesitaremos más mencionar al par (T, ϕ). Si en lugar de (T, ϕ) consideramos otro producto tensorial (T', ϕ') para V y W, sabemos que existe un único isomorfismo $f : T \to T'$ tal que $\phi' = f \circ \phi$, y entonces $f(v \otimes w)$ es el mismo elemento que denotaríamos $v \otimes w$ en T': vemos así que esta notación no introduce ambigüedades.

Como ϕ es una función bilineal, sabemos que para cada v, $v' \in V$, w, $w' \in W$ y a, $b \in \Bbbk$ se tiene que

$$(av + bv') \otimes a \cdot v \otimes w + b \cdot v' \otimes w, \tag{1}$$ {eq:otimes:dist-l}

$$v \otimes (aw + bw') = a \cdot v \otimes w + b \cdot v \otimes w. \tag{2}$$ {eq:otimes:dist-r}

Llamamos a los elementos de la forma $v \otimes w$ de $V \otimes W$ ***tensores elementales***.

{prop:otimes:span}

Proposición 1.4. *Si V y W son espacios vectoriales, entonces los tensores elementales de $V \otimes W$ generan a $V \otimes W$ como espacio vectorial y, de hecho, como grupo abeliano.*

Demostración. Probemos primero la primera afirmación. Basta mostrar que si $\lambda : V \otimes W \to \Bbbk$ es una función lineal que se anula sobre los tensores elementales de $V \otimes W$, entonces λ es idénticamente nula. En efecto, si $S \subseteq V \otimes W$ es el conjunto de los tensores elementales, esto implica que $S^\circ = 0$ y entonces que el subespacio generado por S es $\langle S \rangle = S^{\circ\circ} = 0^\circ = V \otimes W$.

Sea entonces $\lambda : V \otimes W \to \Bbbk$ una función lineal que satisface esa condición, de manera que conmuta el diagrama

$$\begin{tikzcd} & V \otimes W \arrow[d, "\lambda"] \\ U \times V \arrow[ur, "\phi"] \arrow[r, "0"'] & \Bbbk \end{tikzcd}$$

Como $(V \otimes W, \phi)$ es un producto tensorial, se sigue de esto que $\lambda = 0$.

Si ahora $x \in V \otimes W$, entonces lo que acabamos de probar implica que existen $n \geq 0$, $v_1, \ldots, v_n \in V$, $w_1, \ldots, w_n \in W$ y $a_1, \ldots, a_n \in \Bbbk$ tales que $x = \sum_{i \in [\![n]\!]} a_i \cdot v_i \otimes w_i$. Pero entonces $x = \sum_{i \in [\![n]\!]} (a_i v_i) \otimes w_i$ es una suma de tensores elementales: esto nos dice que el conjunto de tensores elementales genera a $V \otimes W$ como grupo abeliano. □

Los elementos más manejables de un producto tensorial son sus tensores elementales, pero no todo elemento es un tensor elemental. Esto nos lleva a tratar de reducir todas las cuestiones relativas a un producto tensorial a condiciones que podamos verificar sobre sus tensores elementales. Una observación útil para ello es el siguiente lema.

Lema 1.5. *Sean V y W dos espacios vectoriales y sea $f : V \to W$ un morfismo de grupos abelianos. Si $S \subseteq V$ es un subconjunto tal que todo elemento de V es suma* *de elementos de S y $f(x \cdot s) = x \cdot f(s)$ para cada $x \in \Bbbk$ y $s \in S$, entonces f es una función lineal.*

Demostración. Sean $v \in V$ y $x \in \Bbbk$. Por hipótesis, existen $n \geq 0$ y $s_1, \ldots, s_n \in S$ tales que $v = \sum_{i \in [\![n]\!]} s_i$, y entonces

$$f(x \cdot v) = f\left(x \cdot \sum_{i \in [\![n]\!]} s_i\right) = f\left(\sum_{i \in [\![n]\!]} x \cdot s_i\right) = \sum_{i \in [\![n]\!]} f(x \cdot s_i)$$

porque f es un morfismo dde grupos abelianos, y usando ahora la hipótesis, vemos que esto es igual a

$$\sum_{i \in [\![n]\!]} x \cdot f(s_i) = x \cdot \sum_{i \in [\![n]\!]} f(s_i) = x \cdot f\left(\sum_{i \in [\![n]\!]} s_i\right) = x \cdot f(v).$$

La función f es entonces lineal. □

{prop:otimes:xvw}

Proposición 1.6. *Sea V y W espacios vectoriales y sea $\mathscr{B} = (v_i)_{i \in I}$ una base de V. Si $x \in V \otimes W$, entonces una única familia $(w_i)_{i \in I}$ tal que $w_i = 0$ para casi todo $i \in I$ y $x = \sum_{i \in I} v_i \otimes w_i$.*

Demostración. De acuerdo a la Proposición 1.4, existen $n \geq 1$, $v'_1, \ldots, v'_n \in V$, $w'_1, \ldots, w'_n \in W$ y $a_1, \ldots, a_n \in \Bbbk$ tales que $x = \sum_{j \in [\![n]\!]} a_j \cdot v'_j \otimes w'_j$. Como $\mathscr{B}$ es una base de V, para cada $j \in [\![n]\!]$ existe una familia $(a_{i,j})_{i \in I}$ tal que $a_{i,j} = 0$ para casi todo $i \in I$ y $v'_j = \sum_{i \in I} a_{i,j} v_i$.

Para cada $i \in I$ sea $w_i = \sum_{j \in [\![n]\!]} a_{i,j} w'_j$. Como para casi todo $i \in I$ el conjunto $\{j \in [\![n]\!] : a_{i,j} \neq 0\}$ es vacío, es $w_i = 0$ para casi todo $i \in I$. Podemos entonces considerar la suma

$$\begin{aligned}\sum_{i \in I} v_i \otimes w_i &= \sum_{i \in I} v_i \otimes \left(\sum_{j \in [\![n]\!]} a_{i,j} w'_j\right) = \sum_{j \in [\![n]\!]} \left(\sum_{i \in I} a_{i,j} v_i\right) \otimes w'_j \\ &= \sum_{j \in [\![n]\!]} v'_j \otimes w'_j = x.\end{aligned}$$

Esto prueba la existencia que se firma en el enunciado.

Sea $\mathscr{B}^* = (\hat{v}_i)_{i \in I}$ la familia de elementos de V^* tal que $\hat{v}_i(v_j) = \delta_{i,j}$ para cada $i, j \in I$. Si $i_0 \in I$, entonces la función $\lambda_{i_0} : (v, w) \in V \otimes W \mapsto \hat{v}_{i_0}(v) w \in W$ es bilineal, así que existe una única función $\bar{\lambda}_{i_0} : V \otimes W \to V$ tal que $\bar{\lambda}_{i_0}(v \otimes w) = \hat{v}_{i_0}(v) W$ para cada $v \in V$ y cada $w \in W$. En particular, se tiene que

$$\bar{\lambda}_{i_0}(x) = \sum_{i \in I} \bar{\lambda}_{i_0}(v_i \otimes w_i) = \sum_{i \in I} \hat{v}_{i_0}(v_i) w_i = w_{i_0}.$$

Como el primer miembro de esta igualdad depende solamente de x y de la base $\mathscr{B}$, esto muestra que la familia $(w_i)_{i \in I}$ que satisface la s condiciones del enunciado está bien determinada. □

{prop:otimes:dim}

Proposición 1.7. *Sean V y W espacios vectoriales y sean $\{v_i : i \in I\}$ y $\{w_j : j \in J\}$ bases de V y de W, respectivamente. El conjunto $\mathscr{B} = \{v_i \otimes w_j : i \in I, j \in J\}$ es una base de $V \otimes W$ y, en particular, tenemos que*

$$\operatorname{dim} V \otimes W = \operatorname{dim} V \cdot \operatorname{dim} W.$$

Demostración. Sabemos que los tensores elementales generan a $V \otimes W$ como espacio vectorial, así que para ver que $\mathscr{B}$ genera a $V \otimes W$ es suficiente que mostremos que todo tensor elemental es una combinación lineal de elementos de $\mathscr{B}$. Sean entonces $v \in V$ y $w \in W$, y sean $(a_i)_{i \in I}$ y $(b_j)_{j \in J}$ familias de elementos de $\Bbbk$ tales que $a_i = 0$ para casi todo $i \in I$, $b_j = 0$ para casi todo $j \in J$, $v = \sum_{i \in I} a_i v_i$ y $w = \sum_{j \in J} b_j w_j$; estas sumas tienen sentido porque sus términos son casi todos nulos. En vista de las ecuaciones (1) y (2), es $u \otimes v = \sum_{i \in I, j \in J} a_i b_j \cdot v_i \otimes w_j$. Esto prueba lo que queríamos.

Para terminar, tenemos que mostrar que $\mathscr{B}$ es un conjunto linealmente independiente de $V \otimes W$. Supongamos entonces que tenemos escalares $a_{i,j} \in \Bbbk$ para cada $i \in I$ y $j \in J$, casi todos nulos, tales que

$$\sum_{i \in I, j \in J} a_{i,j} \cdot v_i \otimes w_j = 0. \tag{3}$$ {eq:base-1}

Sean $i_0 \in I$ y $j_0 \in J$, y sean $\lambda : V \to \Bbbk$ y $\rho : W \to \Bbbk$ las funciones lineales tales que $\lambda(v_i) = \delta_{i_0,i}$ para cada $i \in I$ y $\rho(w_j) = \delta_{j_0,j}$ para cada $j \in J$. La función $\mu : (v, w) \in V \times W \mapsto \lambda(v)\rho(w) \in \Bbbk$ es bilineal, así que tenemos una función lineal $\bar{\mu} : V \otimes W \to \Bbbk$ tal que $\bar{\mu}(v_i \otimes w_j) = \delta_{i_0,i}\delta_{j_0,j}$. De acuerdo a (3), es

$$0 = \bar{\mu}\Big(\sum_{i \in I, j \in J} a_{i,j} v_i \otimes w_j \Big) = \sum_{i \in I, j \in J} a_{i,j} \bar{\mu}(v_i \otimes w_j) = a_{i_0,j_0}.$$

Así, todos los coeficientes que aparecen en (3) son nulos. □

¶ La siguiente observación es frecuentemente útil:
Tranformar esto en un corolario de la Proposición 1.6.

{lema:w0}

Lema 1.8. *Sean V y W espacios vectoriales.*

(*i*) *Si $w_0 \in W$ es no nulo, entonces la función $f : v \in V \mapsto v \otimes w_0 \in V \otimes W$ es inyectiva.*

(*ii*) *Si $\{w_1, \ldots, w_n\} \subseteq V$ es linealmente independiente y $v_1, \ldots, v_n \in V$ son tales que $\sum_{i \in [\![n]\!]} v_i \otimes w_i = 0$ en $V \otimes W$, entonces $v_i = 0$ para todo $i \in [\![n]\!]$.*

Demostración. (*i*) Como $w_0 \neq 0$, existe una función lineal $\lambda : W \to \Bbbk$ tal que $\lambda(w_0) = 1$. Como la función $g : (v, w) \in V \times W \mapsto \lambda(w)v \in V$ es bilineal, existe una funcion lineal $\bar{g} : V \otimes W \to V$ tal que $\bar{g}(v \otimes w) = \lambda(w)v$ para cada $v \in V$ y cada $w \in W$. Si $v \in V$, entonces

$$(\bar{g} \circ f)(v) = \bar{g}(f(v)) = \bar{g}(v \otimes w_0) = \lambda(w_0)v = v,$$

de manera que $\bar{g} \circ f = \mathsf{id}_V$. Esto implica que la función f es inyectiva.

(ii) Sea $i_0 \in [\![n]\!]$. Como $\{w_1, \dots, w_n\}$ es linealmente independiente, existe una función lineal $\lambda : W \to \Bbbk$ tal que $\lambda(w_i) = \delta_{i_0,i}$ para cada $i \in [\![n]\!]$. Como la función $g : (v, w) \in V \times W \mapsto \lambda(w)v \in V$ es bilineal, existe una función lineal $\bar{g} : V \otimes W \to V$ tal que $\bar{g}(v \otimes w) = \lambda(w)v$ para cada $v \in V$ y cada $w \in W$. Ahora bien, la hipótesis es que $\sum_{i\in[\![n]\!]} v_i \otimes w_i = 0$, así que

$$0 = \sum_{i\in[\![n]\!]} \bar{g}(v_i \otimes w_i) = \sum_{i\in[\![n]\!]} \lambda(w_i)v_i = v_{i_0}.$$

Esto prueba el lema. □

¶ El producto tensorial de espacios vectoriales es asociativo y conmutativo, en el siguiente sentido preciso:

{prop:otimes:ass-comm}

Proposición 1.9. *Sean U, V, W espacios vectoriales.*

(i) *Hay un único isomorfismo*

$$\alpha : (U \otimes V) \otimes W \to U \otimes (V \otimes W)$$

tal que $\alpha((u \otimes v) \otimes w) = u \otimes (v \otimes w)$ para cada $u \in U$, $v \in V$ y $w \in W$.

(ii) *Hay un único isomorfismo*

$$\sigma : V \otimes W \to W \otimes V$$

tal que $\sigma(v \otimes w) = w \otimes v$ para cada $v \in V$ y cada $w \in W$.

Demostración. *(i)* La función

$$a : (u \otimes v, w) \in (U \otimes V) \times W \longmapsto u \otimes (v \otimes w) \in U \otimes (V \otimes W)$$

es bilineal, así que existe una única función lineal

$$\alpha : (U \otimes V) \otimes W \to U \otimes (V \otimes W)$$

tal que $\alpha((u \otimes v) \otimes w) = u \otimes (v \otimes w)$ para cada $u \in U$, $v \in V$ y $w \in W$. De la misma forma, la función

$$b : (u, v \otimes w) \in U \times (V \otimes W) \longmapsto (u \otimes v) \otimes w \in (U \otimes V) \otimes W$$

es bilineal, de manera que existe una única función lineal

$$\beta : U \otimes (V \otimes W) \to (U \otimes V) \otimes W$$

tal que $\beta(u \otimes (v \otimes w)) = (u \otimes v) \otimes w$ para cada $u \in U$, $v \in V$ y $w \in W$.

Ahora bien, si $u \in U$, $v \in V$ y $w \in W$, es claro que $(\beta\circ\alpha)((u\otimes v)\otimes w) = (u\otimes v)\otimes w$ y que $(\alpha \circ \beta)(u \otimes (v \otimes w)) = u \otimes (v \otimes w)$. Como los conjuntos

$$\{(u \otimes v) \otimes w : u \in U, v \in V, w \in W\}$$

y

$$\{u \otimes (v \otimes w) : u \in U, v \in V, w \in W\}$$

generan a $(U \otimes V) \otimes W$ y a $U \otimes (V \otimes W)$ como espacios vectoriales, esto implica que $\beta \circ \alpha = \mathsf{id}_{(U\otimes V)\otimes W}$ y $\alpha \circ \beta = \mathsf{id}_{U\otimes(V\otimes W)}$. Concluimos así que α y β son isomorfismos inversos, y esto prueba la primera parte de la proposición.

