21
2ej.

# UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

**FACULTAD DE CIENCIAS**

## ALGEBRAS SIMPLES
## Y EL GRUPO DE BRAUER

Tesis

*que para obtener el título de*

matemático

*presenta*



Rosa María Meneses Hernández



Marzo de 1994


**UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso**

A mis padres,
mi esposo y
al Dr. Félix Recillas J.

# INDICE

## Introducción

En la teoría de campos se demuestra que, existe un isomorfismo entre el grupo de Brauer $\mathbf{B}$ de extensiones finitas $F$, de Galois, de un campo $k$ y el segundo grupo de cohomología de $\Gamma$ con coeficientes en $F^x$:

$$\mathbf{B}(F/k) \cong H^2(\Gamma, F^x)$$

El objeto de la tesis es desarrollar los resultados de álgebras simples sobre $k$, necesarias para establecer el teorema anterior, sin utilizar la cohomología de grupos.

Para ello se divide esencialmente en tres partes:

- Estructura de las álgebras simples,
- Las representaciones de un álgebra simple,
- Conjuntos factoriales y el grupo de Brauer.

# 1 Estructura de las álgebras simples.

**Definición:** Sea $A$ un anillo conmutativo. Por una *álgebra* sobre el anillo $A$ se entendera un conjunto $E$ dotado

(i) de una estructura de $A$-módulo sobre $E$.

(ii) de una operación bilineal

$$\psi: E \times E \to E$$

tal que $(x, y) \longmapsto \psi(x, y) = x \cdot y$ es decir

$$\begin{aligned} \psi(x_1 + x_2, y) &= \psi(x_1, y) + \psi(x_2, y) \\ \psi(x, y_1 + y_2) &= \psi(x, y_1) + \psi(x, y_2) \end{aligned}$$

lo cual se escribe como

$$\begin{aligned} (x_1 + x_2)y &= x_1 y + x_2 y \quad x_1, x_2 \in E,\ y \in E \\ x(y_1 + y_2) &= xy_1 + xy_2 \quad x \in E,\ y_1, y_2 \in E. \end{aligned}$$

(iii) $a\psi(x, y) = \psi(ax, y) = \psi(x, ay) \quad x, y \in E, a \in A$ lo cual se escribe como

$$a(x \cdot y) = (ax)y = x(ay)$$

y se dirá que $E$ *es una* $A$*-álgebra.*

Se dira que $E$ es una *A-álgebra asociativa* si satisface la condición

$$\psi(\psi(x,y),z) = \psi(x,\psi(y,z))$$

lo cual se escribe como

$$(xy)z = x(yz)$$

Se dira que $E$ es un *A-álgebra unitaria* si tiene un elemento

$$1_A \cdot x = x \cdot 1_A = x \quad \forall x \in E$$

Consideremos el caso particular en que $A = k$ campo y $B = K$ campo y supongamos $k \subset K$. Sea $K$ un campo $E$ una $K$-álgebra y $L$ un campo conteniendo al campo $K$

$$K \subset L$$

Ahora fabricamos

$$E \otimes_K L.$$

En otras palabras, dada una $K$-álgebra $E$, extender los coeficientes a una $L$-álgebra significa considerar el álgebra

$$E \otimes_K L.$$

Sea $K$ un campo conmutativo y $A$ una $K$-álgebra o una álgebra sobre $K$ con elemento unitario $1_A \in A$.

Todos los $A$-módulos $M$ que se consideren serán unitarios en el siguiente sentido:

$$1_A \cdot m = m \qquad \forall m \in M.$$

Supongamos que $M' \subset M$, por el *Aniquilador* de $M'$ en $A$ se entenderá el conjunto

$$\mathcal{A}(M') = \{a \in A \,|\, a \cdot m = 0 \quad \forall m \in M'\}.$$

En particular

$$\mathcal{A}(M) = \{a \in A \,|\, a \cdot m = 0 \quad \forall m \in M\}$$

se dirá que $\mathcal{A}$ es aniquilador de $M$.

*Afirmación:* Si $M$ es un $A$-módulo izquierdo entonces $\mathcal{A}(M')$ es una ideal izquierdo de $A$.

En efecto, sean $x, y \in \mathcal{A}(M')$ y sea $x + y \in A$ calculando: $(x+y)m = xm + ym = 0 \quad \forall m \in M' \implies x = y \in \mathcal{A}(M')$.

Sean $a \in A$, $x \in \mathcal{A}(M')$, calculando para toda $m \in M'$ $(a \cdot x)m = a \cdot (xm) = a \cdot 0 = 0 \implies ax \in \mathcal{A}(M')$.

*Afirmación:* $\mathcal{A}(M')$ es un ideal en $A$ bilateral.

En efecto, por lo que precede $\mathcal{A}(M')$ es un ideal izquierdo.

Sean $a \in A$ y $x \in \mathcal{A}(M')$, calculando para toda $m \in M$

$$(xa)m = x(am) = 0$$

$xa$ está definido por ser un elemento de $A$ y $am$ es elemento de $M'$, por eso $x(am) = 0$ lo anterior implica $xa \in \mathcal{A}(M')$.

**Definición:** Sea $A$ una $K$-álgebra y sea $M$ un $A$-módulo. Se dirá que $M$ es simple si no contiene submódulos salvo $\{0\}$ y $M$.

*Afirmación:* Dada una $K$-álgebra. Siempre existen $A$-módulos simples, a saber el ideal $\mathcal{A} \in A$ de mínima dimensión sobre $K$, lo cual tiene sentido puesto que

$$\begin{aligned} K &\hookrightarrow A \\ k &\to k \cdot 1_A \end{aligned}$$

esta aplicación es un isomorfismo.

$$\therefore \quad K \subset A$$

Sea $K$ un campo conmutativo y $A$ una $K$-álgebra unitaria de $\dim_K A = n < +\infty$, si $M$ es $A$-módulo izquierdo y $\mathcal{A} = \{a \in A \,|\, am = 0 \quad \forall m \in M\}$, $\mathcal{A} \subset A$ es el aniquilador de $N$.

**Definición:** Se dice que $M$ es fiel si $\mathcal{A} = 0$.

**Proposición 1:** *Sea $A$ una $K$-álgebra con una $A$-módulo izquierdo fiel y simple $M$. Entonces todo $A$-módulo izquierdo $M'$ es una suma directa de módulos todos isomorfos a $M$*

$$M' = \bigoplus_{i=1}^{n} M_i \quad \textit{tales que} \quad M_i \cong M \quad (1 \leq i \leq n)$$

*Demostración:* En primer lugar se demostrará la proposición para el caso $M' = A$ ($M$ considerado como un $A$-módulo izquierdo).

Recordando que $\mathcal{A} = \{a \in \mathcal{A} \,|\, am = 0 \quad \forall m \in M\}$ es un ideal izquierdo, se afirma que en $M$ existen subconjuntos finitos de aniquilador $A = \{0\}$.

Por ejemplo, una base

$$\{m_1, \ldots, m_r\}$$

de $M = A$ sobre $K$. Puesto que $m = \sum_{i=1}^{r} \alpha_i m_i \qquad \alpha_i \in K$.

Sea $a \in \mathcal{A}$ cualquiera, por lo tanto

$$a \cdot m = 0 \implies \sum_{i=1}^{r} (a\alpha_i) m_i = 0$$

pero esto significa que

$$a\alpha_i = 0 \qquad (1 \leq i \leq r)$$

y si $m \neq 0 \quad \alpha_{i_0} \neq 0$ para algún $1 \leq i_0 \leq r$ además como $\alpha_{i_0} \in K$, existe el inverso

$$0 = a\alpha_{i_0}\alpha_{i_0}^{-1} = a \implies \mathcal{A} = \{0\}$$

Consideremos el mínimo conjunto finito de un aniquilador cero, a saber

$$\{m_1, \ldots, m_n\} \subset M \quad \text{tal que} \quad \mathcal{A}(m_1, \ldots, m_n) = \mathcal{A} = \{0\}.$$

Sean $A_i$ el aniquilador del conjunto $\{m_{i+1}, \ldots, m_n\}$

$$A_i = A_i(m_{i+1}, \ldots, m_n) \qquad 0 \leq i \leq n.$$

Por definición

$$A_0 = A_0(m_1, \ldots, m_n) = \{0\}$$

y es inmediato que

$$A_0 \subset A_1 \subset A_2 \subset \cdots \subset A_{i-1} \subset A_i \subset \cdots \subset A_n = A$$

*Afirmación:* $A_{i-1} \subset A_i$, propiamente.

Supongamos por un instante que

$$A_{i-1} = A_i$$

si $x \in A_i \implies x \cdot m_{i+1} = 0, \ldots, x \cdot m_n = 0$ y como también

$$x \in A_{i-1} \implies x \cdot m_i = 0, \ldots, x \cdot m_n = 0$$

se afirma que el aniquilador

$$\mathcal{A}(m_1, \ldots, m_{i-1}, m_{i+1}, \ldots, m_n) = \{0\}$$

en efecto, sea $y \in \mathcal{A}(m_1, \ldots, m_{i-1}, m_{i+1}, \ldots, m_n)$ la definición implica que en particular

$$ym_{i+1} = 0, ym_{i+2} = 0, \ldots, ym_n = 0$$

Esto implica que $y \in A_i$ y como por hipótesis $y \in A_{i-1}$, es decir $y \in \mathcal{A}(m_1, \ldots, m_n)$ y como $y$ se eligió arbitrariamente en

$$\mathcal{A}(m_1, \ldots, m_{i-1}, m_{i+1}, \ldots, m_n),$$

se obtiene

$$\mathcal{A}(m_1, \ldots, m_{i-1}, m_{i+1}, \ldots, m_n) = \{0\}$$

el cual es un conjunto más pequeño que $\mathcal{A}(m_1, \ldots, m_n)$ y esto contradice la elección de que $\{m_1, \ldots, m_n\}$ es el mínimo conjunto de aniquilador $\{0\}$.

Por consiguiente

$$A_{i-1} \neq A_i \quad \text{y} \quad A_{i-1} \subset A_i \quad i = 1, \ldots, n$$

Ahora consideremos los grupos aditivos

$$M_i = A_i m_i \qquad m_i \in \{m_1, \ldots, m_n\} \subset M$$

$A_i$ es el aniquilador de $\{m_{i+1}, \ldots, m_n\}$ el cual sabemos que es ideal izquierdo en $A$.

$M_i$ es $A$-submódulo de $M$:

$$a_i^{(1)} m_i + a_i^{(2)} m_i = (a_i^{(1)} + a_i^{(2)}) m_i = a_i m_i$$

$M_i$ es un submódulo de $M$ vía la aplicación

$$\varphi_i \colon A_i \times M_i \to M_i$$

definida por la correspondencia

$$(a, m) \longmapsto \varphi_i(a, m) = am$$

$\varphi$ está bien definida puesto que

$$am = a(a_i m_i) = (aa_i) m_i.$$

Como $A_i$ es un ideal, $aa_i \in A_i$

$$\therefore \quad am = a' m_i \quad \text{con} \quad a' \in A_i$$

es decir $\varphi_i(a, m) = am \in M_i$.

Es fácil ver que con $\varphi$, $M_i$ deviene un $A$-módulo izquierdo con $(1 \leq i \leq n)$:

$$\psi_i \colon A_i \to M_i$$

definida por la correspondencia

$$x \longmapsto \psi_i(x) = x m_i$$

es evidente que $\psi_i$ es un $A$-homomorfismo sobre

$$\begin{aligned} \psi_i(x) &= x m_i \in A m_i \\ \psi_i(x + y) &= \psi_i(x) + \psi_i(y) \end{aligned}$$

sea $a \in A$ y sea $x \in A_i \implies ax \in A_i$, entonces

$$\psi_i(ax) = (ax) m_i = a(x m_i) = a \psi_i(x) \quad \forall a \in A, \quad \forall x \in A_i.$$

Además

$$\ker \psi_i = A_{i-1} \quad (1 \leq i \leq n)$$

$A_{i-1} \subset \ker \psi_i$ ya que si $a \in A_{i-1}$, en particular $am_i = 0 \implies a \in \ker \psi$.

Reciprocamente, $\ker \psi_i = A_{i-1}$ porque si $a \in \ker \psi_i \Rightarrow \psi_i(a) = 0 \Rightarrow am_i = 0$ y como $\ker \psi_i \subset A-i$, en particular $a \in A_{i-1}$ con lo cual $\ker \psi \subset A_{i-1}$.

Por lo tanto

$$\ker \psi_i = A_{i-1}$$

pasando al cociente se tiene el isomorfismo $\tilde{\psi}$

$$A_i \Big/ A_{i_1} \overset{\tilde{\psi}_i}{\cong} M_i.$$

Es decir, considerando la aplicación

$$\tilde{\psi}: A_i/A_{i-1} \to M_i$$

definida por la correspondencia

$$\{x\} \longmapsto \tilde{\psi}(\{x\}) = \psi(x)$$

calculando para todo $a$ del anillo $A$:

$$\{ax\} = (ax)A_i = a(xA_{i-1}) = a\{x\}$$

se obtiene

$$\{ax\} = a\{x\}$$

por consiguiente

$$a\tilde{\psi}(\{x\}) = \psi(a\{x\}).$$

Como $A_{i-1} \subset A_i$ es una inclusión propia

$$A_i/A_{i-1} \neq \{0\} \implies M_i \neq \{0\}$$

y como $M_i = A_i m_i \subset M$ y además por hipótesis $M$ es simple, a fortiori $M_i = M \quad (1 \leq i \leq n)$.

Consideremos la aplicación

$$\Phi_i: A_i \to A_i m_1 \times \cdots \times A_i m_i$$

definida por la correspondencia

$$x \longmapsto \Psi_i(x) = (xm_1, \ldots, xm_i)$$

*Afirmación:* $\Phi_i\colon A_i \cong M_i \times \cdots \times M_i$ donde $M_j = M \quad (1 \leq i \leq i)$ para toda $i = 1, \ldots, n$ es evidente que

1) $\Phi_i$ es un $A$-homomorfismo sobre

$$\begin{aligned} \Phi_i(x+y) &= ((x+y)m_1, (x+y)m_2, \cdots, (x+y)m_i) \\ &= (xm_1 + ym_1, \cdots, xm_i + ym_i) \\ &= (xm_1, \cdots, xm_i) + (ym_1, \cdots, ym_i) \\ &= \Phi_i(x) + \Phi_i(y) \\ \Phi_i(a(x)) &= a\Phi_i(x) \end{aligned}$$

*Afirmación:* 2) $\Phi_i$ es inyectiva.

En efecto, sea $x \in A_i$ y supongamos que

$$\Phi_i(x) = 0$$

es decir, $(xm_1, xm_2, \ldots, xm_i) = 0 \iff xm_1 = 0, xm_2 = 0, \ldots, xm_i = 0.$

Por otro lado $x \in A_i \implies xm_{i+1} = 0, xm_{i+2} = 0, \ldots, xm_n = 0$ es decir

$$xm_1 = 0, \ldots, xm_i = 0, xm_{i+1} = 0, \ldots, xm_n = 0 \implies x \in \mathcal{A}(m_1, \ldots, m_n)$$

por consiguiente $x = 0$ y la firmación está demostrada.

(1) y (2) implican que $\Phi_i$ es biyectiva para $i = 1, \ldots, n$.

Continuando, sea $i = 1$,

$$\Phi_1\colon A_1 \to A_1 m_1$$

definida por la correspondencia

$$x \longmapsto xm_1$$

y como

$$A_i/A_{i-1} \cong M_i \quad \text{se tiene}$$

$$A_1/A_0 = A_1 \cong M_1 \cong M \quad \text{para} \quad i = 1$$

y como por definición

$$M_1 = A_1 m_1$$

se obtiene

$$\Phi_1 : A_1 \cong M_1 = M$$

$$\Phi_1 : A_1 \cong M$$

para $i = 2$

$$\Phi_2 : A_2 \to A_2 m_1 \times A_2 m_2$$

por definición $A_2 m_2 = M_2 \cong M$ y como $A_1 \subset A_2 \Rightarrow A_1 m_1 \subset A_2 m_1$ además por definición $A_1 m_1 = M_1 = M \subset A_2 m_1 \subset M, A_2 m_1 = M$

$$\Phi : A_2 \cong M \times M$$

Supongamos que

$$\Phi_i : A_i \cong M \times \cdots \times M \quad i - \text{factores donde } \Phi_i \text{ es como se dijo en (I)}$$

Ahora consideremos

$$\Phi_{i+1} : A_{i+1} \to A_{i+1} m_1 \times \cdots \times A_{i+1} m_i \times A_{i+1} m_{i+1}$$

definida por la correspondencia

$$x \longmapsto \Phi_{i+1}(x) = xm_1, \ldots, xm_i, xm_{i+1}.$$

Como $\Phi_i \cong A_i m_1 \times \cdots \times A_i m_i$

$$\Phi_i \cong M \times \cdots \times M \quad i - \text{factores}$$

Por definición

$$A_{i+1} m_{i+1} = M_{i+1} + M$$

esto implica que

$$\Phi_{i+1} = A_{i+1} \cong A_{i+1} m_1 \times A_{i+1} m_1 \times \cdots \times A_{i+1} m_i$$

$$A_i \subset A_{i+1} \implies A_i m_k \subset A_{i+1} m_k \qquad 1 \leq k \leq i$$

Por hipótesis de inducción

$$A_j m_k = M \qquad (1 \leq j, k \leq i)$$

$$M \subset A_i m_k \subset A_{i+1} m_k \subset M \implies A_{i+1} m_k = M \quad (1 \leq k \leq i)$$

$$\therefore \quad \Phi_{i+1} \colon A_{i+1} \cong M \times \cdots \times M \quad i+1 - \text{factores}$$

por consiguiente $\Phi_n \colon A_n = A \cong M \times \cdots \times M \quad n - \text{factores}$.

Esto prueba la proposición para el caso $M' = A$, ahora demostraremos para cualquier $A'$-módulo izquierdo $M'$ de $\dim_K M' = h < +\infty$.

Sea $\{m'_1, \ldots, m'_h\}$ un sistema de generadores que puede tomarse como la base de $M'$ sobre $K$ y consideremos la aplicación $\psi'$ de

$$A^h = A \times \cdots \times A \qquad (h - \text{factores}) \text{ en } M'.$$

$$\psi' \colon A^h \to M'$$

definida por la correspondencia

$$x = (x_1, \ldots, x_h) \to \psi'(x) = x_1 m'_1 + \cdots + x_h m'_h$$

En realidad se tiene un $A$-morfismo suprayectivo de $M^{nh} = M \times \cdots \times M$ $nh$ factores sobre $M'$

$$F \colon M^{nh} \to M'$$

Sea $N$ su nucleo: $\ker F = N$

Consideremos el máximo subconjunto

$$\{M_{i_1}, \ldots, M_{i_k}\} \subset \{M_1, \ldots, M_{nh}\} \text{ donde } M_i = M \; i = 1, \ldots, nh$$

tal que $N + \sum_{\ell=1}^{k} M_i$ es suma directa que se puede escribir como $N' = N + \sum_{i=1}^{k} M_i$ (reenumerando sólo aquellos $M_{i\ell}$ que son suma directa) entonces para $j > k$ (es decir, para los que no son suma directa) $M_j \cap N' \neq \emptyset$. Como $M_j \cap N'$ es un submódulo de $M_j$, que es isomórfo a $M$: $M = M_j$, además $M$ es simple por hipótesis, entonces

$$M_j \cap N' = M \implies M_j \subset N' \qquad \forall j > k$$

Pero $F$ es sobre entonces

$$N' = N \bigoplus \sum_{i=1}^{k} M_i \to M'$$

con $\ker F = N$, pasando al cociente

$$N'/N \cong M'$$

Por el teorema de E. Noether

$$\begin{aligned} N'/N = N \bigoplus \sum_{i=1}^{k} M_i/N &\cong \sum_{i=1}^{k} M_i/N \cap (\sum M_i) \\ &\cong \sum_{i=1}^{k} M_i \end{aligned}$$

entonces $M' \cong \sum_{i=1}^{k} M_i = M \times \cdots \times M \quad k$-factores.

**Proposición 2.** *Sea $K$ un campo conmutativo, $A$ una $K$-álgebra, $M$ un $A$-módulo izquierdo fiel y simple, $D$ el anillo de endomorfismos de $M$ en sí mismo.*

$$D = End(M)$$

*Entonces $D$ es un álgebra sobre $K$ de división y $A$ es isomorfo con $\mathcal{M}_n(D)$.*
$A \cong \mathcal{M}_n(D)$, *donde* $\mathcal{M}_n(D) = \{c = (d_{ij}) \,|\, d_{ij} \in D \quad \forall 1 \leq i, j \leq n\}$

*Demostración:* De acuerdo con la proposición 1, el álgebra $A$ concebida como $A$-módulo izquierdo es isomorfa con $M^n = M \times \cdots \times M$, $n$ factores: $A \cong M^n$ para alguna $n \geq 1$.

Se conviene en escribir la operación de todo elemento $d \in D$ sobre $M$ como sigue: si $d \in D$ es decir,

$$d: M \to M$$

es un homomorfismo lineal definido por la correspondencia

$$m \longmapsto d(m) = m \cdot d$$

es decir, la operación

$$\psi: M \times D \to M$$

definida por la correspondencia

$$(m, d) \longmapsto \psi(m, d) = m \cdot d$$

como $D$ es subconjunto del anillo de endomorfismos de $M$ sobre $K$. Si definimos la operación

$$\Phi: K \times D \to D$$

definida por la correspondencia

$$(\alpha, d) \longmapsto \Phi(\alpha, d) = \alpha \cdot d, \quad \text{donde}$$

$$\begin{aligned} \alpha d: M &\to M \\ m &\longmapsto \alpha d(m) = \alpha(md) \end{aligned}$$

con esta operación $D$ deviene un espacio vectorial sobre $K$. Se dira que $\dim_k D < +\infty$. En efecto como $M$ es de $\dim_k < +\infty$ el espacio vectorial subyacente al anillo $\mathcal{D}$ de endomorfismos de $M$ sobre $K$ es de dimensión finita y como $D \subset \mathcal{D}$ se obtiene que $\dim_k D < +\infty$.

Si $d \in \mathcal{D}$, es decir, $d: M \to M$ por tanto $\mathrm{Im}(d) = d(M) \subset M$. Si $d \neq 0$ entonces $\mathrm{Im}(d) \neq \{0\} \subset M$, es decir, $M \cong M \Rightarrow \exists\, d^{-1} \in D$. Esto demuestra que $D$ es un álgebra sobre su centro. En efecto sea $Z$ el centro del anillo $D$, el cual es un campo. Ahora consideremos $d_1, d_2 \in D$, $z \in Z$;

$d_1(d_2 z) = (d_1 d_2)z = d_1(z d_2)$, es decir, $D$ es una álgebra con división sobre su centro $Z$.