(ii) Como las funciones

$$s : (v, w) \in V \times W \mapsto w \otimes v \in W \otimes V$$

y

$$r : (w, v) \in W \times V \longmapsto v \otimes w \in V \otimes W$$

son bilineales, existen funciones lineales $\sigma : V \otimes W \to W \otimes V$ y $\rho : W \otimes V \to V \otimes W$ tales que $\sigma(v \otimes w) = w \otimes v$ y $\rho(w \otimes v) = v \otimes w$ para cada $v \in V$ y cada $w \in W$. Se sigue inmediatamente de esto que $(\rho \circ \sigma)(v \otimes w) = v \otimes w$ y $(\sigma \circ \rho)(w \otimes v) = w \otimes v$ para cada $v \in V$ y cada $w \in W$. Como los conjuntos $\{v \otimes w : v \in V, w \in W\}$ y $\{w \otimes v : w \in W, v \in V\}$ generan a $V \otimes W$ y a $W \otimes V$ como espacios vectoriales, esto es suficiente para concluir que $\sigma \circ \rho = \mathsf{id}_{W\otimes V}$ y que $\rho \circ \sigma = \mathsf{id}_{V\otimes W}$. Esto prueba la segunda parte de la proposición. □

¶ Si V y W son espacios vectoriales y $x \in V \otimes W$, sabemos que existe $r \geq 0$ tal que hay $v_1, \ldots, v_r \in V$ y $w_1, \ldots, w_r \in W$ con $x = \sum_{i=1}^{r} v_i \otimes w_i$. El menor r con esta propiedad es el ***rango*** de x. El rango del elemento nulo es cero y es el único que tiene ese rango.

La elección del nombre está motivada por la siguiente observación:

Proposición 1.10. *Sea V un espacio vectorial de dimensión finita y sea V^* su espacio dual. Hay una función lineal $f : V \otimes V^* \to \mathsf{End}(V)$ tal que $f(v \otimes \lambda)(u) = \lambda(u)v$ para cada v, $u \in V$ y cada $\lambda \in V^*$. Esta función es biyectiva, y si $x \in V \otimes V^*$, entonces el rango de x es igual al rango de $f(x)$ en tanto función lineal $V \to V$.*

Demostración. Sea $g : V \times V^* \to \mathsf{End}(V)$ la función tal que $g(v, \lambda)(u) = \lambda(u)v$ para cada v, $u \in V$ y $\lambda \in V^*$. Se trata de una función bilineal, así que existe una función lineal $\bar{g} : V \otimes V^* \to \mathsf{End}(V)$ tal que $\bar{g}(v \otimes \lambda) = g(v, \lambda)$ para todo $v \in V$ y $\lambda \in V^*$.

Sea $h \in \mathsf{End}(V)$ y supongamos que su rango es $s = \mathsf{rg}\, h$. Sea $\{v_1, \ldots, v_n\}$ una base de V elegida de manera que $\{v_1, \ldots, v_s\}$ es una base de la imagen $h(V)$, y sea $\{\hat{v}_1, \ldots, \hat{v}_n\}$ la base dual correspondiente de V^*. Si $h \in \mathsf{End}(V)$ y ponemos $x = \sum_{i,j\in[\![n]\!]} \hat{v}_j(h(v_i)) \cdot v_j \otimes \hat{v}_i$, entonces para cada $v \in V$ tenemos que

$$\begin{aligned} f(x)(v) &= \sum_{i,j\in[\![n]\!]} \hat{v}_j(h(v_i)) \cdot f(v_j \otimes \hat{v}_i)(v) = \sum_{i,j\in[\![n]\!]} \hat{v}_j(h(v_i)) \cdot \hat{v}_i(v) \cdot v_j \\ &= \sum_{i\in[\![n]\!]} \hat{v}_i(v) \cdot h(v_i) = h\Big(\sum_{i\in[\![n]\!]} \hat{v}_i(v) \cdot v_i\Big) = h(v), \end{aligned}$$

de manera que $f(x) = h$. Esto nos dice que f es sobreyectiva; como tanto su dominio dominio como su codominio tienen dimensión n^2, esto implica que, de hecho, se trata de un isomorfismo. Más aún, notemos que si $j \in \{s+1, \dots, n\}$ es $\hat{v}_j(h(v_i)) = 0$, y entonces

$$x = \sum_{j \in [\![s]\!]} v_j \otimes \Big(\sum_{i \in [\![n]\!]} \hat{v}_j(h(v_i)) \hat{v}_i \Big).$$

Vemos así que $\operatorname{\mathsf{rg}} x \leq s = \operatorname{\mathsf{rg}} f(x)$.

Sea $x \in V \otimes V^*$ un elemento no nulo. Si $r \geq 1$, $v_1, \dots, v_r \in V$ y $\lambda_1, \dots, \lambda_r \in V^*$ son tales que $x = \sum_{i \in [\![r]\!]} v_i \otimes \lambda_i$, entonces la función

$$f(x) : v \in V \mapsto \sum_{i \in [\![r]\!]} \lambda_i(v) v_i \in V$$

tiene imagen contenida en el subespacio de V generado por $\{v_1, \dots, v_r\}$. En particular, es $\operatorname{\mathsf{rg}} x \geq \operatorname{\mathsf{rg}} f(x)$. Esto y la desigualdad anterior prueban la segunda afirmación del enunciado. □

La minimalidad que define al rango de un elemento de un producto tensorial tiene la siguiente consecuencia:

{prop:rank:li}

Proposición 1.11. *Sean V y W dos espacios vectoriales y sea $x \in V \otimes W$ un elemento no nulo de rango r. Si $v_1, \dots, v_r \in V$ y $w_1, \dots, w_r \in W$ son tales que $x = \sum_{i \in [\![r]\!]} v_i \otimes w_i$, entonces las familias $(v_i)_{i \in [\![r]\!]}$ y $(w_i)_{i \in [\![r]\!]}$ son linealmente independientes en V y en W, respectivamente.*

Demostración. Supongamos que, por ejemplo, $(v_i)_{i \in [\![r]\!]}$ es linealmente dependiente. Sin pérdida de generalidad, podemos suponer entonces que existen escalares $a_2, \dots, a_r \in \Bbbk$ tales que $v_1 = \sum_{i=2}^r a_i v_i$, y entonces

$$x = v_1 \otimes w_1 + \sum_{i=2}^r v_i \otimes w_i = \sum_{i=2}^r a_i v_i \otimes w_1 + \sum_{i=2}^r v_i \otimes w_i = \sum_{i=2}^r v_i \otimes (a_i w_1 + w_i).$$

Esto es absurdo, porque contradice la minimalidad de r. □

¶ Terminamos esta sección describiendo la forma en que el producto tensorial de espacios vectoriales interactúa con las funciones lineales.

{prop:otimes:maps}

Proposición 1.12. *Sean V, V', W, W' espacios vectoriales. Si $f : V \to V'$ y $g : W \to W'$ son funciones lineales, existe una única función lineal*

$$f \otimes g : V \otimes W \to V' \otimes W'$$

tal que $(f \otimes g)(v \otimes w) = f(v) \otimes g(w)$ para cada $v \in V$ y cada $w \in W$.

Demostración. Como la función $h : (v, w) \in V \times W \mapsto f(v) \otimes g(w) \in V' \otimes W'$ es bilineal, sabemos que hay exactamente una función lineal $f \otimes g : V \otimes W \to V' \otimes W'$ tal que $(f \otimes g)(v \otimes w) = f(v) \otimes g(w)$ para cada $v \in V$ y cada $w \in W$. □

Las siguiente proposición enuncia las dos propiedades básicas de esta construcción.

{prop:otimes:functor}

Proposición 1.13. *Sean V, V', V'', W, W' y W'' espacios vectoriales.*

(*i*) *Es* $\mathsf{id}_V \otimes \mathsf{id}_W = \mathsf{id}_{V\otimes W}$.

(*ii*) *Si* $f : V \to V'$, $f' : V' \to V''$, $g : W \to W'$ *y* $g' : W' \to W''$ *son funciones lineales, entonces*

$$f' \otimes g' \circ f \otimes g = (f' \circ f) \otimes (g' \otimes g).$$

Demostración. Par aprobar ambas afirmaciones, tenemos que probar la igualdad de dos funciones lineales definidas sobre $V \otimes W$. Para ello basta ver que esas dos funciones coinciden sobre los tensores elementales de $V \otimes W$, ya que éstos generan a $V \otimes W$ como espacio vectorial, y esto es inmediato. □

{coro:otimes:isos}

Corolario 1.14. *Sean* V, V', W *y* W *espacios vectoriales. Si* $f : V \to V'$ *y* $g : W \to W'$ *son isomorfismos, entonces* $f \otimes g : V \otimes W \to V' \otimes W'$ *es un isomorfismo.*

Demostración. Sean $r : V \to V'$ y $s : W' \to W$ los isomorfismos inversos de f y de g. La Proposición 1.13 implica que

$$r \otimes s \circ f \otimes g = (r \circ f) \otimes (s \circ g) = \mathsf{id}_V \otimes \mathsf{id}_W = \mathsf{id}_{V\otimes W}$$

y, de manera similar, que $f \otimes g \circ r \otimes s = \mathsf{id}_{V'\otimes W'}$. Vemos así que $f \otimes g$ y $r \otimes s$ son isomorfismos inversos. □

§2. El producto tensorial de álgebras

¶ Fijemos otra vez un cuerpo $\Bbbk$. Todos los espacios vectoriales y, en particular, todas las álgebras que consideramos son $\Bbbk$-espacios vectoriales y $\Bbbk$-algebras.

La siguiente observación será usada muchas veces en lo que sigue:

{lema:alg:map}

Lema 2.1. *Sean A y B dos álgebras y sea $f : A \to B$ una función lineal. Si $f(1_A) = 1_B$ y existe un subconjunto $S \subseteq A$ que genera a A como espacio vectorial y tal que cada vez que s, $t \in S$ se tiene que $f(st) = f(s)f(t)$, entonces f es un morfismo de álgebras*

Demostración. Sean a, $b \in A$. Como S genera a A como espacio vectorial, existe familias finitas $(s_i)_{i\in I}$ y $(t_j)_{j\in J}$ en S y $(a_i)_{i\in I}$ y $(b_j)_{j\in J}$ en $\Bbbk$ tales que $a = \sum_{i\in I} a_i s_i$ y $b = \sum_{j\in J} b_j t_j$. Entonces $ab = \sum_{i\in I, j\in J} a_i b_j s_i t_j$, así que

$$\begin{aligned} f(ab) &= \sum_{i\in I, j\in J} a_i b_j f(s_i t_j) = \sum_{i\in I, j\in J} a_i b_j f(s_i) f(t_j) \\ &= \Bigl(\sum_{i\in I} a_i f(s_i)\Bigr)\Bigl(\sum_{j\in J} b_j f(t_j)\Bigr) = f(a)f(b). \end{aligned}$$

Como $f(1_A) = 1_B$, esto nos dice que f es un morfismo de álgebras. □

¶ Sean A y B dos álgebras. Como se trata en particular de espacios vectoriales, podemos considerar el espacio vectorial $A \otimes B$. La siguiente proposición afirma que hay una estructura de álgebra natural sobre este espacio.

Proposición 2.2. *Si A y B son dos álgebras, existe exactamente una estructura de álgebra sobre $A \otimes B$ tal que*

$$a \otimes b \cdot a' \otimes b' = aa' \otimes bb' \tag{4}$$

{eq:alg-otimes:1}

para cada a, $a' \in A$ y cada b, $b' \in B$. Su elemento identidad es $1_A \otimes 1_B$.

De ahora en adelante, cada vez que consideremos el producto tensorial de dos álgebras, lo consideraremos dotado de esta estructura de álgebra.

Demostración. Como los tensores elementales de $A\otimes B$ generan a $A\otimes B$ como espacio vectorial, es claro que hay a lo sumo una multiplicación bilineal sobre $A\otimes B$ que satisface a condiciones del enunciado. Si la hay, entonces su elemento identidad es $1_A\otimes 1_B$: en efecto, como los tensores elementales generan a $A \otimes B$ como espacio vectorial, para verificar esto alcanza con mostrar que $1_A \otimes 1_B \cdot a \otimes b = a \otimes b = a \otimes b \cdot 1_A \otimes 1_B$, lo que es inmediato en vista de (4). De la misma forma, si existe una multiplicación bilineal que satisface esa condición, entonces es asociativa: para verlo hay que mostrar que $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ para cada x, y, $x \in A \otimes B$ y, como los tensores elementales generan a $A \otimes B$ como espacio vectorial y la multiplicación es bilineal, es suficiente verificar esto cuando x, y y z son tensores elementales —y en ese caso es inmediato. Queda, entonces, probar que hay una multiplicación bilineal en $A \otimes B$ que satisface la condición (4)

Si $a \in A$, sea $\lambda_a^A : x \in A \mapsto ax \in A$, que es una función lineal. De la misma forma, si $b \in B$, tenemos la función lineal $\lambda_b^B : x \in B \mapsto bx \in B$.

Si $a \in A$ y $b \in B$, podemos considerar la función lineal

$$\lambda_a^A \otimes \lambda_b^B : A \otimes B \to A \otimes B$$

y tenemos, de hecho, una función

$$\Lambda : (a, b) \in A \times B \longmapsto \lambda_a^A \otimes \lambda_b^B \in \mathsf{hom}(A \otimes B, A \otimes B)$$

que es bilineal. Existe entonces una función lineal

$$\bar{\Lambda} : A \otimes B \to \mathsf{hom}(A \otimes B, A \otimes B)$$

tal que $\bar{\Lambda}(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ para cada a, $a' \in A$ y cada b, $b' \in B$. Podemos entonces definir una función $\mu : (A \otimes B) \times (A \otimes B) \to A \otimes B$ poniendo para cada a, $a' \in A$ y cada b, $b' \in B$

$$\mu(a \otimes b, a' \otimes b') = \bar{\Lambda}(a \otimes b)(a' \otimes b').$$

Es inmediato verificar que esta función μ es bilineal. Esto muestra que existe una multiplicación bilineal en $A \otimes B$ que satisface la condición (4) y, entonces, prueba la proposición. □

Esta construcción es compatible con los morfismos:

{prop:otimes:alg-map}

Proposición 2.3. *Sean A, A', B, B' algebras. Si $f : A \to A'$ y $g : B \to B'$ son morfismos de álgebras, entonces la función lineal*

$$f \otimes g : A \otimes B \to A' \otimes B'$$

es un morfismo de álgebras.

Demostración. Tenemos que mostrar que es un morfismo de anillos. Para eso alcanza con que mostremos que si a_1, $a_2 \in A$ y b_1, $b_2 \in B$ se tiene que

$$(f \otimes g)(a_1 \otimes b_1 \cdot a_2 \otimes b_2) = (f \otimes g)(a_1 \otimes b_1) \cdot (f \otimes g)(a_2 \otimes b_2),$$

ya que los tensores elementales generan a $A \otimes B$ como espacio vectorial, y esto es inmediato. □

¶ La asociatividad y la conmutatividad del producto tensorial de espacios vectoriales tiene su correlato en el producto tensorial de álgebras.