En el curso de la demostración de la proposición 1, se demostró $A \cong M^n$ para alguna $n$:

Esto implica que el anillo de automorfismos de $A$,

$$\mathrm{Aut}\,(A)$$

es isomorfo con el anillo de automorfismos de $M^n$: $M^n = \mathrm{Aut}\,(M^n) = D$, es decir, $\mathrm{Aut}\,(A) \cong D$.

Para calcularlos consideremos un automorfimo $\lambda$: Aut $(M^n)$ es decir, es un isomorfismo de $M^n$ en $M^n$

$$\lambda: M^n \to M^n, \quad M^n = M \times \cdots \times M, \ n - \text{factores}$$

definido por la correspondencia

$$\begin{aligned}(m_1, \ldots, m_n) &\longmapsto \lambda(m_1, \ldots, m_n) \\ &= (\lambda_1(m_1, \ldots, m_n), \ldots, \lambda_n(m_1, \ldots, m_n))\end{aligned}$$

consideremos uno de éstos, como $\lambda$ es lineal se debe tener

$$\lambda_i(m_1, \ldots, m_n) = m_1 d_{1,i} + \cdots + m_n d_{n,i},$$

como se debe tener

$$\begin{aligned}\lambda_i((m_1, \ldots, m_n) &+ (m_1', \ldots, m_n')) = \lambda_i(m_1 + m_1', \ldots, m_n + m_n') \\ &= (m_1 + m_1')d_{1,i} + \cdots + (m_n + m_n')d_{n,i} \\ &= m_1 d_{1,i} + m_1' d_{1,i} + \cdots + m_n d_{n,i} + m_n' d_{n,i} \\ &= \lambda_i(m_1, \ldots, m_n) + \lambda_i(m_1', \ldots, m_n').\end{aligned}$$

Esto implica que se debe tener $d_{ij} \in D$ para toda $1 \leq i, j \leq n$, es decir,

$$\lambda(m_1, \ldots, m_n) = (\sum_{j=1}^{n} m_1 d_{1,j}, \ldots, \sum_{j=1}^{n} m_n d_{n,j}),$$

o sea que, la podemos identificar con la matriz $\lambda = (d_{ij}), \quad (1 \leq i, j \leq n)$.

$$\begin{aligned}\lambda_i(m_1, \ldots, m_n) &= m_1 d_{1,i} + \cdots + m_n d_{n,i} \Rightarrow \\ &\Rightarrow \lambda_i(m_1, \ldots, m_n) \\ &= \sum_{j=1}^{n} m_j d_{ji} \qquad (1 \leq i \leq n)\end{aligned}$$

Por consiguiente $\lambda(m_1, \ldots, m_n) = \sum_{j=1}^{n} m_j d_{j,1}, \ldots, \sum_{j=1}^{n} m_j d_{j,n}$.

De tal suerte podemos identificar

$$\lambda = (d_{ij}) \qquad (1 \leq i, j \leq n)$$

Todo esto demuestra $\mathrm{Aut}\,(M^n) = \mathcal{M}_n(D)$.

Sea $f \in \mathrm{Aut}\,(A)$, es decir, $f$ es un $A$-isomorfismo de $A$ en $A$

$$f: A \to A$$

definido por la correspondencia

$$x \longmapsto f(x), \quad \text{tal que} \quad f(ax) = af(x)$$

con $a \in A$, $x \in A$ y como $1_A \in A$; $f(x) = f(x \cdot 1_A) = xf(1_A) \quad \forall x \in A$, es decir, $f$ está únivocamente determinado por

$$a = f(1_A)$$

Esto implica que

$$\mathrm{Aut}\,(A) = A.$$

Lo cual permite escribir

$$A = \mathrm{Aut}\,(A) \cong \mathrm{Aut}\,(M^n) = \mathcal{M}_n(D)$$
$$A \cong \mathcal{M}_n(D)$$

$$Z(\mathcal{M}_n(D)) = \left\{ \begin{pmatrix} d & & 0 \\ & \ddots & \\ 0 & & d \end{pmatrix} \mid d \in Z(D) \right\}$$
$$Z = (\mathcal{M}_n(D)) \cong Z(D)$$

y como el centro de $A = Z(A) = K$ por consiguiente $K \cong Z(D)$.

**Teorema 1.** *Sea $A$ una $K$-álgebra*

$$A \quad \textit{es simple} \quad \Longleftrightarrow \quad A \cong \mathcal{M}_n(D)$$

*donde $D$ es un álgebra de división sobre $K$, cuando $A$ está dado y $n$ unívocamente determinada así como $D$ salvo por isomorfismo.*

*Demostración:* Sea $M$ un $A$-módulo simple. Se afirma que $M$ es fiel.

En efecto, como $A$ es simple por hipótesis, no puede tener un ideal bilateral más que $\{0\}$ o ella misma y sabemos que $\mathcal{A}(M) = \{a \in A \,|\, am = 0 \quad \forall m \in M\}$ es un ideal bilateral de $A \quad \mathcal{A}(M) \subset A$. Por lo tanto $\mathcal{A}(M) = \{0\}$, o sea $M$ es fiel.

Recordando la proposición 2.

Dada $A$ y $M$ fiel y simple $\Longrightarrow$ $A \cong \mathcal{M}_n(D)$.

Así obtenemos la necesidad.

*Suficiencia:* Aquí la hipótesis es $A \cong \mathcal{M}_n(D)$.

Consideremos las matrices

$$e_{ij} = (x_{kl}) \in \mathcal{M}_n(D) = A \quad \forall i,j \quad (1 \leq i,j \leq n)$$

satisfaciendo las siguientes condiciones

$$\begin{aligned} x_{ij} &= 1 \\ x_{kl} &= 0 \quad \text{si} \quad (k,\ell) \neq (i,j) \end{aligned}$$

**Lema 1.** *Sea* $a = (a_{ij}) \in \mathcal{M}_n(D)$ *arbitraria, entonces*

$$e_{ij} a e_{hk} = a_{jh} e_{ik}$$

*para toda* $i,j,h,k \quad (1 \leq i,j,h,k \leq n)$.

*Demostración:* Calculemos

$$\begin{aligned} e_{ij} a e_{hk} &= (x_{rs})(a_{tu})(x_{vw}) \\ &= (x_{rs})(\sum_{u=1}^{n} a_{tu} x_{uw}) \\ &= (\sum_{s=1}^{n} \sum_{u=1}^{n} x_{rs} a_{su} x_{uw}) \end{aligned}$$

pero por definición $x_{uw} = 0$ para $(u,w) \neq (h,k)$, así solamente queda

$$e_{ij} a e_{hk} = \left( \sum_{s=1}^{n} x_{rs} a_{sh} x_{hk} \right)$$

también $x_{rs} = 0$ para $(r,s) \neq (i,j)$ quedando:

$$e_{ij}ae_{hk} = (x_{ij}a_{jh}x_{hk})$$

la cual es una matriz en cuyo $i$-ésimo renglón y $k$-ésima columna contiene el elemento $a_{jh}$ de la matriz $a$, por ello se puede escribir como

$$e_{ij}ae_{hk} = a_{jh}e_{ik}$$

**Lema 2.** *Sea $a = (a_{ij}) \in \mathcal{M}_n(D)$ $a \neq 0$ arbitraria y $N$ el ideal bilateral generado por $a$; entonces $N = A$ en $A$: $N \subset A$ generado por la matriz $a$ es igual a $A$*

$$N = A.$$

*Demostración:* Como $a = (a_{ij}) \neq 0$ existe por lo menos un coeficiente $a_{j_0h_0}$ de esta matriz distinto de cero

$$a_{j_0h_0} \neq 0$$

Como $D$ por hipótesis es un álgebra con división existe $a_{j_0h_0}^{-1} \in D$; por tanto utilizando el lema 1 y tomando en cuenta que $N$ es un ideal bilateral obtenemos

$$\begin{aligned} e_{ii_0}ae_{h_0k} &= a_{i_0h_0}e_{ik} \\ e_{ik} &= (a_{i_0h_0}^{-1}e_{ii_0})ae_{h_0k} \in N \end{aligned}$$

$$\Longrightarrow \mathcal{M}_n(D) \subset N \Longrightarrow A \subset N \Longrightarrow A = N$$

**Lema 3.** *Si $M$ es un ideal izquierdo generado por la matriz $e_{11}$ en el álgebra $A$.*

$$M = Ae_{11}$$

*Entonces*

i) *$M$ está formado por las matrices $a = (a_{ij})$ con $a_{ij} = 0$ para toda $j \geq 2$.*

ii) $a \in M \implies e_{ij}a = a_{j1}e_{i1} \quad 1 \leq i,\ j \leq n$

iii) $a \in M, a \neq 0 \implies Ma = M$ *(es decir, $M$ es el ideal mínimo de $A$).*

iv) $x \in M \implies x = xe_{11}$

*Demostración:*

i) Sea $m \in M$, $m = ae_{11}$, $a \in A = \mathcal{M}_n(D)$. Calculando

$$m = (a_{ij})(x_{rs}) = \left(\sum_{j=1}^{n} a_{ij}x_{js}\right) = (a_{i1}x_{11}) = \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & 0 & \dots & 0 \\ \vdots & & \vdots & 0 \\ a_{n1} & 0 & \dots & 0 \end{pmatrix}$$

es la matriz $a_{ij}$ con $a_{ij} = 0$, $j \geq 2$.

ii) Sea $a \in M$, $a = (a_{ij})$. Calculando

$$\begin{aligned} e_{ij}a &= (x_{k\ell})(a_{ij}) = \left(\sum_{\ell=1}^{n} x_{k\ell}a_{\ell s}\right) = (x_{ij}a_{j1}) \\ &= a_{j1}e_{i1} \quad \text{se obtienen} \quad e_{ij}a = a_{j1}e_{i1} \end{aligned}$$

iii) Sea $a \in M$, $a = (a_{ij}) \neq 0$ $\exists a_{i_0 1} \neq 0$ $(1 \leq i_0 \leq n)$ como $D$ es una álgebra con división $\exists a_{i_0 1}^{-1} \in D$ como $e_{ij}a = a_{j1}e_{i1}$ (por el inciso anterior) se obtiene para $i = 1$ y $j = i_0$.

$$e_{1i_0}a = a_{i_0 1}e_{11} \implies e_{11} = a_{i_0 1}^{-1}e_{1i_0}a \in Ma$$

es decir $e_{11} \subset Ma \implies b \in A \implies be_{11} \in M$

$\forall b \in A$, $e_{11} \in Ma$, $be_{11} \in b(Ma) = (bM)a$

$\therefore$ $be_{11} \in Ma$ $\forall b \in A$, es decir $Ae_{11} \subset Ma$ pero $Ae_{11} = M$, entonces $M = Ma$.

iv) $xe_{11} = (x_{k\ell})(e_{ij}) = \left(\sum_{\ell=1} x_{k\ell}e_{\ell j}\right) = (x_{k1}e_{11})$ como $x \in M$, $x = (x_{k\ell})$ con $x_{k\ell} = 0 \quad \forall \ell \geq 2$. $\therefore$ $x = xe_{11}$.

**Corolario.** *(iii) implica que si $a \neq 0$, el ideal generado por $a$ es $M'$ y $\therefore$ un ideal izquierdo mínimo, es decir un $A$-módulo simple.*

*Afirmación:* El anillo de $A$-endomorfismos de $M = Ae_{11}$

$$\mathrm{End}_A(M) \cong D.$$

En efecto, dado un endomorfismo $f \in \mathrm{End}_A(M)$ es decir un $A$-automorfismo $f: M \to M$ tal que $f(am) = af(m)$ $a \in A$, $m \in M$ consideremos la imágen bajo $f$ del generador $M$

$$f(e_{11}) = a \qquad a = (a_{ij}) \in \mathcal{M}_n(D) = A.$$

*Afirmación:* La matriz $a \in A$ es tal que $a_{ij} = 0 \ \ \forall i, j \geq 2$

$$a = \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & & \dots & 0 \\ \vdots & & & \vdots \\ 0 & & \dots & 0 \end{pmatrix}$$

En efecto, calculando $f(e_{ij}e_{11}) = e_{ij}f(e_{11}) = e_{ij}a$ es decir $f(e_{ij}e_{11}) = e_{ij}a$. Aplicando (ii) del lema 3 se obtiene que $e_{ij}a = a_{j1}e_{i1}$ por tanto $f(e_{ij}e_{11}) = a_{j1}e_{i1}$ en particular si $i = 1$, $j = 1$ se obtiene $f(e_{11}e_{11}) = a_{11}e_{11}$ y como $e_{11}e_{11} = e_{11}$, entonces

$$a = f(e_{11}) = a_{11}e_{11} = \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & & \dots & 0 \\ \vdots & & & \vdots \\ 0 & & \dots & 0 \end{pmatrix}$$

En general sea $x \in M$ donde por (i) del lema 3 $x = (x_{ij})$ es tal que $x_{ij} = 0$ $\forall j \geq 2$; por (iv) del lema 3 se escribe $x = xe_{11}$ lo cual permite escribir

$$f(x) = f(xe_{11}) = xf(e_{11})$$

es decir

$$\begin{aligned} f(x) &= xa = \left(\sum_{j=1}^{n} x_{ij}a_{j\ell}\right) = (x_{i1}a_{11}) = (x_{ij}a_{11}) = (x_{ij})a_{11} \\ f(x) &= (x_{ij}a_{11}) \end{aligned}$$

$\therefore a_{11} \in D$ porque las matrices tienen sus coeficientes en $D$.

Se ha demostrado que no importa que elemento $f \in \operatorname{End} M$ se tome, éste siempre es de la forma

$$f(x) = xa \quad \text{con} \quad a = a_{11}e_{11}$$

para toda $x \in M$. Esto nos permite definir la aplicación

$$\begin{aligned} \psi\colon \operatorname{End}(M) &\to D \\ f &\longmapsto \psi(f) = a_{11} \end{aligned}$$

la cual es una función biyectiva, a todo $f$ le corresponde un elemento en $D$ a saber $a_{11}$ y recíprocamente.

Este demuestra que

$$\operatorname{End}(M) \cong D.$$

Consideremos $A$ como $A$-módulo de sí misma, por la *Proposición 1* sabemos que si $M$ es un $A$-módulo simple (como aquí lo supusimos) entonces

$$A \cong \oplus M_i \qquad \text{con} \qquad M_i \cong M$$

pero como $A$ es simple, esta suma se reduce a un sólo elemento

$$A \cong M_1 \qquad \text{con} \qquad M_1 \cong M$$

entonces $A \cong M$ y como $D$ es isomorfo a los endomorfismos de $M$, podemos afirmar que $D$ está unívocamente determinada por $A$ salvo isomorfismo. De la misma manera, como la dimensión de $A$ sobre $K$ es $n^2$ veces la dimensión de $D$, también $n$ está unívocamente determinada

Sea $A$ un álgebra sobre $K$ y sea $\psi$ su operación de multiplicación

$$\psi\colon A \times A \to A$$

definida por la correspondencia

$$(x, y) \longmapsto \psi(x, y) = x \cdot y$$

Si en enseguida se define otra operación $\phi$ sobre el espacio vectorial sobre $K$ subyacentee al álgebra $A$, a saber:

$$\phi: A \times A \to A$$

definida por la correspondencia

$$(x, y) \longmapsto \phi(x, y) = \phi(y, x) = y \cdot x$$

es fácil ver con esta nueva operación el espacio vectorial $A$ sobre $K$ deviene una álgebra sobre $K$ que se denota con el símbolo $A^\circ$. A esta álgebra se le llama *álgebra inversa* del álgebra $A$.

Consideremos la aplicación

$$f: A \times A^\circ \to \mathrm{End}_K(A)^1$$

definida por la correspondencia

$$(a, b) \longmapsto f(a, b)$$

donde $f(a, b)$ es el endomorfismo

$$f(a, b): A \to A$$

definido por la correspondencia

$$x \longmapsto f(a, b)x = axb$$

satisfaciendo las condiciones

1) $f(a, b)$ es bilineal con $a \in A$, $b \in A^\circ$.

2) $kf(a, b) = f(ka, b) = f(a, kb)$ para todo $k \in K = Z(A)$.

Es fácil ver que es bilineal pues $A$ es central además $1_A \cdot k \in A$ recordando que $Z(A) = \{x \in A \mid ax = xa \ \forall\, a \in A\}$.

[1] Un elemento de $\mathrm{End}_K(A)$ es $\psi: A \to A$ tal que $\psi(Kx) = K\psi(x)$

Utilizando la propiedad universal del producto tensorial obtenemos el diagrama conmutativo:

$$\begin{array}{ccc} A \times A^{\circ} & \xrightarrow{\varphi} & A \otimes A^{\circ} = C \\ f \searrow & & \swarrow \exists! F \\ & \mathrm{End}_K(A) & \end{array}$$

donde $F$ es una aplicación lineal tal que $F \circ \varphi = f$ o también $f(a,b) = F(a \otimes b)\ \forall a \in A,\ b \in A^{\circ}$.

**Proposición 3.** *Sea $A$ una $K$-álgebra. Sea $f(a,b)$ un $K$ endomorfismo de $A$ para toda $a \in A$ y toda $b \in A^{\circ}$: $f(a,b) \in End_K(A)$ y sea $F$ una aplicación $K$-lineal de $C = A \otimes A^{\circ}$ en $End_K(A)$.*

$$F{:}C \to End_K(A)$$

*definida por la correspondencia*

$$a \otimes b \to F(a \otimes b) = f(a,b)$$

*Entonces*

$$A \quad \textit{es simple} \quad \Longleftrightarrow \quad F \quad \textit{es suprayectiva}$$

$$A \quad \textit{es simple} \quad \Longleftrightarrow \quad F \quad \textit{es inyectiva}$$

*Cuando esto sucede $F$ es un isomorfimso sobre*

$$F{:}C \cong End_K(A)$$

*Demostración:* Se afirma que $F$ es un homomorfismo. En efecto, $F$ es lineal por construcción. Consideremos $c_1 = a_1 \otimes b_1$, $c_2 = a_2 \otimes b_2 \in A \times A^{\circ}$, si calculamos para $x \in A$

$$\begin{aligned} F(c_1c_2)x &= F((a_1 \otimes b_1) \cdot (a_2 \otimes b_2))x = F(a_1a_2 \otimes b_2 2b_1)x \\ &= f(a_1a_2 \otimes b_2b_1)x = a_1a_2xb_2b_1 \\ &= a_1(f(a_2,b_2)x)b_1 = f(a_1b_1)f(a_2b_2)x \\ &= F(c_1)F(c_2)x \end{aligned}$$

obtenemos

$$\begin{aligned} F(c_1c_2)x &= F(c_1)F(c_2)x \quad \forall x \in A \quad \text{es decir} \\ F(c_1c_2) &= F(c_1)F(c_2) \quad \therefore F \text{ es homomofismo.} \end{aligned}$$

Observemos que si $\dim_K A = N$, $N^2 = \dim_K C$ y $N^2 = \dim_K A \otimes A^\circ = \dim_K \mathrm{End}(A)$

Esto implica que

$$\begin{aligned} F{:}C &\cong \mathrm{End}_K(A) \iff F \text{ es suprayectiva y} \\ F{:}C &\cong \mathrm{End}_K(A) \iff F \text{ es inyectiva} \end{aligned}$$

Supongamos que $A$ no es simple, es decir, $A$ contiene un ideal $I$ bilateral $I \subset A \;\; I \neq \{0\}, I \neq A$. Esto implica que $f$ mapea $I$ en $I$:

$$f{:}I \to I$$

En efecto, calculando para $x \in I$

$$f(a,b)x = axb = (ax)b \in I$$

se obtiene

$$f(a,b)x \in I \quad \forall x \in I$$

Es decir para toda $(a,b) \in A \times A^\circ$ se tiene $F(a \otimes b){:}\, I \to I \;\; \forall (a,b) \in A \times A^\circ$ es decir, $F(a \otimes b) \in \mathrm{End}(I)$, por consiguiente $F(C) \subset \mathrm{End}(I)$ y como $I \subsetneq A$ propiamente se tiene $\mathrm{End}(I) \subseteq \mathrm{End}(A)$.

Por consiguiente

$$\mathrm{Im}C \subseteq \mathrm{End}(A)$$

es decir, $F$ no es suprayectiva. En otras palabras, si $F$ es suprayectiva entonces $A$ es simple.

Supongamos ahora que $A$ es simple. En este caso denotemos con $M$ al espacio vectorial sobre $K$ subyacente al álgebra $A$. si dotamos a $M$ de la operación

$$\phi{:}C \times M \to M$$

definida por la correspondencia

$$(c, m) \longmapsto \phi(c, m) = F(c)m = cm$$

es fácil ver que los axiomas de $C$-módulo sa satisfacen con esta operación de tal suerte que $M$ deviene un $C$-módulo izquierdo $M \in_c \mathcal{M}$.

Sea $M'$ un $C$-submódulo de $M$: $M' \subset M$ se afirma que

$$\begin{aligned} f(a,b)\colon M' &\to M' \\ m' &\longmapsto f(a,b)m' \in M' \end{aligned}$$

en efecto calculando

$$f(a,b)m' = F(a \otimes b)m' = F(c)m' = cm'$$

se obtiene

$$f(a,b)m' = c \cdot m' \in M'$$

y la afirmación esta demostrada.

Por otro lado

$$f(a,b)m' = am'b \in M'$$

Esto implica que $M'$ es un ideal bilateral en $M$ puesto que $a \in A$, $b \in A$ y $m' \in M'$, lo cual significa que $A$ contiene un ideal bilateral, pero por hipótesis $A$ es simple, entonces $M'$ sólo puede ser $M$, en otras palabras $M$ es simple.

Se ha demostrado que $M$ es un $C$-módulo simple. Como todo $C$-endomorfismo $\varphi$ de $M$

$$\varphi\colon M \to M$$

satisface la condición

$$\varphi(cm) = c\varphi(m)$$

usando la definición de $C$-módulo y calculando sabemos que

$$\varphi(c(m)) = \varphi(f(a,b)m) = \varphi(amb)$$

y

$$c\varphi(m) = F(c)\varphi(m) = f(a,b)\varphi(m) = a\varphi(m)b$$

obtenemos que

$$\varphi(amb) = a\varphi(m)b \quad \forall a, b \in A \quad m \in M$$

si $b = m = 1_A$ se obtiene

$$\varphi(a) = a\varphi(1_A) \quad \forall a \in A$$

se afirma que $\varphi(1_A) \in Z(A) = K$. En efecto como $amb \in A$ calculando

$$\begin{aligned} amb\varphi(1_A) &= \varphi(amb) = a\varphi(m)b \\ &= am\varphi(1_A)b \end{aligned}$$

se obtiene

$$amb\varphi(1_A) = am\varphi(1_A)b$$

si $a = m = 1_A$ entonces

$$b\varphi(1_A) = \varphi(1_A)b \quad \forall b \in A$$

Es decir

$$\varphi(1_A) \in Z(A) = K, \quad \varphi(1_A) = \xi \in K$$

Esto último implica qur todo $C$-endomorfismo

$$\varphi: M \to M$$

está definido por la correspondencia

$$m \longmapsto \varphi(m) = \varphi(1_A)m = \xi \cdot m$$

es decir $\varphi(m) = \xi m$ con $\xi \in K$.