{prop:otimes:alg:ass}

Proposición 2.4. *Sean A, B y C tres álgebras.*

(*i*) *Hay un único isomorfismo de álgebras $\alpha : (A \otimes B) \otimes C \to A \otimes (B \otimes C)$ tal que $\alpha((a \otimes b) \otimes c) = a \otimes (b \otimes c)$ para cada $a \in A$, $b \in B$ y $c \in C$.*

(*ii*) *Hay un único isomorfismo de álgebras $\sigma : A \otimes B \to B \otimes A$ tal que $\sigma(a \otimes b) = b \otimes a$ para cada $a \in A$ y cada $b \in B$.*

Demostración. En vista de la Proposición 1.9 sabemos que hay un único isomorfismo $\alpha : (A\otimes B)\otimes C \to A\otimes(B\otimes C)$ de espacios vectoriales tal que $\alpha((a\otimes b)\otimes c) = a\otimes(b\otimes c)$ para cada $a \in A$, $b \in B$ y $c \in C$, y un único isomorfismo $\sigma : A \otimes B \to B \otimes A$ de espacios vectoriales tal que $\sigma(a \otimes b) = b \otimes a$ para cada $a \in A$ y cada $b \in B$. Para probar esta proposición basta entonces mostrar que estos isomorfismos son, de hecho, isomorfismos de álgebras. Como los conjuntos $\{(a \otimes b) \otimes c : a \in A, b \in B, c \in C\}$ y $\{a \otimes b : a \in A, b \in B\}$ generan a los dominios de α y de σ como espacios vectoriales, para esto basta que mostremos que

$$\alpha\big((a \otimes b) \otimes c\big) \cdot \alpha\big((a' \otimes b') \otimes c'\big) = \alpha\big((a \otimes b) \otimes c \cdot (a' \otimes b') \otimes c'\big)$$

para cada a, $a' \in A$, b, $b' \in B$, c, $c' \in C$, y que

$$\sigma(a \otimes b) \cdot \sigma(a' \cdot b') = \sigma(a \otimes b \cdot a' \otimes b')$$

para cada a, $a \in A$ y cada b, $b' \in B$. Esto es inmediato, usando la ecuación (4). □

¶ Recordemos que si A es un álgebra, el ***centro*** de A es el subespacio

$$\mathsf{Z}(A) = \{a \in A : aa' = a'a \text{ para todo } a' \in A\}.$$

Se trata, de hecho, de una subálgebra de A que es conmutativa; en particular, tenemos que $\Bbbk 1_A \subseteq \mathsf{Z}(A)$.

{lema:center:S}

Lema 2.5. *Sea A un álgebra. Si $S \subseteq A$ es un subconjunto que genera a A como álgebra, entonces*

$$\mathsf{Z}(A) = \{a \in A : as = sa \text{ para todo } s \in S\}.$$

Demostración. Denotemos $\mathsf{Z}'(A)$ al conjunto que aparece a la derecha en la igualdad que queremos probar. Es claro que $\mathsf{Z}(A) \subseteq \mathsf{Z}'(A)$, así que bastará que probemos la contención recíproca. Sea $a \in \mathsf{Z}'(A)$.

Sea $S_0 = \{1\}$ y para cada $r \geq 1$ sea $S_r = \{st : s \in S, t \in S_{r-1}\}$. Como S genera a A en tanto álgebra, el conjunto $S_\infty = \bigcup_{r\geq 0} S_r$ genera a A en tanto espacio vectorial. Es evidente que $at = ta$ para cada $t \in S_0$. Supongamos inductivamente que $r \geq 1$ y que $at = ta$ para cada $t \in S_{r-1}$. Si $s \in S$ y $t \in S_{r-1}$, entonces $ast = sat = sta$ porque $a \in \mathsf{Z}'(A)$ y vale la hipótesis inductiva: esto nos dice que $at = ta$ para cada $t \in S_r$. Concluimos de esta forma, de hecho, que $at = ta$ para todo $t \in S_\infty$.

Si ahora $a' \in A$, sabemos que existen $n \geq 1$, $t_1, \ldots, t_n \in S_\infty$ y $b_1, \ldots, b_n \in \Bbbk$ tales que $a' = \sum_{i\in[\![n]\!]} b_i t_i$, y entonces $aa' = \sum_{i\in[\![n]\!]} b_i a t_i = \sum_{i\in[\![n]\!]} b_i t_i a = a'a$. Así, es $a \in \mathsf{Z}(a)$, como queríamos. □

¶ Decimos que un álgebra A es ***central*** si $\mathsf{Z}(A) = \Bbbk 1_A$.

{prop:otimes:central}

Proposición 2.6. *Sean A y B dos álgebras. Si B es central, entonces hay un isomorfismo de álgebras $f : \mathsf{Z}(A) \to \mathsf{Z}(A \otimes B)$ tal que $f(a) = a \otimes 1_B$ para cada $a \in \mathsf{Z}(A)$.*

Demostración. La función $f : a \in \mathsf{Z}(A) \mapsto a \otimes 1_B \in A \otimes B$ es lineal. Si $a \in \mathsf{Z}(A)$, $a' \in A$ y $b' \in B$, entonces

$$\begin{aligned} a' \otimes b' \cdot f(a) &= a' \otimes b' \cdot a \otimes 1_B = a'a \otimes b' = aa' \otimes b' = a \otimes 1_B \cdot a' \otimes b' \\ &= f(a) \cdot a' \otimes b'. \end{aligned}$$

Como el conjunto $\{a' \otimes b' : a' \in A, b' \in B\}$ genera a $A \otimes B$ como álgebra, esto, junto el Lema 2.5, nos permite concluir que $f(a) \in \mathsf{Z}(A \otimes B)$.

Se sigue del Lema 1.8 que la función f es inyectiva. Para terminar, queda que mostremos que su imagen en $\mathsf{Z}(A \otimes B)$.

Sea entonces $x \in \mathsf{Z}(A \otimes B)$. Existen $n \geq 0$, un conjunto linealmente independiente $\{a_1, \ldots, a_n\}$ en A y $b_1, \ldots, b_n \in B$ tales que $x = \sum_{i=1}^{n} a_i \otimes b_i$. Si $b \in B$, entonces como x es central en $A \otimes B$ es

$$0 = 1 \otimes b \cdot x - x \cdot 1 \otimes b = \sum_{i \in [\![n]\!]} a_i \otimes (bb_i - b_i b).$$

Como $\{a_1, \ldots, a_n\}$ es linealmente independiente, esto implica que $bb_i = b_i b$ para cada $i \in [\![n]\!]$. Como b es arbitrario, vemos así que $b_1, \ldots, b_n \in \mathsf{Z}(B) = \Bbbk 1_B$. Existen entonces escalares $\lambda_1, \ldots, \lambda_n \in \Bbbk$ tales que $b_i = \lambda 1_B$ para cada $i \in [\![n]\!]$ y, en consecuencia,

$$x = \sum_{i \in [\![n]\!]} a_i \otimes b_i = \Big(\sum_{i \in [\![n]\!]} \lambda_i a_i \Big) \otimes 1_B.$$

Así, existe $a \in A$ tal que $x = a \otimes 1_B$. Si ahora $a' \in A$, entonces como x es central en $A \otimes B$ es

$$0 = a' \otimes 1_B \cdot x - x \cdot a' \otimes 1_B = (a'a - aa') \otimes 1_B,$$

de manera que $a'a = aa'$. La arbitrariedad de a' en A, ahora, implica que $a \in \mathsf{Z}(A)$. Concluimos de esta forma que $x = a \otimes 1_B = f(a)$, como queríamos. □

{coro:otimes:central}

Corolario 2.7. *Si A y B son dos álgebras centrales, entonces $A \otimes B$ también es central.*

Demostración. De acuerdo a la proposición, la función $a \in \mathsf{Z}(A) \mapsto a \otimes 1_B \in \mathsf{Z}(A \otimes B)$ es un isomorfismo porque B es central. Por otro lado, como A es central, la función $\lambda \in \Bbbk \mapsto \lambda\, 1_A \in \mathsf{Z}(A)$ es un isomofismo. Componiendo estas funciones vemos que $\lambda \in \Bbbk \mapsto \lambda\, 1_{A \otimes B} \in \mathsf{Z}(A \otimes B)$ es un isomorfismo. □

§3. Álgebras centrales simples

¶ Un álgebra es ***simple*** si no tiene ideales biláteros no nulos propios.

¶ En general, el producto tensorial de dos álgebras simples no es simple. Hay un caso especial e importante en el que sí podemos concluir eso:

{prop:simple:otimes}

Proposición 3.1. *Si A es un álgebra central y simple y B es un álgebra simple, entonces el producto tensorial $A \otimes B$ también simple.*

Demostración. Sea $I \subseteq A \otimes B$ un ideal no nulo; queremos probar que $I = A \otimes B$. Sea x un elemento no nulo de I de rango mínimo n. Sean $a_1, \dots, a_n \in A$ y $b_1, \dots, b_n \in B$ tales que $x = \sum_{i \in [\![n]\!]} a_i \otimes b_i$; de la Proposición 1.11 sabemos que podemos suponer que la familia $(b_1, \dots, b_n)$ es linealmente independiente.

De la definición del rango de x se sigue que $a_1 \neq 0$, así que el ideal bilátero Aa_1A de A es no nulo. Como A es simple, esto implica que $1_A \in Aa_1A$ y entonces existen $m \geq 1$ y $l_1, r_1, \dots, l_m, r_m \in A$ tales que $1_A = \sum_{j \in [\![m]\!]} l_j a_1 r_j$.

Sea $y = \sum_{j \in [\![m]\!]} (l_j \otimes 1_B \cdot x \cdot r_j \otimes 1_B)$, que es un elemento de I. Para cada $i \in [\![n]\!]$ ponemos $a'_i = \sum_{j \in [\![m]\!]} l_j a_i r_j$, de manera que es $y = \sum_{i \in [\![n]\!]} a'_i \otimes b_i$. Notemos que es $a'_1 = 1_A$. Si $a \in A$, entonces el elemento

$$a \otimes 1_B \cdot y - y \cdot a \otimes 1_B = \sum_{i \in [\![n]\!]} (aa'_i - a'_i a) \otimes b_i$$

tiene rango *menor* que n —ya que el término que corresponde a $i = 1$ se anula— y pertenece a I: esto solo es posible si es nulo, en vista de la forma en que elegimos a x. Como la familia $(b_1, \dots, b_n)$ es linealmente independiente, la segunda parte del Lema 1.8 nos dice que $aa'_i = a'_i a$ para cada $i \in [\![n]\!]$. Así, es $a'_1, \dots, a'_n \in \mathsf{Z}(A) = \Bbbk 1_A$, y existen entonces $\lambda_1, \dots, \lambda_n \in \Bbbk$ tales que $a'_i = \lambda_i 1_A$ para cada $i \in [\![n]\!]$. Observemos que $\lambda_1 = 1$, ya que $a'_1 = 1_A$.

Vemos así que $y = \sum_{i \in [\![n]\!]} \lambda_i 1_A \otimes b_i = 1_A \otimes b$ con $b = \sum_{i \in [\![n]\!]} \lambda_i b_i$. Como $(b_1, \dots, b_n)$ es linealmente independiente y $\lambda_1 \neq 0$, es $b \neq 0$ y en consecuencia el ideal bilátero BbB de B es no nulo. Como B es simple, esto significa que existen $k \geq 1$ y $s_1, t_1, \dots, s_k, t_k \in B$ tales que $\sum_{j \in [\![k]\!]} s_j b t_j = 1_B$, y entonces

$$1_{A \otimes B} = 1_A \otimes 1_B = \sum_{j \in [\![k]\!]} (1_A \otimes s_j \cdot y \cdot 1_A \otimes t_j) \in I.$$

Así, el ideal I no es un ideal propio de $A \otimes B$, que es lo que teníamos que mostrar. □

Ejemplo 3.2. Sea p un número primo, sea $\Bbbk = \mathbb{F}_p(t)$ el cuerpo de funciones racionales en una variable t con coeficientes en el cuerpo de Galois $\mathbb{F}_p$, sea $t^{1/p}$ una raíz p-ésima de t en una clausura algebraica de $\Bbbk$ y sea $A = \Bbbk(t^{1/p})$, que es una $\Bbbk$-álgebra de dimensión p. Como se trata de un cuerpo, A es un álgebra simple. Sin embargo, el álgebra álgebra $A \otimes A$ no es simple. En efecto, sea $x = t^{1/p} \otimes 1 - 1 \otimes t^{1/p}$. Se trata de un elemento no nulo de $A \otimes A$ y

$$x^p = t \otimes 1 - 1 \otimes t = 0$$

ya que $t \in \Bbbk$. Como x es nilpotente, el ideal (x) de $A \otimes A$ es propio. Por supuesto, el álgebra A no es central, ya que es conmutativa de dimensión mayor que 1. $\square$

¶ Si A es un álgebra, el ***álgebra opuesta*** a A es el álgebra A^{op} que concide con A en tanto espacio vectorial y cuyo producto $\cdot_{\mathsf{op}}$ es tal que

$$a \cdot_{\mathsf{op}} b = ba$$

para cada a, $b \in A$.

{prop:aaop}

Proposición 3.3. *Si A es un álgebra central y simple, entonces A^{op} también es central y simple. Si A tiene dimensión finita, hay un isomorfismo de álgebras*

$$A \otimes A^{\mathsf{op}} \cong \mathsf{End}(A).$$

Demostración. Es inmediato verificar que el centro de A^{op} es el mismo que el de A —esto tiene sentido, ya que ambas álgebras tienen el mismo espacio vectorial subyacente— y que los ideales biláteros de A^{op} son los mismos que los de A. Esto prueba la primera afirmación.

Supongamos ahora que A tiene dimensión finita. La función $f : A \times A^{\mathsf{op}} \to \mathsf{End}(A)$ tal que $f(a,b)(x) = abx$ para cada $a \in A$, $b \in A^{\mathsf{op}}$ y $x \in A$, es bilineal, así que existe una función lineal $\bar{f} : A \otimes A^{\mathsf{op}} \to \mathsf{End}(A)$ tal que $f(a \otimes b)(x) = axb$ para cada $a \in A$, $b \in A^{\mathsf{op}}$ y $x \in A$.

Esta función $\bar{f}$ es un morfismo de álgebras. Para verlo, alcanza con verificar que $\bar{f}(a \otimes b) \circ \bar{f}(a' \otimes b') = \bar{f}(a \otimes b \cdot a' \otimes b')$ para cada a, $a' \in A$ y b, $b' \in A^{\mathsf{op}}$, ya que los tensores elementales generan al álgebra $A \otimes A^{\mathsf{op}}$ como espacio vectorial, y esto es inmediato, teniendo en cuenta que $a \otimes b \cdot a' \otimes b' = aa' \otimes b'b$ en el álgebra $A \otimes A^{\mathsf{op}}$.