Esto demuestra que los

$$\mathrm{End}_C M \cong K.$$

Ahora queremos un $C$-módulo fiel:

Sea $C' = \{c \in C \,|\, cm = 0 \quad \forall m \in M\}$ (el aniquilador de $M$ en $C$)

$$\begin{aligned} C' &= \{c \in C \,|\, F(c)m = 0 \quad \forall m \in M\} \\ C' &= \ker F \quad \text{que es un ideal en } C \end{aligned}$$

Esto permite definir el cociente

$$C/C'$$

Con esto dotaremos a $M$ de una estructura de $C/C'$-módulo como sigue

$$\psi: C/C' \times M \to M$$

definida por la correspondencia

$$(\{c\}, m) \longmapsto \tilde{\psi}(\{c\}, m) = cm$$

es fácil comprobar que esta apliación así definida es independiente del representante $C$ de la clase $\{c\}$.

Con esta operación es fácil también verificar que $M$ deviene un $C/C'$-módulo.

$$M \in_{C/C'} \mathcal{M}$$

es inmediato que el aniquilador de este $C/C'$-módulo es el ideal $\{0\}$, es decir $M$ es un $C/C'$-módulo fiel.

Como todo $C/C'$-endomorfismo

$$\phi: M \to M$$

es de la forma

$$m \longmapsto \phi(m) = zm \quad z \in Z(C/C')$$

Aplicando la proposición 2 a la $K$-álgebra $C/C'$ y al $C/C'$-módulo $M$ simple y fiel se obtiene que

$$C/C' \cong \mathcal{M}_n(K)$$

Como la $\dim_K M = n = N \quad \dim_K C/C' = \dim \mathcal{M}_n(K)$ y $\dim_K C/C' = \dim C \implies C' = \{0\}$. Todo esto demuestra $C \cong \mathcal{M}_n(K) \implies Z(C) = K$ y como $\mathcal{M}_n(K) \cong \mathrm{End}(A)$

$$C \cong \mathrm{End}_K(A)$$

**Corolario 1.** *Sea $L$ un campo que contiene al campo $K$. $L \supset K$. Entonces el álgebra*

$$A_L = A \otimes L \quad \textit{es simple} \quad \Longleftrightarrow \quad A \quad \textit{es simple}$$

*Demostración:* Se tiene el siguiente diagrama conmutativo:

$$\begin{array}{ccc} A_L \times A_L^\circ & \xrightarrow{\varphi} & A_L \otimes_L A_L^\circ \stackrel{?}{=} C_L \\ f_L \searrow & & \swarrow \ \exists!\, F_L : F_L(a \otimes b) = f_L(a,b) \\ & \mathrm{End}_K(A_L) & \end{array}$$

$$F_L : A_L \otimes A_L^\circ \to \mathrm{End}(A_L)$$

definida por la correspondencia

$$(a \otimes b) \longmapsto f_L(a,b)$$

donde

$$f_L(a,b) : A_L \to A_L$$

definida por la correspondencia

$$x \longmapsto f(a,b)x = axb$$

$f$ es bilineal.

Se afirma que $C_L = C \otimes_K L$. En efecto, por definición

$$C_L = (A \otimes_L L) \otimes (A^\circ \otimes_K L),$$

$A_L^\circ = A^\circ \otimes_K L$. pero como $L$ es conmutativo

$$C_L = (A \otimes A^\circ) \otimes (L \otimes_L L) = (A \otimes A^\circ) \otimes L = C \otimes_L L$$

es decir

$$C_L = A_L \otimes A_L^\circ$$

así obtenemos por la proposición 3 que $F_L$ mapea $C_L$ en los $\mathrm{End}_K(A_L)$.

**Corolario 2.** *Si $L$ es un campo algebraicamente cerrado que contiene a $K$: $L \supset k$. Entonces*

$$A \quad \textit{es simple} \quad \Longleftrightarrow \quad A_L \cong \mathcal{M}_n(L) \quad \textit{para} \quad n \geq 1.$$

*Demostración:* Observemos que si $D$ es una álgebra con división sobre $K$: ($1_D \in D$, $k \cdot 1_D \in D$) lo cual se puede suponer que $D \supset K$. Entonces si $\xi \in D - K$, $K(\xi)/K$ de $[K(\xi):K] = n$. Esto implica que si $L$ es algebráicamente cerrado $L = \overline{L}$ no existe ningún álgebra con división $D$ sobre $L$ distinta de $L$.

Si $A'$ es un álgebra sobre $L$, simple $\Longleftrightarrow$ $A' \cong \mathcal{M}_n(L)$, en particular $A_L$ es simple $\Longleftrightarrow$ $A_L \cong \mathcal{M}_n(L)$, si ahora aplicamos el corolario 1 se obtiene el corolario 2.

$$A \quad \text{es simple} \quad \Longleftrightarrow \quad A_L \cong \mathcal{M}_n(L).$$

**Corolario 3.** *la dimensión sobre $K$ es de la forma $n^2$* $\dim_K(A) = n^2$ *para alguna $n \geq 1$.*

*Demostración:* De acuerdo con el corolario 2 si $L = \overline{K}$ ($\overline{K}$ la cerradura algebraica de $K$) como por hipótesis $A$ es simple $\Longrightarrow$ $A_L \cong \mathcal{M}_n(L)$ para $n \geq 1$ y como $\dim_K A_L = n^2$.

Por otro lado

$$\dim_K A_L = \dim_K(A \otimes_K L) = \dim_K A$$

por consiguiente

$$\dim_K A = n^2 \quad \text{para cierta} \quad n \geq 1$$

**Corolario 4.** *Sean $A$, $B$ álgebras simples sobre $K$. Entonces el álgebra sobre $K$*

$$A \otimes_K B$$

*es simple*

*Demostración:* Sea $L = \overline{K}$, como

$$(A \otimes B)_L = A_L \otimes B_L \tag{1}$$

la hipótesis implica

$$\begin{aligned} A_L &\cong \mathcal{M}_n(L) \\ B_L &\cong \mathcal{M}_n(L) \\ A_L \otimes B_L &\cong \mathcal{M}_n(L) \otimes \mathcal{M}_m(L) \cong \mathcal{M}_{mn}(L) \end{aligned}$$

(1) implica (por corolario 2)

$$(A \otimes B)_L \cong \mathcal{M}_{mn}(L) \implies A \otimes B \quad \text{es simple}$$

**Corolario 5.** *Sea $A$ un álgebra simple sobre $K$ de $\dim_K(A) = n^2$, $L$ un campo tal que $L \supset K$ y sea*

$$F: A \to \mathcal{M}_n(L)$$

*un homomorfismo $K$-lineal, entonces la extensión lineal $L$-lineal*

$$F_L: A_L \to \mathcal{M}_n(L)$$

*es un isomorfismo.*

*Demostración:* Obsérvese que

$$A \hookrightarrow A \otimes_K L$$

definido por la correspondencia

$$a \longmapsto a \otimes_K 1_L$$

como todo $x \in A \otimes_K L$ se escribe como

$$x = \sum a_i \otimes_L \ell_i = \sum (a \times 1_K)\ell_i$$

entonces $F_L: A_L \to \mathcal{M}_n(L)$ definida por la correspondencia

$$x \to F_L(X) = \sum (F(a_i) \otimes L)\ell_i$$

Evidentemente la extensión $L$-lineal de $F$, a saber $F_L$, es un homomorfismo

$$F_L\left((a \otimes b)(b \otimes \ell)\right) = F_L(a \otimes \ell) F_L(a \otimes \ell)$$

$$F_L: A_L \to \mathcal{M}_n(L)$$

sea $I = \ker F_L = A_L$ $I$ es un ideal bilateral en $A_L$ pero el *Corolario 1* afirma que $A_L$ es simple, y como $F_L \neq 0$ entonces $\operatorname{Ker} F_L = \{0\}$ o sea $F_L$ es inyectiva.

Por lo anterior $F_L$ es biyectiva

$$A_L \cong \mathcal{M}_n(L)$$

Como $n^2 = \dim A = \dim A_L = \dim \mathcal{M}_n(L)$

$$\Longrightarrow A_L \cong \mathcal{M}_n(L) \quad \text{es sobre.}$$

**Corolario 6.** *Sea $L$ una extensión de $K$ $[L:K] = n$ y sea $A$ una álgebra simple de*

$$\dim_K A = n^2$$

*conteniendo un campo $L'$ isomorfo a $L$:*

$$L \cong L' \subset A$$

*Entonces*

$$A_L \cong \mathcal{M}_n(L)$$

*Demostración:* Supongamos que $L \subset A$. Considerese la aplicación

$$\psi: L \times A \to A$$

definida por la correspondencia

$$(\xi, a) \longmapsto \psi(\xi, a) = \xi \cdot a$$

es fácil ver que $A$ deviene un espacio vectorial $V$ sobre $L$ de $\dim_L V = n$.

$$V/L$$

Para toda $a \in A$ consideremos la aplicación $\alpha \in \mathrm{Aut}_K V$

$$\alpha: V \to V$$

definido por la correspondencia

$$v \longmapsto \alpha(v) = a \cdot v \quad a \in A, v \in V$$

es decir, para toda $a \in A$ se tiene una $\alpha \in \mathrm{Aut}\,(V)$

$$a \rightsquigarrow \alpha = (\ell_{ij}) \in \mathcal{M}_n(L)$$

esta correspondencia define un homomorfismo

$$F: A \to \mathcal{M}_n(L)$$

Por el corolario 5, se tiene el corolario 6.

**Proposición 4.** *Sea $A$ un álgebra simple sobre $K$. Entonces todo automorfismo $\alpha$ de $A$ sobre $K$ es de la forma $x \longmapsto a^{-1}xa$ con $a \in A^x$.*

*Demostración:* Se afirma todo elemento de $A \otimes A^\circ$ es de la forma única $\sum_{i=1}^{n} a_i \otimes b_i$ donde $\{a_1, \ldots, a_N\}$ es una base del álgebra $A$ y $b_i \in A^\circ$ para $i = 1, \ldots, N$.

En efecto $x \in A \otimes A^\circ$ en general $x = \sum_{i,j} \lambda_{ij} z_i \otimes w_j \quad z_i \in A, \quad w_j \in A^\circ$, $\lambda_{ij} \in K$ si $\{a_1, \ldots, a_N\}$ es base de $A$ entonces

$$\begin{aligned} z_i &= \sum_{K=1}^{N} \alpha_{ij} a_k, \quad \alpha_{ik} \in K \quad (1 \leq k \leq N) \\ x &= \sum_{i,j} \lambda_{ij} \left( \sum_{k=1}^{N} \alpha_{ik} a_k \right) \otimes w_j = \sum_{k=1}^{N} \left( \sum_{i,j} \lambda_{ij} \alpha_{ik} a_k \otimes w_j \right) \\ &= \sum_{k=1}^{N} (a_k \otimes \sum_{i,j} \lambda_{ij} \alpha_{ik} w_j) \end{aligned}$$

$$= \sum_{k=1}^{N} a_k \otimes b_k \qquad \text{con} \qquad b_k = \sum \lambda_{ij}\alpha_{ik}w_j, \quad b_k \in A^\circ$$

$$x = \sum_{i=1}^{N} a_i \otimes b_i$$

La representación es única pues si hubiera otra sucedería que

$$x = \sum_{i=1}^{N} a_k \otimes b_k = \sum_{i=1}^{N} a_k \otimes b'_k$$

puesto que

$$\sum_{i=1}^{N} a_k \otimes (b_k - b'_k) = 0 \implies b_k - b'_k = 0$$

ya que $a_k$ son linealmente independientes en $K$.