Como A y A^{op} son centrales y simples, la Proposición 3.1 nos dice que $A \otimes A^{\mathsf{op}}$ es un álgebra simple y, en consecuencia, el morfismo de álgebras $\bar{f}$ tiene que ser inyectivo. Se trata por lo tanto de un isomorfismo, ya que su dominio y su codominio tienen la misma dimensión: en efecto, es $\mathsf{dim}\, A \otimes A^{\mathsf{op}} = (\mathsf{dim}\, A)^2 = \mathsf{dim}\, \mathsf{End}(A)$. $\square$

§4. Álgebras de matrices

¶ Si A es un álgebra y $n \geq 1$, escribimos $\mathsf{M}_n(A)$ al álgebra de las matrices n-por-n con coeficientes en A. Si $i, j \in [\![n]\!]$ y $a \in A$, escribimos $e_{i,j}(a)$ a la matriz de $\mathsf{M}_n(\Bbbk)$ que tiene todas sus componentes nulas, salvo por la (i,j)-ésima, que es igual a a; si $a = 1_A$, escribimos simplemente $e_{i,j}$ en lugar de $e_{i,j}(1_A)$. La familia $(e_{i,j})_{i,j\in[\![n]\!]}$ es una base de $\mathsf{M}_n(A)$ como A-módulo izquierdo, es

$$1_{\mathsf{M}_n(A)} = \sum_{i\in[\![n]\!]} e_{i,i},$$

y si $i, j, k, l \in [\![n]\!]$ y $a, b \in A$, se tiene que

$$e_{i,j}(a) \cdot e_{k,l}(b) = \delta_{j,k}\, e_{i,l}(ab).$$

{prop:otimes:ma}

Proposición 4.1. *Si A es un álgebra y $n, m \geq 1$, entonces hay un isomorfismo de álgebras $\mathsf{M}_n(\Bbbk) \otimes A \cong \mathsf{M}_n(A)$.*

Demostración. Sea $f : \mathsf{M}_n(\Bbbk) \times A \to \mathsf{M}_n(A)$ la función tal que si $m = (m_{i,j})_{i,j\in[\![n]\!]}$ es un elemento de $\mathsf{M}_n(\Bbbk)$ y $a \in A$ es $f(m,a) = \sum_{i,j\in[\![n]\!]} m_{i,j} e_{i,j}(a)$. Es inmediato verificar que se trata de una función bilineal, así que determina una función $\bar{f} : \mathsf{M}_n(\Bbbk) \otimes A \to \mathsf{M}_n(A)$ tal que $\bar{f}(e_{i,j} \otimes a) = e_{i,j}(a)$ para cada $i, j \in [\![n]\!]$ y cada $a \in A$. Consideremos, por otro lado, la función $g : \mathsf{M}_n(A) \to \mathsf{M}_n(\Bbbk) \otimes A$ tal que si $M = (M_{i,j})_{i,j\in[\![n]\!]} \in \mathsf{M}_n(A)$ es $g(M) = \sum_{i,j\in[\![n]\!]} e_{i,j} \otimes M_{i,j}$. Veamos que $\bar{f}$ y g son isomorfismos de álgebras inversos.

Si $M = (M_{i,j})_{i,j\in[\![n]\!]} \in \mathsf{M}_n(A)$, entonces

$$\bar{f}(g(M)) = \sum_{i,j\in[\![n]\!]} \bar{f}(e_{i,j} \otimes M_{i,j}) = \sum_{i,j\in[\![n]\!]} e_{i,j}(M_{i,j}) = M,$$

y esto nos dice que $\bar{f} \circ g = \mathsf{id}_{\mathsf{M}_n(A)}$. Por otro lado, para ver que $g \circ \bar{f}$ es la función identidad de $\mathsf{M}_n(\Bbbk) \otimes A$ basta ver que coincide con ella en los elementos de la forma $e_{i,j} \otimes a$ con $i, j \in [\![n]\!]$ y $a \in A$, ya que estos generan a su dominio como espacio vectorial. Sean entonces $i, j \in [\![n]\!]$ y $a \in A$, y calculemos: es

$$g(\bar{f}(e_{i,j} \otimes a)) = g(e_{i,j}(a)) = e_{i,j} \otimes a,$$

en vista de la definición de la matriz $e_{i,j}(a)$.

Nos queda mostrar que $\bar{f}$ y g son isomorfismos de álgebras, y para ello alcanza a esta altura con mostrar que $\bar{f}$ es un morfismo de álgebras. Si $i, j, k, l \in [\![n]\!]$ y $a, b \in A$, entonces

$$\bar{f}(e_{i,j} \otimes a \cdot a_{k,l} \otimes b) = \bar{f}(e_{i,j} e_{k,l} \otimes ab) = \delta_{j,k} \bar{f}(e_{i,l} \otimes ab = \delta_{j,k} e_{i,l}(ab)$$

y

$$\bar{f}(e_{i,j} \otimes a) \cdot \bar{f}(e_{k,l} \otimes b) = e_{i,j}(a) \cdot e_{k,l}(b) = \delta_{j,k} e_{i,l}(a,b).$$

Que estas dos expresiones sean iguales completa la prueba. □

{prop:alg-otimes:nm}

Proposición 4.2.

(*i*) *Si* n, $m \geq 1$, *hay un isomorfismo de álgebras*

$$\mathsf{M}_m(\Bbbk) \otimes \mathsf{M}_n(\Bbbk) \cong \mathsf{M}_{mn}(\Bbbk).$$

(*ii*) *Si* A *es un álgebra y* n, $m \geq 1$, *entonces hay un isomorfismo*

$$\mathsf{M}_m(\mathsf{M}_n(A)) \cong \mathsf{M}_{mn}(A).$$

Demostración. (*i*) Hay una función bilineal $f : \mathsf{M}_m(\Bbbk) \times \mathsf{M}_n(\Bbbk) \to \mathsf{M}_{mn}(\Bbbk)$ tal que para cada i, $j \in [\![m]\!]$ y cada k, $l \in [\![n]\!]$ es $f(e_{i,j}, e_{k,l}) = e_{n(i-1)+k,n(j-1)+l}$, así que hay una función lineal $\bar{f} : \mathsf{M}_m(\Bbbk) \otimes \mathsf{M}_n(\Bbbk) \to \mathsf{M}_{mn}(\Bbbk)$ tal que para cada i, $j \in [\![m]\!]$ y cada k, $l \in [\![n]\!]$ es $\bar{f}(e_{i,j} \otimes e_{k,l}) = e_{n(i-1)+k,n(j-1)+l}$.

Como $1_{\mathsf{M}_m(\Bbbk)} = \sum_{i\in[\![m]\!]} e_{i,i}$ y $1_{\mathsf{M}_n(\Bbbk)} = \sum_{i\in[\![n]\!]} e_{i,i}$, es

$$\begin{aligned}\bar{f}(1_{\mathsf{M}_m(\Bbbk)\otimes\mathsf{M}_n(\Bbbk)}) &= \bar{f}(1_{\mathsf{M}_m(\Bbbk)} \otimes 1_{\mathsf{M}_n(\Bbbk)}) = \sum_{i\in[\![m]\!],j\in[\![n]\!]} \bar{f}(e_{i,i} \otimes e_{j,j}) \\ &= \sum_{i\in[\![m]\!],j\in[\![n]\!]} e_{n(i-1)+j,n(i-1)+j} = \sum_{k\in[\![mn]\!]} e_{k,k} = 1_{\mathsf{M}_{mn}(\Bbbk)}. \qquad (5)\end{aligned}$$ {eq:mm:1}

Por otro lado, si i, i', j, $j' \in [\![m]\!]$ y cada k, k', l, $l' \in [\![n]\!]$, entonces

$$\begin{aligned}\bar{f}(e_{i,j} \otimes e_{k,l} \cdot e_{i',j'} \otimes e_{k',l'}) &= \bar{f}(e_{i,j}e_{i',j'} \otimes e_{k,l}e_{k',l'}) \\ &= \delta_{j,i'}\delta_{l,k'} f(e_{i,j'} \otimes e_{k,l'}) = \delta_{j,i'}\delta_{l,k'} e_{n(i-1)+k,n(j'-1)+l'}\end{aligned}$$

y

$$\begin{aligned}\bar{f}(e_{i,j} \otimes e_{k,l}) \cdot \bar{f}(e_{i',j'} \otimes e_{k',l'}) &= e_{n(i-1)+k,n(j-1)+l} \cdot e_{n(i'-1)+k',n(j'-1)+l'} \\ &= \delta_{n(j-1)+l,n(i'-1)+k'} e_{n(i-1)+k,n(j'-1)+l'},\end{aligned}$$

y es fácil ver que estas dos expresiones son iguales. Como el conjunto

$$\mathscr{B} = \{e_{i,j} \otimes e_{k,l} : i, j \in [\![m]\!], k, l \in [\![n]\!]\}$$

es una base de $\mathsf{M}_m(\Bbbk)\otimes\mathsf{M}_n(\Bbbk)$ como espacio vectorial, esto junto con (5) nos permite concluir que que $\bar{f}$ es un morfismo de álgebras gracias al Lema 2.1. Finalmente, como la imagen del la base $\mathscr{B}$ es la base $\{e_{i,j} : i, j \in [\![mn]\!]$ de $\mathsf{M}_{mn}(\Bbbk)$, la función $\bar{f}$ es un isomorfismo.

(*ii*) Usando la Proposición 4.1 y la primera parte de la Proposición 2.4, obtenemos isomorfismos de álgebras

$$\begin{aligned}\mathsf{M}_m(\mathsf{M}_n(A)) &\cong \mathsf{M}_m(\Bbbk) \otimes \mathsf{M}_n(A) \cong \mathsf{M}_m(\Bbbk) \otimes (\mathsf{M}_n(\Bbbk) \otimes A) \\ &\cong (\mathsf{M}_m(\Bbbk) \otimes \mathsf{M}_n(\Bbbk)) \otimes A\end{aligned}$$

y

$$\mathsf{M}_{mn}(A) \cong \mathsf{M}_{mn}(\Bbbk) \otimes A,$$

así que el resultado buscado es consecuencia de la existencia del isomorfismo $\mathsf{M}_m(\Bbbk) \otimes \mathsf{M}_n(\Bbbk) \cong \mathsf{M}_{mn}(\Bbbk)$ probada en la primera parte. □

{prop:center:mk}

Proposición 4.3. *Si $n \geq 1$, entonces el álgebra de matrices $\mathsf{M}_n(\Bbbk)$ es central.*

Demostración. Sea $m = (m_{i,j})_{i,j\in[\![n]\!]} \in \mathsf{Z}(\mathsf{M}_n(\Bbbk))$. Sean i_0, $j_0 \in [\![n]\!]$. Si i, $j \in [\![n]\!]$, la componente (i,j)-esima del producto me_{i_0,j_0} es $\delta_{j_0,j}m_{i,i_0}$ mientras que la del producto $e_{i_0,j_0}m$ es $\delta_{i_0,i}m_{j_0,j}$. Como m es central, concluimos que es

$$\delta_{j_1,j_2}m_{i_2,i_1} = \delta_{i_1,i_2}m_{j_1,j_2}$$

para cada i_1, i_2, j_1, $j_2 \in [\![n]\!]$. Tomando $j_1 = j_2 = 1$, vemos que $m_{i,j} = 0$ si i $j \in [\![n]\!]$ son distintos, y que $m_{i,i} = m_{1,1}$ cualquiera sea $i \in [\![n]\!]$. Esto nos dice que $m = m_{1,1}I$, con $I \in \mathsf{M}_n(\Bbbk)$ la matriz identidad. □

{coro:ma:central}

Corolario 4.4. *Sea A es un álgebra, sea $n \geq 1$. Hay una función*

$$a \in \mathsf{Z}(A) \mapsto a1_{\mathsf{M}_n(A)} \in \mathsf{Z}(\mathsf{M}_n(A))$$

y es un isomorfismo de álgebras. En particular, si A es un álgebra central, entonces $\mathsf{M}_n(A)$ también es central.

Demostración. La proposición nos da un isomorfismo

$$a \in \mathsf{Z}(A) \mapsto 1_{\mathsf{M}_n(\Bbbk)} \otimes a \in \mathsf{Z}(\mathsf{M}_n(\Bbbk) \otimes A) \tag{6}$$

{eq:zma:1}

mientras que la Proposición 4.1 y su prueba nos da un isomorfismo

$$h : \mathsf{M}_n(\Bbbk) \otimes A \to \mathsf{M}_n(A)$$

tal que $h(1_{\mathsf{M}_n(A)} \otimes a) = aI$ para cada $a \in A$, que se restringe a un isomorfismo

$$h_{\mathsf{Z}} : \mathsf{Z}(\mathsf{M}_n(\Bbbk) \otimes A) \to \mathsf{Z}(\mathsf{M}_n(A)).$$

La composición de éste con el isomorfismo de (6) es la función del enunciado, que es entonces un isomorfismo. Esto prueba la primera afirmación del colorario, y la segunda sigue inmediatamente de ésta. □

{prop:simple:ma}

Proposición 4.5. *Sea A un álgebra y sea $n \geq 1$. El álgebra de matrices $\mathsf{M}_n(A)$ es simple si y solamente si A es simple.*

Demostración. Supongamos primero que A es simple y mostremos que $\mathsf{M}_n(A)$ también lo es. Sea I un ideal no nulo de $\mathsf{M}_n(A)$: hay que probar que $I = \mathsf{M}_n(A)$.

Sea $m \in I$ un elemento no nulo. Como $m \neq 0$, existen i_0, $j_0 \in [\![n]\!]$ tal que la componente (i_0, j_0)-ésima de m es $m_{i_0,j_0} \neq 0$. Como $Am_{i_0,j_0}A$ es un ideal bilátero no nulo del álgebra A, que es simple, no puede ser propio y, en particular, contiene a 1_A. Esto significa que existe $m \geq 1$ y l_1, r_1, …, l_m, $r_m \in A$ tales que $1_A = \sum_{k\in[\![m]\!]} l_k m_{1,1} r_k$. Observemos que para cada $s \in [\![n]\!]$ tenemos que

$$e_{s,s} = \sum_{k\in[\![m]\!]} e_{s,i_0}(l_k)me_{j_0,s}(r_k) \in I,$$

de manera que $1_{\mathsf{M}_n(A)} = \sum_{s\in[\![n]\!]} e_{s,s} \in I$, como queríamos.

Para probar la afirmación recíproca, supongamos que A no es simple y sea $I \subseteq A$ un ideal propio no nulo. Es inmediato verificar que el conjunto $\mathsf{M}_n(I)$ de todas las matrices de $\mathsf{M}_n(A)$ que tiene todas sus componentes en I es un ideal propio no nulo de $\mathsf{M}_n(A)$: esto muestra que esta álgebra no es simple. $\square$

§5. El grupo de Brauer de un cuerpo

¶ Si A y B son dos álgebras, decimos que A es ***similar*** a B, y escribimos $A \sim B$, si existen n, $m \geq 1$ y un isomorfismo de álgebras $\mathsf{M}_n(A) \cong \mathsf{M}_m(B)$. Observemos que es inmediato que dos álgebras isomorfismas son similares.