Sabemos que la proposición 3 que $F(A \otimes A^\circ) \cong \mathrm{End}_K(A)$ tal que dada $\alpha \in \mathrm{End}_K(A)$ existe

$$\alpha = F(\sum a_i \otimes b_i) = \sum_{i=1}^{N} F(a_i \otimes b_i) = \sum f(a_i \otimes b_i)$$

sea $x \in A$, entonces

$$\alpha(x) = F(\sum_{i=1}^{N}(a_i \otimes b_i))x = \sum f(a_i \otimes b_i) = \sum_{i=1}^{N} a_i x b_i$$

así

$$x \longmapsto \alpha(x) = \sum_{i=1}^{N} a_i x b_i, \qquad x \in A$$

Consideremos $x, y \in A$ y si calculamos

$$\alpha(x,y) = \alpha(x)\alpha(y) = (\sum_{i=1}^{N} a_i x b_i)\alpha(y) = \sum_{i=1}^{N} a_i x b_i \alpha(y)$$

obtenemos

$$\alpha(xy) = \sum_{i=1}^{N} a_i x b_i \alpha(y)$$

pero por definición

$$\alpha(xy) = \sum_{i=1}^{N} a_i x y b_i$$

por lo tanto

$$\sum_{i=1}^{N} a_i x b_i \alpha(y) = \sum_{i=1}^{N} a_i x y b_i,$$

es decir

$$\sum_{i=1}^{N} a_i x y b_i - \sum_{i=1}^{N} a_i x b_i \alpha(y) = 0$$

$$\sum_{i=1}^{N} a_i x (y b_i - b_i \alpha(y)) = 0$$

fija $y = y_0$ se tiene $\sum_{i=1}^{N} a_i x (y_0 b_i - b_i \alpha(y_0)) = 0$

$$\sum f(a_i, y_0 b_i - b_i \alpha(y_0)) x = 0$$

$$\sum F(a_i \otimes (y_0 b_i - b_i \alpha(y_0)) x = 0 \qquad \forall x \in A$$

Sabemos que por la proposición 3 $A \times A^{\circ} \cong F(A \otimes A^{\circ}) \cong \mathrm{End}(A)$

$$\sum_{i=1}^{N} a_i \otimes (y_0 b_i - b_i \alpha(y_0)) \implies y_0 b_i - b_i \alpha(y_0) = 0 \quad (1 \leq i \leq N)$$

Como ya se eligio arbitrariamente en $A$: $y_0 \in A$

$$y b_i = b_i \alpha(y) \qquad \forall y \in A \quad (1 \leq i \leq N). \tag{1}$$

Se afirma que $y(b_i A) \subset A \qquad \forall y \in A.$

En efecto, sea $z \in A$, entonces por (1)

$$\begin{aligned} (y b_i) z &= (b_i \alpha(y)) z \\ y(b_i z) &= b_i(\alpha(y) z) \in b_i A \end{aligned}$$

es decir

$$y(b_i A) \subset b_i A$$

pero

$$\forall a \in A, \quad a = \alpha(y) \quad \therefore \quad b_i \alpha(y) z \in b_i A$$

además $b_iA \cdot z \subset A \quad \forall z \in A$

$\therefore$ $b_iA$ es ideal bilateral, pero por hipótesis $A$ es simple, entonces

$$b_iA = \{0\} \quad \text{o} \quad b_iA = A$$

como $\sum_{i=1}^{N} a_i \otimes b_i \neq 0 \implies$ alguna $b_i \neq 0$ o sea

$$b_iA = A$$

Por consiguiente existe

$$b_i^{-1}$$

si definimos $a = b_i \neq 0$.

$(1) \implies \alpha(y) = a^{-1}ya \quad \forall y \in A.$

**Corolario:** *Como $\alpha$ y $a$ como en la prosición 4, y sea $a' \in A$ tal que $a'\alpha(x) = xa'$ para toda $x \in A$. Entonces $a' = \xi a$ con $\xi \in K$.*

*Demostración:* Por hipótesis se tiene

$$a'\alpha(x) = a' \quad \text{con} \quad a' \in A$$

entonces se puede decir por la proposición 4

$$a'a^{-1}xa = xa' \implies a'a^{-1}x = xa'a^{-1} \quad \forall x$$

esto significa que $a'a^{-1} \in Z(A)$ y $Z(A) = K$

$\therefore$ $a'a^{-1} = \xi$ con $\xi \in K$ es decir $a' = \xi a$.

**Proposición 5.** *Sea $D$ una álgebra con división sobre $K$ con $D \neq K$. Entonces $D$ contiene una extensión separable $L$ de $K$ distinta de $K$.*

*Demostración:* Sea $1_D \in D$ esto implica que $K \cdot 1_D \subset D$. Tómese un espacio suplementario $E$ al $K = K \cdot 1_D$ así podemos escribir

$$D = K \cdot 1_D \oplus E$$

consideremos los mapeos

$$\varphi = \mathrm{pr}_E : D \to E$$

definida por la correspondencia

$$x = k \cdot 1_D \oplus e \to \mathrm{pr}_E \cdot x = e$$

y

$$\psi_m : D \to D$$

definido por la correspondencia

$$x \longmapsto \psi_m(x) = x^m, \qquad m \geq 1$$

componiendo estas

$$\mathrm{pr}_E \circ \psi_m : D \to E$$

$$x \longmapsto \mathrm{pr}_E \psi_m(x) = \varphi(x^m)$$

es fácil que esta aplicación es polinomial puesto que

$$\varphi(x^m) = \varphi((k+e)^m) = k_1 \cdot e^1 + \cdots + e^m \quad \text{con} \quad k_1, \ldots, k_{m-1} \in K$$

Esta aplicación polinomial se puede extender linealmente a la aplicación

$$\varphi_L : D_L \to E_L$$

donde $L$ es un campo tal que

$$L \supset K$$

y sigue siendo polinomial.

Sea $\xi \in D - K \implies K(\xi)/K$ es finita y de grado $1 < [K(\xi) : K] < N = \dim_K(D)$. Como $K(\xi)$ es una extensión algebraica, es una extensión separable o contiene una extensión separable.

$$K \subset M \subset K(\xi) \qquad M/K \text{ ext. separable}$$

Supongamos, que la proposición es falsa, es decir, toda extensión de $K$ contenida en $D$ es puramente inseparable, a fortiori la $\mathrm{car}\, K = p > 1$.

Esto implica que todo elemento $\mathcal{H} \in D$ satisface una ecuación de la forma

$$\mathcal{H}^{p^n} - x = 0 \qquad \text{con} \qquad x \in K$$

de tal suerte que $[K(\mathcal{H}): K] = p^n$.

Calculando $[D: K] = [D: K(\mathcal{H})][K(\mathcal{H}): K]$

$$N = [D: K(\mathcal{H})]p^n$$

esto implica que

$$p^n \mid q \qquad \text{la máxima potencia de } p \text{ en } N$$

lo cual significa que

$$\mathcal{H}^q \in K$$

volviendo al mapeo

$$\varphi: D \to E$$

$$x \longmapsto \varphi(x^q) = \varphi(k^q \oplus e^q) = 0$$

Esto sigue sucediendo para

$$\varphi_L: D_L \to E_L$$

$$x \longmapsto \varphi_L(x^q) = 0$$

La aplicación de

$$D_L \to D_L$$

definida por la correspondencia

$$x \longmapsto x^q$$

envía $D$ en $L$ donde $L = Z(D_L)$

Pero esto conduce a la siguiente contradicción: si suponemos que $L$ es una extensión algebráica cerrada sobre $K$ y como se sabe que $D$ es simple $\Longrightarrow$ $D_L$ también es simple y entonces

$$D_L \cong \mathcal{M}_n(L)$$

si tomamos $x = e_{11} \implies x^q = e_{11} \notin Z(D_L)$ porque $e_{11}$ no es una matriz cuyos elementos de la diagonal son distintos entonces no estta en el centro. Por lo tanto queda establecido que toda extensión es separable.

**Corolario:** *Si $A$ es una álgebra simple sobre $K$ y si $L$ es la cerradura separable de $K$. $L \supset K$. Entonces*

$$A_L \cong \mathcal{M}_n(L)$$

*Demostración:* La hipótesis implica que $L$ no tiene extensiones separables distintas de $L$, pero la proposición 5 afirma que $D$ contiene una extensión separable, pero como $L$ es la mayor entonces $D = L$. Por otro lado $A$ es simple $\Rightarrow$ $A_L$ es simple y por la proposición 1 $A_L \cong \mathcal{M}_n(D)$ o sea $A_L \cong \mathcal{M}_n(L)$.

## 2 Las Representaciones de un Algebra Simple.

Sea $A$ un álgebra sobre $K$, simple, $L/K$: $L \supset K$

$$\mathcal{M}_L = \{F: A \to \mathcal{M}_n(L) \,|\, F \text{ es } K\text{-lineal}\}$$

Si $F \in \mathcal{M}_L$ entonces la aplicación

$$F: A \to \mathcal{M}_n(L)$$

está unívocamente definida por la correspondencia

$$a_i \to F(a_i) = X_i \qquad X_i \in \mathcal{M}_n(L) \tag{2}$$

Esto permite extender por la linealidad, a la transformación $L$-lineal

$$F_L: A_L \to \mathcal{M}_n(L)$$

donde $A_L = A \otimes_K L$.

De acuerdo con (1) se obtiene una correspondencia biunívoca entre $\mathcal{M}_L$ y $\{(X_1,\ldots,X_N)\,|\,X_i = F(a_i) = X_i \quad 1 \leq i \leq N \quad \forall F \in \mathcal{M}_L\}$, con $N = n^2$

$\mathcal{M}_L \cong \{(X_1,\ldots,X_N)\,|\,X_i = F(a_i), F \in \mathcal{M}_L \quad 1 \leq i \leq N\}\; F \longleftrightarrow (X_1,\ldots,X_N)$.

Por el corolario 5 de la proposición 3, si $F \in \mathcal{M}_L$ entonces

$$F_L\colon A_L \to \mathcal{M}_n(L)$$

es un isomorfismo sólo si $F$ es un homomorfismo. Si esto sucede, se dirá que $F$ es una $L$-representación de $A$.

$$\widehat{A} = \{F\colon A \to \mathcal{M}_n(L)\,|\,F \quad \text{es una } L\text{-representación}\}$$

Si $F$ y $F' \in \widehat{A}$ se afirma que $F'_L \circ F'_L$ es un automorfismo de $\mathcal{M}_n(L)$. En efecto, como

$$F_L\colon A_L \cong \mathcal{M}_n(L) \qquad \text{y} \qquad F_L\colon A_L \cong \mathcal{M}_n(L)$$

se obtiene una afirmación.

Si $L$ es algebraicamente cerrado entonces $\widehat{A} \neq \emptyset$.

Como $A$ es simple $A_L$ también es simple por la proposición 4. El automorfismo $F'_L \circ F_L^{-1}$ de $A_L$ es de la forma

$$X \to F'_L \circ F_L^{-1}(X) = Y^{-1}XY$$

$$x \in \mathcal{M}_n(L), \quad Y \in \mathcal{M}_n^x(L)$$

Como $F \in \widehat{A}$

$$F\colon A \to \mathcal{M}_n(L)$$

definida por la correspondencia

$$a \longmapsto F(a) = X \in \mathcal{M}_n(L)$$

Esto implica que $F'(a) = Y^{-1}F(a)Y$

Como $F'_L \circ F'_L(F(a)) = Y^{-1}F(a)Y$ y $a \in A$, se obtiene $F'F^{-1}(F(a)) = Y^{-1}F(a)Y$ puesto que $F_L\,|_A = F$.