Proposición 5.1. *La relación de similaridad es una relación de equivalencia.*

Demostración. Que es reflexiva y simétrica es evidente, así que alcanza con mostrar que es transitiva. Supongamos que A, B y C son tres álgebras y que $A \sim B$ y que $B \sim C$, de manera que existen n, m, r, $s \geq 1$ tales que hay isomorfismos $\mathsf{M}_n(A) \cong \mathsf{M}_m(B)$ y $\mathsf{M}_r(B) \cong \mathsf{M}_s(C)$. Es claro entonces que hay isomorfismos $\mathsf{M}_r(\mathsf{M}_n(A)) \cong \mathsf{M}_r(\mathsf{M}_m(B))$ y $\mathsf{M}_m(\mathsf{M}_r(B)) \cong \mathsf{M}_m(\mathsf{M}_s(C))$. La segunda parte de la Proposición 4.2 nos dice que hay isomorfismos $\mathsf{M}_{rn}(A) \cong \mathsf{M}_r(\mathsf{M}_n(A))$, $\mathsf{M}_m(\mathsf{M}_s(C)) \cong \mathsf{M}_{ms}(C)$ y $\mathsf{M}_r(\mathsf{M}_m(B)) \cong \mathsf{M}_{rm}(B) \cong \mathsf{M}_m(\mathsf{M}_r(B))$, así que componiendo obtenemos un isomorfismo $\mathsf{M}_{rn}(A) \cong \mathsf{M}_{ms}(C)$. Resulta entonces que $A \sim C$, que es lo que queríamos mostrar. □

Proposición 5.2. *Sean A y B dos álgebras. Si A es central y simple y $A \sim B$, entonces B es central y simple.*

Demostración. La hipótesis es que existen n, $m \geq 1$ tales que hay un isomorfismo de álgebras $\mathsf{M}_n(A) \cong \mathsf{M}_m(B)$. Como A es central y simple, el Corolario 4.4 y la Proposición 4.5 nos dicen que $\mathsf{M}_n(A)$ es central y simple, así que $\mathsf{M}_m(B)$ tiene las mismas dos propiedades. Esos resultados, entonces, nos permiten concluir que B también las tiene. □

¶ Denotamos $\mathsf{Br}(\mathbb{k})$ al conjunto de las clases de similaridad de álgebras centrales simples. Si A es un álgebra central simple, escribimos $[A]$ a la clase de similaridad de A en $\mathsf{Br}(\mathbb{k})$.

Proposición 5.3. *Hay una única estructura de grupo abeliano sobre $\mathsf{Br}(\mathbb{k})$ tal que para cada par de álgebras centrales simples A y B es*

$$[A] \cdot [B] = [A \otimes B].$$

Llamamos a $\mathsf{Br}(\mathbb{k})$, dotado de esta estructura de grupo, el ***grupo de Brauer*** del cuerpo $\mathbb{k}$.

Demostración. Sean A, A', B y B' álgebras centrales simples tales que $A \sim A'$ y $B \sim B'$, de manera que existen n, m, r, $s \geq 1$ tales que hay isomorfismos de álgebras $f : \mathsf{M}_n(A) \to \mathsf{M}_m(A')$ y $g : \mathsf{M}_r(B) \to \mathsf{M}_s(B')$. De acuerdo al Corolario 2.7 y a la Proposición 3.1, las álgebras $A \otimes B$ y $A' \otimes B'$ son centrales y simples.

Sabemos que

$$\begin{aligned}\mathsf{M}_{nr}(A\otimes B) &\cong \mathsf{M}_{nr}(\Bbbk)\otimes A\otimes B\\ &\cong \mathsf{M}_n(\Bbbk)\otimes \mathsf{M}_r(\Bbbk)\otimes A\otimes B\\ &\cong \mathsf{M}_n(\Bbbk)\otimes A\otimes \mathsf{M}_r(\Bbbk)\otimes B\\ &\cong \mathsf{M}_n(A)\otimes \mathsf{M}_r(B)\end{aligned}$$

y, de la misma forma,

$$\mathsf{M}_{ms}(A'\otimes B')\cong \mathsf{M}_m(A')\otimes \mathsf{M}_s(B')$$

Como $f\otimes g : \mathsf{M}_n(A)\otimes \mathsf{M}_r(B)\to \mathsf{M}_m(A')\otimes \mathsf{M}_s(B')$ es un isomorfismo de álgebras, tenemos que $\mathsf{M}_{nr}(A\otimes B)$ y $\mathsf{M}_{ms}(A'\otimes B')$ son álgebras isomorfas y, en consecuencia, que $A\otimes B\sim A'\otimes B'$.

Hay entonces una función $\cdot : \mathsf{Br}(\Bbbk)\times \mathsf{Br}(\Bbbk)\to \mathsf{Br}(\Bbbk)$ tal que $[A]\cdot[B]=[A\otimes B]$ para cada par de álgebras centrales simples A y B. Veamos que esta función hace de $\mathsf{Br}(\Bbbk)$ un grupo abeliano.

- El álgebra trivial $\Bbbk$ es central y simple, así que determina una clase $[\Bbbk]\in \mathsf{Br}(\Bbbk)$. Si A es un álgebra central y simple, es inmediato que las funciones $a\in A\mapsto 1\otimes a\in \Bbbk\otimes A$ y $a\in A\mapsto a\otimes 1\in A\otimes \Bbbk$ son isomorfismos de álgebras, así que, en particular, es $\Bbbk\otimes A\sim A\sim A\otimes \Bbbk$ y $[\Bbbk]\cdot[A]=[A]=[A]\cdot[\Bbbk]$. Esto significa que $[\Bbbk]$ es un elemento neutro en $\mathsf{Br}(\Bbbk)$.
- Si A, B y C son álgebras centrales y simples, sabemos de la Proposición 2.4 que hay un isomorfismo de álgebras $(A\otimes B)\otimes C\cong A\otimes(B\otimes C)$, de manera que $(A\otimes B)\otimes C\sim A\otimes(B\otimes C)$ y, por lo tanto, $([A]\cdot[B])\cdot[C]=[A]\cdot([B]\cdot[C])$. La multiplicación de $\mathsf{Br}(\Bbbk)$ es entonces asociativa.
- Finalmente, si A es un álgebra central y simple, sabemos de la Proposición 3.3 que A^{op} también es central y simple y que hay un isomorfismo $A\otimes A^{\mathsf{op}}\cong \mathsf{End}(A)$. Si $n=\dim A$, entonces $\mathsf{End}(A)\cong \mathsf{M}_n(\Bbbk)$, así que vemos que $A\otimes A^{\mathsf{op}}\sim \Bbbk$, esto es, que $[A]\cdot[A^{\mathsf{op}}]=[\Bbbk]$. Concluimos así que la clase $[A]$ tiene a $[A^{\mathsf{op}}]$ como inverso a derecha en $\mathsf{Br}(\Bbbk)$. En vista de lo ya probado, se trata también, de hecho, de un inverso a izquierda.

Esto completa la prueba. □

§6. Álgebras de división

¶ El objetivo de esta sección es explicitar la relación que hay entre el grupo de Brauer y el problema de clasificar las álgebras de división.

Empezamos por un resultado auxiliar.

{lema:end}

Lema 6.1. *Sea A un álgebra.*

(i) Hay un isomorfismo de álgebras $\mathsf{End}_A(A) \cong A^{\mathsf{op}}$.

(ii) Si M es un A-módulo izquierdo y $n \geq 1$, hay un isomorfismo de álgebras $\mathsf{End}_A(M^n) \cong \mathsf{M}_n(\mathsf{End}_A(M))$.

En el primer punto, $\mathsf{End}_A(A)$ denota el álgebra de endomorfismos de A visto como A-módulo izquierdo; en la segunda, M^n es el A-módulo suma directa $M \oplus \cdots \oplus M$ de n sumandos iguales a M.

Demostración. (i) Consideremos la función $\phi : f \in \mathsf{End}_A(A) \mapsto f(1_A) \in A$, que es lineal. Si $f \in \mathsf{End}_A(A)$ es tal que $\phi(f) = f(1_A) = 0$, entonces para cada $a \in A$ tenemos que $f(a) = f(a \cdot 1_A) = a \cdot f(1_A) = 0$, de manera que f es idénticamente nula: esto muestra que ϕ es inyectiva. Por otro lado, si $b \in A$, la función $f_b : a \in A \mapsto ab \in A$ es un elemento de $\mathsf{End}_A(A)$ y $\phi(f_b) = b$: vemos así que ϕ es sobreyectiva. Se trata, entonces, de un isomorfismo de espacios vectoriales. Si f, $g \in \mathsf{End}_A(A)$, es

$$\phi(f \circ g) = f(g(1_A)) = f(g(1_A) \cdot 1_A) = g(1_A) \cdot f(1_A) = \phi(g) \cdot \phi(f),$$

así que $\phi : \mathsf{End}_A(A) \to A^{\mathsf{op}}$ es un isomorfismo de álgebras.

(ii) Si $i \in [\![n]\!]$ sean $q_i : M \to M^n$ y $p_i : M^n \to M$ los morfismos de A-módulos tales que $q_i(m) = (0, \ldots, 0, m, 0, \ldots, 0)$, como el elemento m ocupando la i-ésima coordenada, para cada $m \in M$, y $p_i(m_1, \ldots, m_n) = m_i$ para cada $(m_1, \ldots, m_n) \in M^n$. Es inmediato verificar que para cada i, $j \in [\![n]\!]$ es

$$p_i \circ q_j = \begin{cases} \mathsf{id}_M, & \text{si } i = j; \\ 0, & \text{en caso contrarior;} \end{cases}$$

y que

$$\sum_{i \in [\![n]\!]} q_i \circ p_i = \mathsf{id}_{M^n}.$$

Sea $\Phi : \mathsf{End}_A(M^n) \to \mathsf{M}_n(\mathsf{End}_A(M))$ la función tal que $\Phi(f) = (p_i \circ f \circ q_j)_{i,j \in [\![n]\!]}$ para cada $f \in \mathsf{End}_A(M^n)$. Es inmediato verificar que se trata de una función lineal. Es inyectiva: si $f \in \mathsf{End}_A(M^n)$ no es nulo, existe un elemento no nulo $(m_1, \ldots, m_n) \in M^n$ con imagen $(m'_1, \ldots, m'_n) = f(m_1, \ldots, m_n)$ no nula, así que existen i, $j \in [\![n]\!]$ tales que $m_j \neq 0$ y $m'_i \neq 0$, y entonces el morfismo $q_i \circ f \circ p_i$ no es nulo, ya que manda m_j a m'_i: esto nos dice que $\Phi(f) \neq 0$.

Por otro lado, Φ es sobreyectiva. Si $(f_{i,j})_{i,j\in[\![n]\!]}$ es un elemento de $\mathsf{M}_n(\mathsf{End}_A(M))$, entonces $f = \sum_{i,j\in[\![n]\!]} q_i \circ f_{i,j} \circ p_j$ es un elemento de $\mathsf{End}_A(M^n)$ para el que se tiene que $\Phi(f) = (f_{i,j})_{i,j\in[\![n]\!]}$, ya que para cada k, $l \in [\![n]\!]$ es

$$p_k \circ f \circ q_l = \sum_{i,j\in[\![n]\!]} p_k \circ q_i \circ f_{i,j} \circ p_j \circ q_l = p_k \circ q_k \circ f_{k,l} \circ p_l \circ q_l = f_{k,l}.$$

Finalmente, si f, $g \in \mathsf{End}_A(M^n)$, entonces

$$p_i \circ (f \circ g) \circ q_j = p_i \circ f \circ \mathsf{id}_{M^n} \circ g \circ q_j = \sum_{k\in[\![n]\!]} (p_i \circ f \circ q_k) \circ (p_k \circ g \circ q_j),$$

y esto implica que $\Phi(f \circ g) = \Phi(f) \cdot \Phi(g)$. Así, Φ es un morfismo de álgebras. □

¶ El siguiente resultado es un caso especial de un célebre teorema de Wedderburn.

{prop:wedd}

Proposición 6.2. *Si A es un álgebra simple de dimensión finita, existen un álgebra de división D y $n \geq 1$ tal que hay un isomorfismo de álgebras*

$$A \cong \mathsf{M}_n(D).$$

Si A es central, entonces D es central.

Demostración. Sea A un álgebra simple de dimensión finita. El conjunto de los ideales izquierdos de A no es vacío y cada uno de ellos es un subespacio vectorial de A: podemos entonces elegir un ideal izquierdo I minimal. El subespacio IA de A es un ideal bilátero y no nulo, así que $IA = A$ porque A es simple. Esto significa que existen $n \geq 1$ y $x_1, \ldots, x_n \in A$ tales que $1_A \in \sum_{i\in[\![n]\!]} Ix_i$, y podemos suponer que n fue elegido de manera que sea el menor entre los números que tienen esa propiedad; en particular, esa minimalidad implica que $Ix_i \neq 0$ para cada $i \in [\![n]\!]$. Como la suma es un ideal izquierdo, esto nos dice que, de hecho, $A = \sum_{i[\![n]\!]} Ix_i$.

La función $x \in I \mapsto xx_i \in Ix_i$ es claramente un morfismo sobreyectivo de A-módulos izquierdos y, como I no contiene submódulos —es decir ideales— propios no nulos, esa función es inyectiva. Vemos así que para cada $i \in [\![n]\!]$ el subespacio Ix_i es un ideal izquierdo minimal de A.

Si $i_0 \in [\![n]\!]$, entonces $Ix_{i_0} \cap \sum_{i\in[\![n]\!]\setminus\{i_0\}} Ix_i$ es un subideal de Ix_{i_0}. Si no es cero, entonces coincide con Ix_{i_0} y, en consecuencia, $\sum_{i\in[\![n]\!]\setminus\{i_0\}} Ix_i = \sum_{i\in[\![n]\!]} Ix_i = A$: esto es imposible, por la forma en que elegimos a n. Concluimos de esta forma que $A = \bigoplus_{i\in[\![n]\!]} Ix_i$. Como todos los ideales Ix_i son isomorfos a I en tanto A-módulos izquierdos, esto nos dice que hay un isomorfismo de A-módulos izquierdos $A \cong I^n$.

Sea $f : I \to I$ un endomorfismo de I como A-módulo. Tanto el núcleo como la imagen de f son submódulos de I y, como I es no tiene submódulos propios no nulos, cada uno de ellos es o bien nulo o bien coincide con I. Esto nos dice que o bien f es un isomorfismo o bien es nulo. En consecuencia, el álgebra $D = \mathsf{End}_A(I)$ es un álgebra de división.

Usando las dos partes del Lema 6.1, tenemos isomorfismos de álgebras

$$A^{\mathsf{op}} \cong \mathsf{End}_A(A) \cong \mathsf{End}_A(I^n) \cong \mathsf{M}_n(\mathsf{End}_A(I)) = \mathsf{M}_n(D)$$

así que $A \cong \mathsf{M}_n(D^{\mathsf{op}})$; por supuesto, D^{op} es un álgebra de división, ya que D lo es. Esto prueba la primera afirmación de la proposición. La segunda afirmación es consecuencia inmediata del Corolario 4.4, que implica que hay un isomorfismo de álgebras $\mathsf{Z}(D^{\mathsf{op}}) \cong \mathsf{Z}(\mathsf{M}_n(D^{\mathsf{op}})) \cong \mathsf{Z}(A)$. □

El álgebra de división D y el número n que aparecen en esta proposición están unívocamente determinados por el álgebra A. Esto es consecuencia de la Proposición 6.4 que probamos más abajo. Para hacerlo, necesitamos el siguiente lema.

{lema:wedd}

Lema 6.3.