Por tanto $F'(a) = Y^{-1}F(a)Y \quad \forall a \in A$ es decir

$$F' = Y^{-1}FY$$

Además cuando $F$ y $F'$ están dados, el corolario de la proposición 4 demuestra que $Y$ está unívocamente determinado salvo por un factor en el centro $L^x$ de $\mathcal{M}_n(L)^x$.

**Proposición 6.** *Sea $A$ un álgebra simple sobre $K$ de $\dim_K A = n^2$. Entonces existe una $K$-funcional lineal distinta de cero*

$$\tau: A \to K$$

*y una función con valores en $K$*

$$\nu: A \to K$$

*Si $L$ es una extensión de $K$: $L \supset K$ y si $F \in \widehat{A}$ entonces $\tau$ está definida por la correspondencia*

$$a \longmapsto \tau(a) = tr(F(a))$$

*y $\nu$ está definida por la correspondencia*

$$a \longmapsto \nu(a) = \det(F(a))$$

*Si el campo es infinito entonces los polinomios son funciones polinomiales.*

*Demostración:* Sea $\{a_1, \ldots, a_N\}$ una base de $A$ sobre $K$ con $N = n^2$. Si $L$ es la cerradura algebraica separable de $K$ en alguna cerradura algebraica de $K$, es decir,

$$L = \bigcup_{L_s \supset K} , \qquad [L_s: K] = n_s < +\infty$$

$L$ es un campo infinito. Por el corolario anterior existe una $L$-representación $F$ de $A$: $F \in \widehat{A}$ ($F: A \xrightarrow{\sim} \mathcal{M}_n$) y sea $F_L: A_L \to \mathcal{M}_n(L)$ su $L$ extensión lineal a $A_L = A \otimes_K L$, (entonces todas estas representaciones $F$ pueden ser escritas como $F' = Y^{-1}FY$ con $Y \in \mathcal{M}_n(L)^x$) con la cual definimos la aplicación

$$\tau: A_L \to K$$

por medio de la correspondencia

$$a \longmapsto \tau(a) = \mathrm{tr}(F_L(a))$$

así como la aplicación

$$\nu: A_L \to K$$

definida por la correspondencia

$$a \longmapsto \nu(a) = \det(F_L(a)).$$

Se afirma que $\tau$ es una $L$-forma lineal.

En efecto, como todo elemento

$$x \in A_L = A \otimes_K L$$

se puede escribir como

$$x = x_1 a_1 + \cdots + x_N a_N \qquad x_i \in L \quad (1 \leq i \leq N)$$

y si

$$F_L: A_L \to \mathcal{M}_n(L)$$

es la extensión lineal a $A_L$ de $F$.

Calculando para toda $a \in A_L$, $a = \sum_{i=1}^{N} x_i a_i$.

$$\begin{aligned} \tau(a) &= \operatorname{tr}(F_L(a)) \\ &= \operatorname{tr}(F_L(x_1 a_1 + \cdots + x_N a_N)) \\ &= \operatorname{tr}(x_1 F_L(a_1) + \cdots + x_N F_L(a_N)) \\ &= x_1 \operatorname{tr} F_L(a_1) + \cdots + x_N \operatorname{tr} F_L(a_N) \end{aligned}$$

obtenemos

$$\tau(a) = \ell_1 x_1 + \cdots + \ell_N x_N \quad \ell_i = \operatorname{tr}(F_L(a_i)) \in L$$

Análogamente se afirma que $\nu$ es un polinomio en $x_1, \ldots, x_N$. En efecto, calculando para toda $a \in A_L$

$$\begin{aligned} \nu(a) &= \det(F_L(a)) = \det(x_1 F_L(a_1) + \cdots + x_N F_L(a_N)) \\ &= \det(x_1(a_{k\ell}^{(1)}) + \cdots + x_N(a_{k\ell}^{(N)})) = \det\left(\sum_{i=1}^{N} x_i a_{k\ell}^{(i)}\right) \\ &= \sum \ell_{i_1,\ldots,i_m} x_{i_1}^{e_{i_1}} \cdots x_{i_m}^{e_{i_m}} \quad ; e_{i_1} + \cdots + e_{i_m} = N \quad x_i \in L \end{aligned}$$

obtenemos

$$\nu(a) = \sum \ell_{i_1 \cdots i_m} x_{i_1}^{e_{i_1}} \cdots x_{i_m}^{e_{i_m}} \qquad e_{i_1} + \cdots + e_{i_m} = N$$

es decir $\nu(a)$ es un polinomio en $x_1, \ldots, x_N$ con coeficientes en $L$.

Sea $\mathrm{Gal}\,(L/K)$ el grupo de Galois de la extensión $L$. Consideremos $\sigma \in \mathrm{Gal}(L/K)$ y definamos la aplicación

$$F^\sigma : A \to \mathcal{M}_n(L)$$

definido por la correspondencia

$$\begin{aligned} a \longmapsto F^\sigma(a) &= \sigma(F(a)) \\ &= \sigma(a_{ij}) \\ &= (\sigma a_{ij}) \end{aligned}$$

Se afirma que $F^\sigma$ es una $K$-forma lineal.

En efecto, si $a, b \in A$

$$\begin{aligned} f^\sigma(a+b) &= \sigma(F(a+b)) = \sigma(F(a) + F(b)) \\ &= \sigma((a_{ij}) + (b_{ij})) \\ &= \sigma(a_{ij} + b_{ij}) \\ &= (\sigma a_{ij} + \sigma b_{ij}) \\ &= (\sigma a_{ij}) + (\sigma b_{ij}) \\ &= F^\sigma(a) + F^\sigma(b) \end{aligned}$$

obtenemos

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

Sea $k \in K$, $a \in A$ y si calculamos

$$\begin{aligned} F^\sigma(ka) &= \sigma(F(ka)) \\ &= \sigma(kF(a)) = \sigma(k)\sigma(F(a)) \\ &= kF^\sigma(a) \end{aligned}$$

obtenemos $F^\sigma(ka) = kF^\sigma(a)$

$$\therefore \quad F \quad \text{es} \quad K\text{-forma lineal}$$

Evidentemente es un isomorfismo de $A$ en $\mathcal{M}_n(L)$ puesto que la aplicación

$$(a_{ij}) \longmapsto \tilde{\sigma}(a_{ij}) = (\sigma a_{ij})$$

es evidentemente un isomorfismo. Por consiguiente la composición

$$\begin{array}{ccccc} A & \xrightarrow{F} & \mathcal{M}_n(L) & \xrightarrow{\sigma} & \mathcal{M}_n(L) \\ a & \longmapsto & F(a) & \to & \sigma F(a) \end{array}$$

es un isomorfismo. Lo cual implica que su $L$-extensión

$$F_L^\sigma : A_L \to \mathcal{M}_n(L)$$

$F^\sigma$ es una $L$-representación de $A$: $F^\sigma \in \widehat{A}$.

Con esta $L$-representación definamos las aplicaciones

$$\tau^\sigma : A_L \to \mathcal{M}_n(L)$$

definida por la correspondencia

$$a \longmapsto \tau^\sigma(a) = \sum_{i=1}^{N} \sigma(\ell_i) x_i$$

y

$$\nu^\sigma : A_L \to \mathcal{M}_n(L)$$

definida por la correspodencia

$$a \longmapsto \nu^\sigma(a) = \sum_{i=1}^{N} \sigma(\ell_{i_1,\ldots,i_N}) x_{i_1}^{e_{i_1}} \cdots x_{i_m}^{e_{i_m}}$$

se afirma que

$$\begin{aligned} \tau^\sigma(a) &= \operatorname{tr}(F_L^\sigma(a)) \qquad \forall \sigma \in \operatorname{Gal}(L/K) \\ \nu^\sigma(a) &= \det(F_L^\sigma(a)) \end{aligned}$$

Calculando

$$\det(F^\sigma(a)) = \det\left(F_L^\sigma\left(\sum x_i a_i\right)\right)$$

por ser $F$ $L$-lineal

$$\begin{aligned}\det(F^\sigma(a)) &= \det(\sum x_i F^\sigma(a_i)) \\ &= \det(\sum x_i \sigma(F(a_i))) \\ &= \det((\sum_{i=1}^{N} x_i(\sigma a^i_{k\ell}))) \\ &= \sum_{i=1}^{N} \sigma(\ell_{i_1\ldots i_N}) x_{i_1}^{e_{i_1}} \cdots x_{i_N}^{e_{i_N}} \\ &= \nu^\sigma(a)\end{aligned}$$

obtenemos

$$\det(F^\sigma(a)) = \nu^\sigma(a)$$

Habida cuenta de la discusión inicial se afirma que dadas dos $L$-representaciones, en nuestro caso $F^\sigma$, $F \in \widehat{A}$ existe una $Y \in \mathcal{M}_n^\times(L)$ tal que $F_L^\sigma = Y^{-1}F_L Y$.

Por tanto, si calculamos

$$\begin{aligned}\tau^\sigma(a) &= \operatorname{tr}(F_L^\sigma(a)) = \operatorname{tr}(Y^{-1}F_L(a)Y) \\ &= \operatorname{tr} F_L(a) = \tau(a)\end{aligned}$$

obtenemos

$$\tau^\sigma(a) = \tau(a) \qquad \sigma \in \operatorname{Gal}(L/K)$$

Calculando

$$\begin{aligned}\nu^\sigma(a) &= \det(F_L^\sigma(a)) = \det(Y^{-1}F_L(a)Y) \\ &= \det(F(a)) = \nu(a)\end{aligned}$$

Así

$$\nu^\sigma(a) = \nu(a)$$

**Definiciones:** Las funciones $\tau$ y $\nu$ definidas en la proposición 6 se llaman la *traza reducida* y *la norma reducida* en $A$.

Evidentemente por proposiciones de la traza

$$\tau(xy) = \tau(yx)$$

también las propiedades del determinante

$$\nu(xy) = \nu(x)\nu(y)$$

para todo $x, y$ en $A$. En particular, $\nu$ determina un morfismo de $A^x$ sobre $K^x$.

**Corolario:** *Sea $A$ un álgebra simple sobre $K$ de $\dim_K A = N = n^2$ y sea*

$$\nu: A \to K$$

*la función de la proposición 6. Entonces para todo $a \in A$ los automorfismos del espacio vectorial subyacente del álgebra $A$*

$${}_a\rho: A \to A$$

*definido por la correspondencia*

$$x \to {}_a\rho(x) = ax$$

*y*

$$\rho_a: A \to A$$

*definido por la correspondencia*

$$x \longmapsto \rho_a(x) = xa$$

*tienen la misma norma:*

$$N_{A/K}(a) = (\nu(a))^n$$

*Demostración:* Sea $L$ una cerradura algebraica separable de $K$. De acuerdo con el corolario de la proposición 5 existe una $L$-representación de $A$:

$$F: A \to \mathcal{M}_n(L)$$

cuya extensión lineal $F_L$ al álgebra $A_L = A \otimes_K L$ por definición es un isomorfismo de $A_L$ sobre $\mathcal{M}_n(L)$

$$F_L: A_L \cong \mathcal{M}_n(L)$$

y como

$$A \cong A \otimes 1_L \subset A_L$$

es decir $A \subset A_L$ por tanto dado $a \in A$ se tiene $a = F_L(a) \in \mathcal{M}_n(L)$

$$_a\rho = {}_{F(a)}\rho : \mathcal{M}_n(L) \to \mathcal{M}_n(L)$$

definido por la correspondencia

$$x = (x_{ij}) \to F(a)$$

$$\rho(x) = F(a)x = F(a)(x_{ij})$$

la matriz asociada a la transformación

$$\cdot_{F(a)}\rho$$

es una matriz $n^2 \times n^2$ entonces si

$$R = (a_{k,\ell}^{(i,j)}) \subset \mathcal{M}_{n^2}(L)$$

Como $N_{A_L}(a) = N_{\mathcal{M}_n(L)/K}(F(a)) = \det[F(a)]^n$.