(i) *Todos los ideales izquierdos minimales de un álgebra simple de dimensión finita son isomorfos en tanto módulos izquierdos.*

(ii) *Más generalmente, dos módulos izquierdos simples sobre un álgebra simple de dimensión finita son isomorfos.*

(iii) *Si D es un álgebra de división y $n \geq 1$, entonces para cada ideal izquierdo minimal I de $\mathsf{M}_n(D)$ hay un isomorfismo de álgebras $\mathsf{End}_{\mathsf{M}_n(A)}(I) \cong D^{\mathsf{op}}$.*

Demostración. (ii) Sea A un álgebra simple de dimensión finita y sean $I \subseteq A$ un ideal izquierdo minimal y J un A-módulo izquierdo simple. Como vimos en la prueba de la Proposición 6.2, existen $n \geq 1$ y $x_1, \ldots, x_n$ tales que para cada $i \in [\![n]\!]$ el ideal Ix_i es isomorfo a I como A-módulo izquierdo y $A = \bigoplus_{i \in [\![I]\!]} Ix_i$. Por otro lado, si $y \in J$ es un elemento no nulo, entonces la función $f : a \in A \mapsto ay \in J$ es un morfismo sobreyectivo de A-módulos izquierdos. Como $J \neq 0$ y $A = \bigoplus_{i \in [\![I]\!]} Ix_i$, es claro que existe $i_0 \in [\![n]\!]$ tal que la restricción $f|_{Ix_{i_0}} : Ix_{i_0} \to J$ no es nula. Como tanto Ix_{i_0} como J no poseen submódulos no nulos propios, esta restricción tiene que ser un isomorfismo, así que $Ix_{i_0} \cong J$. Como sabemos ya que $I \cong Ix_{i_0}$, esto prueba el lema.

(i) Como todo ideal izquierdo minimal en un álgebra es en particular un módulo izquierdo simple, esto es consecuencia directa de la parte (ii) del lema.

(iii) En la primera parte probamos que todos los ideales minimales de $A = \mathsf{M}_n(D)$ son isomorfos en tanto A-módulos izquierdos, así que todos tienen álgebras de endomorfismos isomorfas. Bastará que probemos la parte (ii), entonces, para un ideal minimal especial.

Sea $I = Ae_{1,1}$, que es un ideal izquierdo de A; sus elementos son las matrices que tienen todas sus columnas nulas, salvo posiblemente la primera. Se trata de un ideal izquierdo minimal: para verlo, basta ver que cualquiera de sus elementos no nulos lo genera en tanto ideal izquierdo. Si $x \in I \setminus 0$, existe $i \in [\![n]\!]$ tal que la componente $(i,1)$-ésima de x es $x_{i,1} \neq 0$, y entonces $e_{1,1} = e_{1,i}(x_{i,1}^{-1})x \in Ax$: esto implica que x genera a I.

Sea ahora $f : I \to I$ un morfismo de A-módulos izquierdos y sea $u = f(e_{1,1})$. Como $e_{1,1} = e_{1,1}e_{1,1}$ en A, es

$$u = f(e_{1,1}) = f(e_{1,1}e_{1,1}) = e_{1,1}f(e_{1,1}) = e_{1,1}u,$$

y esto nos dice que todas las columnas de u, salvo posiblemente la primera, son nulas. Así, existe $d \in D$ tal que $u = e_{1,1}(d)$. Vemos de esta forma que existe una función $\phi : \mathsf{End}_A(I) \to D$ tal que para cada $f \in \mathsf{End}_A(I)$ es $f(e_{1,1}) = e_{1,1}(\phi(f))$.

Si f, $g : I \to I$ son morfismos de A-módulos izquierdos, por un lado tenemos que

$$\begin{aligned}(f \circ g)(e_{1,1}) &= f\big(g(e_{1,1})\big) = f\big(e_{1,1}(\phi(g))\big) = f\big(e_{1,1}(\phi(g)) \cdot e_{1,1}\big) \\ &= e_{1,1}(\phi(g)) \cdot f(e_{1,1}) = e_{1,1}(\phi(g)) \cdot e_{1,1}(\phi(f)) \\ &= e_{1,1}\big(\phi(g) \cdot \phi(f)\big)\end{aligned}$$

y, por otro, que $(f \circ g)(e_{1,1}) = e_{1,1}(\phi(f \circ g))$, así que es $\phi(f \circ g) = \phi(g) \cdot \phi(f)$. Esto nos dice que $\phi : \mathsf{End}_A(I) \to D^{\mathsf{op}}$ es un morfismo de álgebras. En la prueba de la Proposición 6.2 vimos que $\mathsf{End}_A(I)$ es un álgebra de división, así que ϕ es necesariamente inyectiva. Por otro lado, si $d \in D$, entonces la función $f_d : x \in I \mapsto xd \in I$ es claramente un elemento de $\mathsf{End}_I(A)$ tal que $\phi(f_d) = d$, así que ϕ es sobreyectiva. El morfismo ϕ es entonces un isomofismo, y esto prueba lo que queremos. □

{prop:wedd:uniq}

Proposición 6.4. *Sean D y D' álgebras de división de dimensión finita y sean n, $m \geq 1$. Si hay un isomorfismo de álgebras $\mathsf{M}_n(D) \cong \mathsf{M}_m(D')$, entonces $D \cong D'$ y $n = m$.*

Demostración. Supongamos que $\phi : \mathsf{M}_m(D') \to \mathsf{M}_n(D)$ es un isomorfismo de álgebras y sea $I' \subseteq \mathsf{M}_m(D')$ un ideal izquierdo no nulo minimal. Es claro que $\phi(I')$ es un ideal izquierdo no nulo minimal de $\mathsf{M}_n(D)$ y que ϕ induce un isomorfismo de álgebras

$$\mathsf{End}_{\mathsf{M}_m(D')}(I') \cong \mathsf{End}_{\mathsf{M}_n(D)}(\phi(I')). \tag{7}$$ {eq:wedd:uniq}

De acuerdo a la Proposición 4.5, las álgebras $\mathsf{M}_n(D)$ y $\mathsf{M}_m(D')$ son simples, así que la segunda parte del Lema 6.3 implica que hay isomorfismos de álgebras $D \cong \mathsf{End}_{\mathsf{M}_n(D)}(\phi(I'))$ y $D' \cong \mathsf{End}_{\mathsf{M}_m(D')}(I')$. Componiendo con el isomorfismo (7), vemos que D y D' son álgebras isomorfas. En particular, estas dos álgebras tienen la misma dimensión y entonces de la igualdad

$$m^2 \dim D' = \dim \mathsf{M}_m(D') = \dim \mathsf{M}_n(D) = n^2 \dim D,$$

que se deduce de que ϕ es un isomorfismo, podemos concluir que $n = m$. □

{prop:brauer:div}

Proposición 6.5. *Sea $\mathscr{D}(\Bbbk)$ el conjunto de clases de isomorfismo de álgebras de división centrales; si D es una tal álgebra, escribamos $\langle D\rangle \in \mathscr{D}(\Bbbk)$ a su clase. La función*

$$\langle D\rangle \in \mathscr{D}(\Bbbk) \longmapsto [D] \in \mathsf{Br}(\Bbbk)$$

es una biyección.

Demostración. Llamemos ϕ a la función del enunciado.

Sea primero $\alpha \in \mathsf{Br}(\Bbbk)$. Si A es un álgebra central simple tal que $\alpha = [A]$, sabemos, de la Proposición 6.2, que existen un álgebra de división D y $n \geq 1$ tal que hay un isomorfismo $A \cong \mathsf{M}_n(D)$. Esto implica que $A \sim D$ y, en consecuencia, que $\phi(\langle D\rangle) = [A] = \alpha$. La función ϕ es, por lo tanto, sobreyectiva.

Sean ahora D y D' dos álgebras de división, y supongamos que $[D] = [D']$, de manera que existen n, $m \geq 1$ tales que hay un isomorfismo de álgebras $\mathsf{M}_n(D) \cong \mathsf{M}_m(D')$. La Proposición 6.4 nos dice entonces que D y D' son ellas mismas isomorfas como álgebras. Esto prueba que la función ϕ es inyectiva y completa la prueba de la proposición. $\square$

¶ Usando esta conexión del grupo de Brauer con las álgebras de división, podemos calcular algunos ejemplos. Empezamos, sin embargo, por un lema auxiliar.

{lema:minimal}

Lema 6.6. *Sea D un álgebra de dimensión finita y sea $x \in D$. Si $f : \Bbbk[X] \to D$ es el morfismo de álgebras tal que $f(X) = x$, entonces existe un único polinomio mónico, no constante e irreducible $p \in \Bbbk[X]$ tal que $\ker f = (p)$.*

Como es natural, llamamos a p el ***polinomio minimal de x en D.***

Demostración. Como D tiene dimensión finita y $\Bbbk[X]$ no, el núcleo de f es no trivial. Como $\Bbbk[X]$ es un dominio de ideales principales, existe un único polinomio mónico $p \in \Bbbk[X]$ tal que $\ker f = (p)$. Como $f(1_{\Bbbk[X]}) = 1_D \neq 0$, es $p \neq 1_{\Bbbk[X]}$ y, en consecuencia, p no es constante.

Supongamos que p es reducible, de manera que existen polinomios p_1, $p_2 \in \Bbbk[X]$ no constantes tal que $p = p_1p_2$. Se sigue de esto que $0 = f(p) = f(p_1)f(p_2)$ y, como D es un álgebra de división, que alguno de $f(p_1)$ o $f(p_2)$ es cero, es decir, que o p_1 o p_2 está en $\ker f$. Esto es imposible. $\square$

{prop:br:closed}

Proposición 6.7. *Si $\Bbbk$ es algebraicamente cerrado, entonces $\mathsf{Br}(\Bbbk) = 0$.*

Demostración. En vista de la Proposición 6.5, basta que mostremos que todas las álgebras de división de dimensión finita son isomorfas a $\Bbbk$.

Sea D, entonces, un álgebra de división de dimensión finita y sea $x \in D$. Hay un morfismo de álgebras $f : \Bbbk[X] \to D$ tal que $f(X) = x$. El Lema 6.6 implica que hay un polinomio $p \in \Bbbk[X]$ mónico, no constante e irreducible tal que $\ker f = (p)$. Como el cuerpo $\Bbbk$ es algebraicamente cerrado, esto implica que p tiene grado 1 y existe entonces $\alpha \in \Bbbk$ tal que $p = X - \alpha$. Como $p(x) = 0$, esto nos dice que $x - \alpha 1_D = 0$, esto es, que $x = \alpha 1_D \in \Bbbk 1_D$. Concluimos de esta forma que $D = \Bbbk 1_D$, como queríamos. $\square$

{prop:br:rr}

Proposición 6.8. *Es $\mathsf{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. La clase no trivial es la del álgebra $\mathbb{H}$ de cuaterniones.*

Demostración. Sea D una $\mathbb{R}$-álgebra de división de dimensión finita y supongamos que $\dim D > 1$, de manera que existe $x \in D \setminus \mathbb{R}1_D$. El núcleo del morfismo de álgebras $f : \mathbb{R}[X] \to D$ tal que $f(X) = x$ está generado por un polinomio $p \in \mathbb{R}[X]$ no constante, mónico e irreducible: sabemos que esto implica que $\deg p = 2$ y, entonces, que la imagen de f es una subálgebra C de D isomorfa a $\mathbb{R}[X]/(p)$ que es, a su vez, isomorfa a $\mathbb{C}$. Existe, en particular, un elemento $i \in D$ tal que $i^2 = -1$.

Sean ahora $D_+ = \{y \in D : iy = yi\}$ y $D_- = \{y \in D : iy = -yi\}$; se trata de subespacios vectoriales de D. Si $z \in D$, entonces $\frac{1}{2}(z - izi) \in D_+$ y $\frac{1}{2}(z + izi) \in D_0$, de manera que $z = \frac{1}{2}(z - izi) + \frac{1}{2}(z + izi) \in D_+ + D_-$. Por otro lado, si $z \in D_+ \cap D_-$, entonces $zi = iz = -zi$ y, en consecuencia, $2iz = 0$; como $2i \neq 0$ in D, porque $i \neq 0$, esto implica que $z = 0$. Vemos así que $D = D_+ \oplus D_-$. Es claro que 1_D, $i \in D_+$.

Si u, $v \in D_+$, entonces

$$i(uv) = iuv = uiv = uvi = (uv)i,$$

así que $uv \in D_+$. Como $1_D \in D_+$, esto implica que D_+ es una subálgebra de D. Si $u \in D_+ \setminus 0$, entonces

$$iu^{-1} = u^{-1}uiu^{-1} = u^{-1}iuu^{-1} = u^{-1}i,$$

y esto nos dice que $u^{-1} \in D_+$. Vemos de esta forma que D_+ es una subálgebra de división de D. Como contiene a C en su centro, se trata, de hecho, de una C-álgebra de división de dimensión finita y como C es un cuerpo algebraicamente cerrado, la Proposición 6.7 nos dice que $D_+ = C$. En particular, $\{1, i\}$ es una base de D_+ como espacio vectorial sobre $\mathbb{R}$.

No puede ser que sea $D_- = 0$: en ese caso sería $D = D_+$ y, en consecuencia, $i \in \mathsf{Z}(D) = \mathbb{R}1_D$ y, por hipótesis, D es central. Existe entonces un elemento no nulo $y \in D_-$. Es inmediato ver que si $z \in D_+$ es $yz \in D_-$ y que si $z \in D_-$ es $yz \in D_+$,y esto implica que tenemos funciones $z \in D_+ \mapsto yz \in D_-$ y $z \in D_- \mapsto yz \in D_+$, que claramente son lineales. Como y no es un divisor de cero en D, estas dos funciones son inyectivas y, entonces, $\dim D_+ = \dim D_-$ y $\{y, yi\}$ es una base de D_- sobre $\mathbb{R}$.

Sea $q \in \mathbb{R}[X]$ el polinomio minimal de y en D, que no es constante. Como $y \notin \mathbb{R}1_D$, q no es lineal y, como es irreducible sobre $\mathbb{R}$, su grado es necesariamente 2. Existen a, $b \in \mathbb{R}$ tales que $q = X^2 + aX + b = 0$. Se sigue de esto que

$$0 = iq(y) = i(y^2 + ay + b) = (y^2 - ay + b)i$$

y, en conscuencia, y también anula el polinomio $X^2 - aX + b$. Esto implica que $a = 0$. Como $q = X^2 + b$ es irreducible sobre $\mathbb{R}$, debe ser $b > 0$, y entonces existe $c > 0$ tal que $b = c^2$. Si ponemos $j = y/c$, entonces $y \in D_-$ y $j^2 = -1$.

Concluimos de esta forma que D tiene a $\{1, i, j, ji\}$ como base sobre $\mathbb{R}$, que $i^2 = j^2 = -1$, y que $ij = -ji$. Es evidente ahora que $D \cong \mathbb{H}$.

Hemos probado que hay exactamente dos álgebras de división reales centrales de dimension finita: $\mathbb{R}$ y $\mathbb{H}$. Como evidentemente no son isomorfas, $\mathsf{Br}(\mathbb{R})$ tiene dos elementos. La proposició sigue ahora inmediatamente. $\square$

§7. Extensión de escalares

¶ Sea $E/\Bbbk$ una extensión de cuerpos. En esta sección y las siguientes consideraremos espacios vectoriales y álgebras sobre $\Bbbk$ y sobre E. Convendremos en que los términos «espacio vectorial» y «álgebra», sin calificar, se refieren a espacios vectoriales y álgebras sobre nuestro cuerpo base $\Bbbk$, mientras que para referirnos a los conceptos correspondientes sobre E diremos «E-espacio vectorial» y «E-álgebra». Usaremos la misma convención para todos los otros conceptos relativos a un cuerpo; así, por ejemplo, haremos una diferencia entre «funciones lineales» y «funciones E-lineales».

¶ Empezamos con una construcción que produce E-espacios vectoriales a partir de espacios vectoriales.

Proposición 7.1. *Si V es un espacio vectorial, entonces el espacio vectorial $V^E = E \otimes V$ es de una única forma un E-espacio vectorial de manera que para cada e, $e' \in E$ y cada $v \in V$ es $e \cdot e' \otimes v = ee' \otimes v$.*

Decimos que el E-espacio vectorial V^E se obtiene del espacio vectorial E por ***extensión de escalares***; si es necesario poner de maniefiesto el cuerpo $\Bbbk$ lo escribiremos $V^{E/\Bbbk}$. De ahora en adelante, cada vez que mencionemos a V^E lo veremos como un E-espacio vectorial de esta forma.

Demostración. Como el conjunto de los tensores elementales de V^E genera a V^E como grupo abeliano, es claro que hay a lo sumo una estructura de E-espacio vectorial que satisface la confición del enunciado. Bastará entonces que probemos la existencia de una tal estructura.

Si $e \in E$, la función $\lambda_e^E : e' \in E \mapsto ee' \in E$ es lineal, así que hay una función lineal $\lambda_e^E \otimes \mathsf{id}_V : V^E \to V^E$ tal que $\lambda_e^E(e' \otimes v) = ee' \otimes v$ para cada $e' \in E$ y cada $v \in V$. Podemos entonces considerar la función

$$\lambda : (e, x) \in E \times V^E \mapsto \lambda_e^E(x) \in V^E,$$

que da una acción de E sobre V^E. Es inmediato verifica que esta acción hace del grupo abeliano subyacente a V^E un E-espacio vectorial. Si e, $e' \in E$ y $v \in V$, entonces $e \cdot e' \otimes v$ es, para esta acción, igual a $\lambda(e, e' \otimes v) = \lambda_e^E(e' \otimes v) = ee' \otimes v$, como queremos. □

Proposición 7.2. *Sea V un espacio vectorial. El conjunto $\{1_E \otimes v : v \in V\}$ genera a V^E como E-espacio vectorial. Si $\mathscr{B}$ es una base de V como espacio vecorial, entonces el conjunto $\mathscr{B}^E = \{1_E \otimes v : v \in \mathscr{B}\}$ es una base de V^E como E-espacio vectorial y, en particular, es*

$$\mathsf{dim}_E\, V^E = \mathsf{dim}\, V.$$

Demostración. Sea $\mathscr{B}$ una base de V. Si $x \in V^E$, de la Proposición 1.6 sabemos que existe una única familia $(e_i)_{i \in I}$ de elementos de E tal que $e_i = 0$ para casi todo

$i \in I$ y $x = \sum_{i\in I} e_i \otimes v_i = \sum_{i\in I} e_i \cdot 1_E \otimes v_i$. Vemos así que $\mathscr{B}^E$ es una base de a V^E como E-espacio vectorial.

Como $\mathscr{B}^E$ es un subconjunto de $\{1_E \otimes v : v \in V\}$, esto en particular prueba la primera afirmación de la proposición. Por otro lado, la igualdad de las dimensiones de V sobre $\Bbbk$ y de V^E sobre E es ahora inmediata. □

{prop:ext:adj}

Proposición 7.3. *Sean V un espacio vectorial y W un E-espacio vectorial. Si $f : V \to W$ es una función lineal, entonces existe exactamente una función E-lineal $\bar{f} : V^E \to W$ tal que $\bar{f}(1_E \otimes v) = f(v)$ para todo $v \in W$.*

Demostración. La función $(e, v) \in E \times V \mapsto e \cdot f(v) \in W$ es bilineal, así que existe una función $\bar{f} : V^E \to W$ que satisface la condición del enunciado y, como el conjunto $\{1_E \otimes v : v \in V\}$ geenera a V^E como E-espacio vectorial, esta función $\bar{f}$ es la única que la satisface. □

La extensión de escalares también puede hacerse con las funciones lineales, con las propiedades esperables:

{prop:ext:functor}

Proposición 7.4.

(*i*) *Si V y W son espacios vectoriales y $f : V \to W$ es una función lineal. entonces la función $f^E = \mathsf{id}_E \otimes f : V^E \to W^E$ es E-lineal.*

(*ii*) *Si V es un espacio vectorial, entonces la función $(\mathsf{id}_V)^E : V^E \to V^E$ es la función identidad de V^E.*

(*iii*) *Si V, W, U son espacios vectoriales y $f : V \to W$ y $g : W \to U$ son funciones lineales, entonces $(g \circ f)^E = g^E \circ f^E$.*

(*iv*) *Si V y W son espacios vectoriales y $f : V \to W$ es un isomorfismo de espacios vectoriales, entonces $f^E : V^E \to W^E$ es un isomorfismo de E-espacios vectoriales.*

Si es necesario poner de manifiesto el cuerpo $\Bbbk$, escribiremos $f^{E/\Bbbk}$ en lugar de simplemente f^E.

Demostración. Las partes (*ii*) y (*iii*) son consecuencias directas de la primera y la segunda parte de la Proposición 1.13. Mostremos la parte (*i*). Si e, $e' \in E$ y $v \in V$, entonces

$$\begin{aligned} f^E(e \cdot e' \otimes v) &= (\mathsf{id}_E \otimes f)(ee' \otimes v) = ee' \otimes f(v) = e \cdot e' \otimes f(v) \\ &= e \cdot (\mathsf{id}_E \otimes f)(e' \otimes v) = e \cdot f^E(e' \otimes v). \end{aligned}$$

Como el conjunto de los tensores elementales de V^E genera a V^E como grupo abeliano, esto es suficiente para concluir que f^E es E-lineal.

Veamos finalmente la veracidad de la última afirmación. Si $f : V \to W$ es un isomorfismo de espacios vectoriales, entonces existe una función lineal $g : W \to V$ tal que $g \circ f = \mathsf{id}_V$ y $f \circ g = \mathsf{id}_W$, en consecuencia

$$g^E \circ f^E = (g \circ f)^E = (\mathsf{id}_V)^E = \mathsf{id}_{V^E}$$

en vista de lo que ya probamos. De la misma forma es $f^E \circ g^E = \mathsf{id}_{W^E}$, de manera que f^E es un isomorfismo de E-espacios vectoriales. □

Finalmente, la construcción de la extensión de escalares y la del producto tensorial son compatibles:

{prop:ext:otimes}

Proposición 7.5.

(i) Si V y W son espacios vectoriales, entonces existe un isomorfismo de E-espacios vectoriales $\eta_{V,W} : V^E \otimes_E W^E \to (V \otimes W)^E$ tal que para cada $v \in V$ y cada $w \in W$ es $\eta_{V,W}((1_E \otimes v) \otimes (1_E \otimes w)) = 1_E \otimes (v \otimes w)$.

(ii) Si V, V', W, W' son espacios vectoriales y $f : V \to V'$ y $g : W \to W'$ son funciones lineales, entonces conmuta el diagrama

$$\begin{tikzcd} V^E \otimes W^E \arrow[r, "f^E \otimes g^E"] \arrow[d, "\eta_{V,W}"'] & V'^E \otimes W'^E \arrow[d, "\eta_{V',W'}"] \\ (V \otimes W)^E \arrow[r, "(f \otimes g)^E"] & (V' \otimes W')^E \end{tikzcd}$$

Demostración. (i) Si $v \in V$, tenemos una función lineal $l_v : w \in W \mapsto v \otimes w \in V \otimes W$, así que podemos considerar la función E-lineal $(l_v)^E : W^E \to (V \otimes W)^E$. Hay entonces una función $L : v \in V \mapsto (l_v)^E \in \mathsf{hom}_E(W^E, (V \otimes W)^E)$. Si a, $a' \in \Bbbk$ y v, $v' \in V$, entonces para cada $w \in W$ es

$$\begin{aligned} L(av + a'v')(1_E \otimes w) &= (l_{av+a'v'})^E(1_E \otimes w) = 1_E \otimes ((av + a'v') \otimes w) \\ &= a \cdot 1_E \otimes (v \otimes w) + a' \cdot 1_E \otimes (v' \otimes w) \\ &= a \cdot (l_v)^E(1_E \otimes w) + a' \cdot (l_{v'})^E(1_E \otimes w) \\ &= \big(a \cdot L(v) + a' \cdot L(v')\big)(1_E \otimes w). \end{aligned}$$

Como el conjunto $\{1_E \otimes w : w \in W\}$ genera a W^E como E-espacio vectorial, esto es suficiente para probar que $L(av + a'v') = aL(v) + a'L(v')$ y, en consecuencia, que la función L es lineal. La Proposición 7.3 nos dice entonces que existe una función E-lineal $\bar{L} : V^E \to \mathsf{hom}_E(W^E, (V \otimes W)^E)$ tal que $\bar{L}(1_E \otimes v) = L(v)$ para todo $v \in V$, y podemos definir una función

$$e_{V,W} : (x, y) \in V^E \times W^E \longmapsto \bar{L}(x)(y) \in (V \otimes W)^E.$$

La E-linealidad de $\bar{L}$ implica inmediatamente que $e_{V,W}$ es E-bilineal, y entonces existe una función E-lineal $\eta_{V,W} : V^E \otimes_E W^E \to (V \otimes W)^E$ tal que para cada $v \in V$ y cada $w \in W$ es

$$\begin{aligned} \eta_{V,W}((1_E \otimes v) \otimes (1_E \otimes w)) &= \bar{L}(1_E \otimes v)(1_E \otimes w) = L(v)(1_E \otimes w) \\ &= (l_v)^E(1_E \otimes w) = 1_E \otimes l_v(w) \\ &= 1_E \otimes (v \otimes w). \end{aligned} \tag{8}$$

{eq:ext:1}

La función $r : (v, w) \in V \times W \mapsto (1_E \otimes v) \otimes (1_E \otimes w) \in V^E \otimes_E W^E$ es bilineal, así que existe una función $\bar{r} : V \otimes W \to V^E \otimes_E W^E$ tal que $\bar{r}(v \otimes w) = (1_E \otimes v) \otimes (1_E \otimes w)$

para cada $v \in V$ y cada $w \in W$. Usando la Proposición 7.3, concluimos que existe una función $R : (V \otimes W)^E \to V^E \otimes_E W^E$ tal que para cada $x \in V \otimes W$ es $R(1_E \otimes x) = \bar{r}(x)$. En particular, si $v \in V$ y $w \in W$ es $R(1_E \otimes (v \otimes w)) = (1_E \otimes v) \otimes (1_E \otimes w)$.

Usando ésto y la expresión (8), es inmediato verificar que las composiciones $R \circ \eta_{V,W}$ y $\eta_{V,W} \circ R$ coinciden con las identidades de los E-espacios vectoriales $V^E \otimes_E W^E$ y $(V \otimes W)^E$ en los elementos de $\{(1_E \otimes v) \otimes (1_E \otimes w) : v \in V, w \in W\}$ y $\{1_E \otimes (v \otimes w) : v \in V, w \in W\}$, respectivamente. Como estos conjuntos generan a $V^E \otimes_E W^E$ y a $(V \otimes W)^E$ como E-espacios vectoriales, esto nos permite concluir que $\eta_{V,W}$ y R son isomorfismos de E-espacios vectoriales inversos. Esto completa la prueba de la primera parte de la proposición.

(ii) Como el conjunto $\{(1_E \otimes v) \otimes (1_E \otimes w) : v \in V, w \in W\}$ genera a $V^E \otimes_E W^E$ como E-espacio vectorial y todas las funciones que aparecen en el diagrama son E-lineales, para ver que el diagrama conmuta es suficiente con ver que conmuta sobre los elementos de aquél conjunto. Esto es inmediato. □

{prop:ext:trans}

Proposición 7.6. *Sea F/E una extensión de cuerpos.*

(i) *Si V es un espacio vectorial, hay un isomorfismo $\tau : (V^{E/\Bbbk})^{F/E} \to V^{F/\Bbbk}$ de F-espacios vectoriales tal que $\tau(1_F \otimes (1_E \otimes v)) = 1_F \otimes v$ para todo $v \in V$.*

(ii) *Si V y W son espacios vectoriales y $f : V \to W$ es una función lineal, entonces las funciones F-lineales $(f^{E/\Bbbk})^{F/E}$ y $f^{F/\Bbbk}$ son iguales.*

Demostración. Hacer. □

§8. El grupo de Brauer relativo de una extensión de cuerpos

¶ Como en la sección anterior, sea $E/\Bbbk$ una extensión de cuerpos. El cuerpo E es, de manera natural, un álgebra y entonces para cada álgebra A el E-espacio vectorial $A^E = E \otimes A$ es una $\Bbbk$-álgebra. La función lineal $e \in E \mapsto e \otimes 1_A \in A^E$ es un morfismo de $\Bbbk$-álgebras y es inmediato verificar que su imagen está contenida en el centro $\mathsf{Z}(A^E)$. Así, el anillo A^E es, de manera natural, una E-álgebra.

Proposición 8.1.

(*i*) *Si $f : A \to B$ es un morfismo de álgebras, entonces la función E-lineal $f^E : A^E \to B^E$ es un morfismo de E-álgebras.*

(*ii*) *Si $\mathsf{id}_A : A \to A$ es el morfismo identidad de un álgebra A, entonces $(\mathsf{id}_A)^E : A^E \to A^E$ es el morfismo identidad de la E-álgebra A^E.*

(*iii*) *Si $f : A \to B$ y $g : B \to C$ son morfismos de álgebras, entonces se tiene que $(g \circ f)_E = g_E \circ f_E : A_E \to C_E$.*

(*iv*) *Si $f : A \to B$ es un isomorfismo de álgebras, entonces $f^E : A^E \to B^E$ es un isomorfismo de E-álgebras.*

Demostración. De acuerdo a la Proposición 2.3, la función $f^E : A^E \to B^E$ es un morfismo de $\Bbbk$-álgebras; como es E-lineal, es, de hecho, un morfismo de E-álgebras. Esto prueba la afirmación (i). Por otro lado, las afirmaciones (ii), (iii) y (iv) son consecuencia inmediata de la primera, segunda y tercera parte de la Proposición 7.4, respectivamente. □

¶ Queremos determinar de qué manera el proceso de extensión de escalares interactúa con la construcción del grupo de Brauer. Un primer paso es el siguiente:

{prop:ext:alg-otimes}

Proposición 8.2. *Si A y B son dos álgebras, hay un isomorfismo de E-álgebras $\eta_{A,B} : A^E \otimes_E B^E \to (A \otimes B)^E$ tal que $\eta_{A,B}((1_E \otimes a) \otimes (1_E \otimes b)) = 1_E \otimes (a \otimes b)$ para cada $a \in A$ y cada $b \in B$.*

Demostración. De acuerdo a la Proposición 7.5 sabemos que hay un isomorfismo de E-espacios vectoriales $\eta_{A,B} : A^E \otimes B^E \to (A \otimes B)^E$ tal que para cada $a \in A$ y cada $b \in B$ es $\eta_{A,B}((1_E \otimes a) \otimes (1_E \otimes b)) = 1_E \otimes (a \otimes b)$. Basta, entonces, que mostremos que se esta función es un morfismo de E-álgebras. Como es E-lineal y el conjunto $\{(1_E \otimes a) \otimes (1_E \otimes b) : a \in A, b \in B\}$ genera a $A^{\otimes}_{E} B^E$ como E-espacio vectorial, es suficiente que mostremos que

$$\begin{aligned}\eta_{A,B}\big((1_E \otimes a) \otimes (1_E \otimes b) \cdot (1_E \otimes a') \otimes (1_E \otimes b')\big) \\ = \eta_{A,B}\big((1_E \otimes a) \otimes (1_E \otimes b)\big) \cdot \eta_{A,B}\big((1_E \otimes a') \otimes (1_E \otimes b')\big)\end{aligned}$$

para cada a, $a' \in A$ y cada b, $b' \in B$. Esto es inmediato. □

El siguiente resultado nos dice que la clase de álgebras que intervienen en la construcción del grupo de Brauer es preservada por la extensión de escalares.

{prop:ext:cs}

Proposición 8.3. *Si A es un álgebra central y simple, entonces A^E es una E-álgebra central y simple.*

Demostración. Supongamos que A es un álgebra central y simple. Como E es un álgebra simple, la Proposición 3.1 implica que $A^E = E \otimes A$ es un álgebra simple, y se sigue de esto trivialmente que es también una E-álgebra simple. Por otro lado, la Proposición 2.6 nos dice que hay un isomorfismo de álgebras $e \in E = \mathsf{Z}(E) \mapsto e \otimes 1_A \in \mathsf{Z}(E \otimes A) = \mathsf{Z}(A^E)$, y esto significa precisamente que A^E es una E-álgebra central □

Finalmente, la relación de similaridad se comporta de la manera correcta al extender escalares:

{prop:ext:sim}

Proposición 8.4.

(*i*) *Si A es un álgebra y $n \geq 1$, entonces hay un isomorfismo de E-álgebras*

$$(\mathsf{M}_n(A))^E \cong \mathsf{M}_n(A^E).$$

(*ii*) *Si dos álgebras A y B son similares, entonces las E-álgebras A^E y B^E son similares.*

Demostración. Hacer. □

{prop:kappa}

Proposición 8.5. *Hay una única función $\kappa_{E/\Bbbk} : \mathsf{Br}(\Bbbk) \to \mathsf{Br}(E)$ tal que para cada álgebra central simple A es*

$$\kappa_{E/\Bbbk}([A]) = [A^E].$$

Esta función es un homomorfismo de grupos.

Demostración. Que hay una función $\kappa_{E/\Bbbk} : \mathsf{Br}(\Bbbk) \to \mathsf{Br}(E)$ tal que $\kappa_{E/\Bbbk}([A]) = [A^E]$ para cada álgebra central y simple A es consecuencia inmedita de la Proposición 8.3 y de la segunda parte de la Proposición 8.4. Que se trata de un morfismo de grupos se deduce de la Proposición 8.2 y de la definición del producto en un grupo de Brauer. □

Proposición 8.6. *Sean $E/\Bbbk$ y F/E extensiones de cuerpos.*

(*i*) *Si A es un álgebra, entonces hay un isomorfismo de F-álgebras $(A_E)_F \cong A_F$.*

(*ii*) *Conmuta el diagrama*

$$\begin{tikzcd} \mathsf{Br}(\Bbbk) \arrow[r, "\kappa_{E/\Bbbk}"] \arrow[dr, "\kappa_{F/\Bbbk}"'] & \mathsf{Br}(E) \arrow[d, "\kappa_{F/E}"] \\ & \mathsf{Br}(F) \end{tikzcd}$$

Demostración. Hacer. □

¶ Si $E/\Bbbk$ es una extensión de cuerpos y $\kappa_{E/\Bbbk} : \mathsf{Br}(\Bbbk) \to \mathsf{Br}(E)$ es el homomorfismo construido en la Proposición 8.5, llamamos ***grupo de Brauer relativo de la extensión*** $E/\Bbbk$ y escribimos $\mathsf{Br}(E/\Bbbk)$, al núcleo de $\kappa_{E/\Bbbk}$. Si $\iota_{E/\Bbbk} : \mathsf{Br}(E/\Bbbk) \to \mathsf{Br}(\Bbbk)$ es la inclusión, tenemos una sucesión exacta

$$0 \longrightarrow \mathsf{Br}(E/\Bbbk) \xrightarrow{\iota_{E/\Bbbk}} \mathsf{Br}(\Bbbk) \xrightarrow{\kappa_{E/\Bbbk}} \mathsf{Br}(E)$$

Proposición 8.7. *Si $E/\Bbbk$ y F/E son extensiones de cuerpos, entonces $\mathsf{Br}(E/\Bbbk)$ es un subgrupo de $\mathsf{Br}(F/\Bbbk)$ y conmuta el diagrama*

$$\begin{tikzcd}
\mathsf{Br}(E/\Bbbk) \arrow[r, hook] \arrow[dr, "\iota_{E/\Bbbk}"'] & \mathsf{Br}(F/\Bbbk) \arrow[d, "\iota_{F/\Bbbk}"] \\
& \mathsf{Br}(\Bbbk)
\end{tikzcd}$$

Demostración. Hacer. □

§9. Descenso galoisiano

¶ Fijemos una extensión finita de cuerpos $E/\Bbbk$ y supongamos que es galoisiana y que $G = \mathsf{Gal}(E/\Bbbk)$ es su grupo de Galois.

¶ El cuerpo E es, en particular, un E-espacio vectorial, pero el grupo G actúa sobre E por automorfismos de $\Bbbk$-espacio vectorial pero *no* de espacio vectorial: en efecto, si e, $v \in E$ y $g \in G$, es $g \cdot (e \cdot v) = (g \cdot e) \cdot (g \cdot v)$, precisamente porque G actúa por automorfismos de anillo. Esto motiva la siguente definición.

Decimos que una acción de G sobre un E-espacio vectorial por automorfismos de $\Bbbk$-espacios vectoriales es ***E-semilineal*** si

$$g \cdot (e \cdot v) = (g \cdot e) \cdot (g \cdot v)$$

para cada $g \in G$, $e \in E$ y $v \in V$. Por ejemplo, la acción de G sobre E es E-semilineal.

{prop:cross}

Proposición 9.1. *Sea $\{u_g : g \in G\}$ un conjunto de símbolos tal que $u_g \neq u_h$ si g, $h \in G$ son distintos y consideremos el E-espacio vectorial $E \rtimes G$ que tiene a $(u_g)_{g\in G}$ como base.*

- (i) *Hay una única estructura de $\Bbbk$-álgebra sobre el E-espacio vectorial $E \rtimes G$ tal que $u_g \cdot e = g(e) \cdot u_g$ y $u_g \cdot u_h = u_{gh}$ para cada $e \in E$, g, $h \in G$. Su elemento identidad es u_{1_G}.*
- (ii) *Si V es un E-espacio vectorial sobre el que G actúa de manera E-semilineal, existe exactamente una estructura $\triangleright$ de $E \rtimes G$-módulo izquierdo sobre V tal que para cada $e \in E$, $g \in G$ y $v \in V$ es*

$$eu_g \triangleright v = e \cdot (g \cdot v).$$

- (iii) *Recíprocamente, si V es un $E \rtimes G$-módulo izquierdo con acción $\triangleright$, entonces hay una única estructura de E-espacio vectorial sobre V y una única acción E-semilineal de G sobre V tales que $e \cdot v = eu_{1_g} \triangleright v$ u $g \cdot v = u_g \triangleright v$ para cada $e \in E$, $g \in G$ y $v \in V$.*

Por ejemplo, como E es un E-espacio vectorial sobre el que G actúa de forma E-semilineal, E es de manera natural un $E \rtimes G$-módulo izquierdo, con acción tal que $eu_g \triangleright e' = eg(e')$ para cada e, $e' \in E$ y $g \in G$. Será dotado de esta acción que lo consideraremos siempre un $E \rtimes G$-módulo izquierdo.

Demostración. Hacer □

{prop:90:1}

Proposición 9.2. *La $\Bbbk$-álgebra $E \rtimes G$ es central y simple. Todo $E \rtimes G$-módulo izquierdo simple es isomorfo a E.*

Demostración. Sea $z = \sum_{g\in G} e_g u_g$ un elemento del centro de $E \rtimes G$, con $e_g \in E$ para cada $g \in G$. Si $h \in G$ es distinto de 1_G, existe $e \in E$ tal que $h(e) \neq 0$. Como z es central, $0 = ez - ze = \sum_{g\in G}(ee_g - e_g g(e))u_g$ y, como $(u_g)_{g\in G}$ es una base de $E \rtimes G$ como E-espacio vectorial, vemos que en particular el coeficiente de u_h, que es $(e - h(e))e_h$, se anula: esto sólo es posible si, de hecho, $e_h = 0$.

Concluimos de esta manera que $z = eu_{1_G}$ para algún $e \in E$. Si $g \in G$, entonces como z es centrales $0 = zg - gz = (e - g(e))u_g$ y debe ser $g(e) = e$. La arbitrariedad de g implica que $e \in E^G = \Bbbk$: así, $z \in \Bbbk 1_{E \rtimes G}$ y, en consecuencia, el álgebra $E \rtimes G$ es central.

Sea ahora $I \subseteq E \rtimes G$ un ideal bilátero no nulo, de manera que existen $n \geq 1$, $e_1, \ldots, e_n \in E$ no nulos y $g_1, \ldots, g_n \in G$ distintos tales que $x = \sum_{i \in [\![n]\!]} e_i u_{g_i} \in I$; sin pérdida de generalidad podemos suponer que n es el mínimo número para el que existe un tal elemento en I. Reemplazando a x por $e_1^{-1} x u_{g_1^{-1}}$, podemos suponer además que $e_1 = 1_E$ y que $g_1 = 1_G$. Sea $j \in \{2, \ldots, n\}$. Como $g_j \neq 1_G$, existe $e \in E$ tal que $g_j(e) \neq e$; el elemento $ex - xe = \sum_{i=2}^{n} (e - g_i(e)) e_i u_{g_i}$ está en I y en vista de la forma en que fue elegido n, el coeficiente de u_{g_j} en esta expresión tiene que ser nulo: se sigue que $e_j = 0$. Concluimos de esta forma que $x = 1_{E \rtimes G}$ y, entonces, que $I = E \rtimes G$. El álgebra $E \rtimes G$ es por lo tanto simple.

Del Lema 6.3 sabemos que todos los $E \rtimes G$-módulos izquierdos simples son isomorfos, así que para probar la segunda afirmación de la proposición bastará que mostremos que E es un $E \rtimes G$-módulo izquierdo simple. Esto es inmediato: todo submódulo es, en particular, un E-subespacio, y E no posee E-subespacios propios no nulos. □

Una consecuencia inmediata de la segunda afirmación de la Proposición 9.1 es el siguiente resultado, conocido como el Teorema 90 de Hilbert.

{coro:90:2}

Corolario 9.3. *Si $\phi : G \to E^\times$ es una función tal que $\phi(gh) = g(\phi(h))\phi(g)$ para cada g, $h \in G$, entonces existe $y \in E^\times$ tal que $\phi(g) = y/g(y)$ para todo $g \in G$.*

Demostración. Consideremos el E-espacio vectorial $V = E$ dotado de la acción de G tal que $g \cdot v = \phi(g)g(v)$ para cada $g \in G$ y $v \in V$. Es inmediato verificar que se trata de una acción E-semilineal, así que V es, como en la Proposición 9.1, un $E \rtimes G$-módulo izquierdo de manera natural. Como $\mathsf{dim}_E V = 1$, se trata de un $E \rtimes G$-módulo simple, y la Proposición 9.2 nos dice que existe un isomorfismo de $E \rtimes G$-módulos $f : E \to V$. Sea $y = f(1_E)$, que es un elemento no nulo de E. Como f es $E \rtimes G$-lineal, si $g \in G$ es

$$y = f(1_E) = f(u_g \cdot 1_E) = u_g \cdot f(1_E) = u_g \cdot y = \phi(g) \cdot g(y),$$

así que $\phi(g) = y/g(y)$. Esto prueba el corolario. □

Si V es un E-espacio vectorial sobre el que G actúa por funciones $\Bbbk$-lineales, el subconjunto V^G es un $\Bbbk$-subespacio de V, así que si $r : V^G \to V$ es la función inclusión, que es $\Bbbk$-lineal, la Proposición 7.3 nos da una función E-lineal $\bar{r} : (V^G)^E \to V$ tal que $\bar{r}(1_E \otimes v) = v$ para todo $v \in V^G$. Poco podemos decir de esta función salvo en un caso especial:

Proposición 9.4. *Si V es un E-espacio vectorial sobre el que G actúa E-semilinealmente, entonces la función $\bar{r} : (V^G)^E \to V$ es un isomorfismo de E-espacios vectoriales.*

Demostración. Supongamos que la función $\bar{r}$ no es inyectiva. Esto implica que existen $n \geq 1$, elementos $v_1, \ldots, v_n \in V^G$ linealmente independientes sobre $\Bbbk$ y escalares $e_1, \ldots, e_n \in E$ tales que $\sum_{i \in [\![n]\!]} e_i v_i = 0$ en V; podemos suponer, además, que n es el menor número con esta propiedad y, en consecuencia, que $e_i \neq 0$ para todo $i \in [\![n]\!]$.

Sea $g \in G$ distinto de 1_G. Como la acción de G sobre V es E-semilineal, tenemos que $\sum_{i \in [\![n]\!]} g(e_i) v_i = 0$, y entonces

$$\sum_{i \in [\![n]\!]} \left(e_i - \frac{g(e_i) e_1}{g(e_1)} \right) v_i = 0.$$

Como el término de esta suma correspondiente a $i = 1$ es nulo, la elección de n implica que, de hecho, $e_i = g(e_i) e_1 / g(e_1) = 0$ para todo $i \in [\![n]\!]$, de manera que el cociente $g(e_i)/e_i \in E^\times$ depende solamente de g y no de i. Consideremos la función $\phi : g \in G \mapsto g(e_1)/e_1 \in E^\times$. Si $g, h \in G$, entonces

$$\phi(gh) = \frac{gh(e_1)}{e_1} = g\left(\frac{h(e_1)}{e_1} \right) \frac{g(e_1)}{e_1} = g(\phi(h))\phi(g).$$

Vemos así que la función ϕ satisface la condición del Corolario 9.3, éste nos dice que existe $y \in E^\times$ tal que $\phi(g) = y/g(y)$ para todo $g \in G$. Si $i \in [\![n]\!]$, esto implica que $g(ye_i) = ye_i$ para cada $g \in G$, así que $ye_i \in \Bbbk$. Como

$$\sum_{i \in [\![n]\!]} y e_i v_i = 0$$

y los coeficientes de esta combinación lineal están en $\Bbbk$, la hipótesis de que los vectores $v_1, \ldots, v_n$ son linealmente independientes sobre $\Bbbk$ nos permite concluir que $e_i = 0$ para todo $i \in [\![n]\!]$. Como esto es absurdo, vemos de esta forma que la función $\bar{r}$ es inyectiva. $\square$