Recordando las identificaciones se puede escribir

$$N_{A/K}(a) = (\nu(a))^n$$

**Corolario 2.** *Sea $D$ un álgebra de división sobre $K$, $\tau_0$ y $\nu_0$ son la traza y norma reducidas respectivamente del álgebra $D$. Si $A = \mathcal{M}_n(D)$ entonces para toda matriz $x = (x_{ij}) \in A$ se tiene*

$$\tau(x) = \sum_{i=1}^{n} \tau_0(x_{ii})$$

*si $x$ es diagonal, es decir $x_{ij} = 0 \quad (1 \leq j < i \leq n)$*

$$\nu(x) = \prod_{i=1}^{n} \nu_0(x_{ii})$$

*Demostración:* Sabemos que dada $D$ un álgebra con división siempre existe una $L/K$ extensión separable en $D$: $L \subset D$.

Por tanto existe una $L$-representación $F$ del álgebra $D$

$$F: D \to \mathcal{M}_n(L)$$

y de aquí se define

$$\begin{aligned} \tau_0(d) &= \operatorname{tr}(F(d)) \\ \nu_0(d) &= \det(F(d)) \qquad \forall d \in D \end{aligned}$$

Es fácil ver que la aplicación

$$G: A \to \mathcal{M}_n(D)$$

definida por la correspondencia

$$x = (x_{ij}) \longmapsto G(x) = F((x_{ij}))$$

es una $D$-representación. Por consiguiente

$$\begin{aligned} \tau(x) &= \operatorname{tr}(G(x)) = \operatorname{tr}(F(x_{ij})) \\ &= \sum_{i=1}^{n} \operatorname{tr}(F(x_{ii})) \\ &= \sum \tau_0(x_{ii}) \end{aligned}$$

Habida cuenta que $x = (x_{ij})$ es una matriz diagonal podemos escribir

$$\begin{aligned} \nu(x) &= \det(F(x_{ij})) = \prod_{i=1}^{n} \det(F(x_{ii})) \\ &= \prod_{i=1}^{n} \nu_0(x_{ii}) \\ \nu(x) &= \prod_{i=1}^{n} \nu_0(x_{ii}) \end{aligned}$$

# 3 Conjuntos Factoriales y el Grupo de Brauer

Ahora se demostrara que el grupo de Brauer puede definirse en términos de "conjuntos factoriales".

Sea $K$ un campo, $\widetilde{K}$ una cerradura algebráica y se $K_{\text{sep}}$ la máxima extensión separable de $K$ en $\widetilde{K}$. Recordemos que

$$K_{\text{sep}} = \bigcup_{\substack{L \supset K \\ \text{separable} \\ [L:K]=n<\infty}} L \subset \widetilde{K} = K_{\text{sep}} \subset \widetilde{K}$$

Se denotará por $\mathcal{G}$ el grupo de Galois de $K_{\text{sep}}$ sobre $K$

$$\mathcal{G} = \text{Gal}(K_{\text{sep}}/K)$$

topologizando con la topología usual, a saber, tomando como sistema fundamental de vecindades del unitario $\epsilon \in \mathcal{G}$ a todos los subgrupos asociados a las extensiones separables $L/K$ de dimensión $n$

$$[L: K] = n < \infty$$

lo anterior indica que $\mathcal{G}$ es un grupo topológico compacto totalmente disconexo.

Como $\widetilde{K}$ es puramente inseparable sobre $K_{\text{sep}}$, todo automorfismo de $K_{\text{sep}}$ se puede extender de manera única a una extensión de $\widetilde{K}$ así $\mathcal{G}$ puede identificarse con el grupo de todos los automorfismos de $\widetilde{K}$ sobre $K$.

**Definición 1:** Sea $\mathcal{G}^{(m)} = \mathcal{G} \times \cdots \times \mathcal{G}$ $m$ factores iguales a $\mathcal{G}$. Sea $\mathcal{H}$ un subgrupo abierto de $\mathcal{G}$. Entonces se dirá que todo mapeo $f$ de $\mathcal{G}^{(m)}$ en un conjunto arbitrario $S$

$$f: \mathcal{G}^{(m)} \to S$$

es $\mathcal{H}$-regular si $f$ es constante sobre las clases residuales de $\mathcal{G}^{(m)} \text{mod} \mathcal{H}^{(m)}$

$$\mathcal{H}^{(m)} = \mathcal{H} \times \cdots \times \mathcal{H} \qquad (m \text{ copias de } \mathcal{H})$$

$$\mathcal{G}^{(m)}/\mathcal{H}^{(m)} = \mathcal{G}/\mathcal{H} \times \cdots \times \mathcal{G}/\mathcal{H}$$

es decir, depende más que de las clases

$$\xi\sigma_1 \cdots \xi\sigma_m, \qquad \sigma_1, \ldots, \sigma_m \in \mathcal{G}$$

en otras palabras

$$f(\sigma_1, \ldots, \sigma_n) = f(\mathcal{H}\sigma_1, \ldots, \mathcal{H}\sigma_n)$$

y por abuso de lenguaje se dice que $f$ es localmente constante.

Obsérvese que si $S$ está dotado de la topología discreta. Entonces una función $\xi$-regular es continua. Además por ser $\mathcal{G}^{(m)}$ compacto, es uniformente continua.

**Definición 2.** Sea $\mathcal{G}^{(m)} = \mathcal{G} \times \cdots \times \mathcal{G}$ ($m$-factores) un mapeo $f$ de $\mathcal{G}^{(m)}$ en $\mathcal{M}_n(K_{\text{sep}})$ se dirá que es *covariante* si satisface la condición

$$f(\sigma_1\lambda, \sigma_2\lambda, \cdots, \sigma\lambda) = f(\sigma_1, \cdots, \sigma_m)^{\lambda} \quad \forall \sigma_1, \ldots, \sigma_m, \lambda \in \mathcal{G}$$

**Lema 1.** *Sea $\mathcal{H}$ un subgrupo abierto de $\mathcal{G}$: $\mathcal{H} \subset \mathcal{G}$ y sea $L/K$ con $L \subset K_{sep}$ tal que*

$$L = \{x \in K_{sep} \mid \sigma x = x \quad \forall \sigma \in \mathcal{H}\}$$

*un mapeo $f$ $\mathcal{H}$-regular*

$$f: \mathcal{G} \to K_{sep}$$

*es covariante si y sólo si esta definida por la correspondencia*

$$\sigma \longmapsto f(\sigma) = \xi^{\sigma} \quad con \quad \xi \in L$$

*Demostración:* La condición es necesaria: como por hipótesis $f$ es covariante

$$f(\epsilon\sigma) = f(\epsilon)^{\sigma}$$

se denotará con $f(\epsilon) = \xi$ entonces

$$f(\sigma) = f(\epsilon\sigma) = f(\epsilon)^{\sigma} = \xi^{\sigma}$$

$$\therefore \quad f(\sigma) = \xi^{\sigma} \qquad \forall \sigma \in \mathcal{G}$$

la cual se puede escribir como

$$\begin{aligned} \xi^{\sigma} &= f(\sigma)^{\tau} = \xi^{\sigma\tau} \\ \xi^{\sigma} &= \xi^{\sigma\tau} \iff \sigma(\xi) = \sigma\tau(\xi) \\ \iff \xi &= \tau\xi \qquad \forall \tau \in \mathcal{H} \end{aligned}$$

por consiguiente $\xi \in L$.

El recíproco se obtiene de manera inmediata.

**Lema 2.** *sea $\mathcal{H}$ un subgrupo abierto del grupo*

$$\mathcal{G} = Gal(K_{sep}/K) \quad \textit{y sean el espacio vectorial sobre } K\text{:}$$

$$X_m = \{f : \mathcal{G}^m \to K_{sep} \mid f \quad \textit{es } \mathcal{G}\textit{-regular y covariante}\}$$

*y el espacio vectorial sobre $K_{sep}$*

$$X'_m = \{f : \mathcal{G}^{(m)} \to K_{sep} \mid f \ \textit{es } \mathcal{H}\textit{-regular}\}$$

*Entonces*

(i) $X'_m = X_m \otimes K_{sep}$

(ii) $\dim_{K_{sep}} X'_m = \dim_K X_m = n^m \qquad n = [\mathcal{G} : \mathcal{H}]$

*Demostración:* En primer lugar consideremos el campo

$$L = \{x \in K_{\text{sep}} \mid \sigma x = x \quad \forall \sigma \in \mathcal{H}\}$$

La hipótesis $n = [\mathcal{G} : \mathcal{H}]$ implica que $\dim_K L = n$.

En seguida consideremos un sistema completo de representantes de las clases $\mathcal{H}\sigma$ residuales mod $\mathcal{H}$ en $\mathcal{G}$:

$$\sigma = \{\sigma_1, \ldots, \sigma_n\}$$

Observemos que todo elemento $x \in X_m$ está unívocamente determinado por los valores que toma sobre el producto $L$ cartesiano

$$\alpha \times \alpha \times \cdots \times \alpha \qquad m - \text{factores iguales}$$

los cuales se pueden asignar arbitrariamente

$$x(\sigma_{i_1}, \ldots, \sigma_{i_m}) = a_{i_1,\ldots,i_m}$$

Esto permite definir las funciones

$$f_{i_1,\ldots,i_m}: \mathcal{G}^{(m)} \to K_{\text{sep}}$$

por medio de la correspondencia

$$\begin{aligned}(x_1, \ldots, x_m) &\longmapsto f_{i_1,\ldots,i_m}(x_1, \ldots, x_m) \\ &= \begin{cases} 1 & \text{si } (x_1, \ldots, x_m) = (\sigma_{i_1}, \ldots, \sigma_{i_m}) \\ 0 & \text{en caso contrario} \end{cases}\end{aligned}$$

con $(i_1, \ldots, i_m) \qquad 1 \leq i_k \leq n.$

Estas $n^m$ funciones pertenecen al espacio $X_m$ y son linealmente independientes sobre $K$.

En efecto, calculando si

$$\begin{aligned} 0 &= \Big(\sum_{(i_1,\ldots,i_m)} c_{i_1,\ldots,i_m} f\Big)(\sigma_{j_1,\ldots,\sigma_{j_m}}) \\ &= \sum_{(i_1,\ldots,i_m)} c_{i_1,\ldots,i_m} f_{i_1,\ldots,i_m}(\sigma_{j_1}, \ldots, \sigma_{j_m}) = c_{j_1,\ldots,j_m} \\ &\Longrightarrow c_{j_1\ldots j_m} = 0 \qquad \forall (j_1 \cdots j_m) \end{aligned}$$

Por lo tanto, son linealmente independientes.

Además las funciones

$$\{f_{i_1,\ldots,i_m}\}$$

generan al espacio $X_m$. En efecto, sea $x \in X_m$ y supongamos $x(\sigma_{i_1}, \ldots, \sigma_{i_m}) = a_{i_1,\ldots,i_m} \quad \forall (i_1, \ldots, i_m)$ es inmediato que podemos escribir

$$x = \sum a_{i_1,\ldots,i_m} f_{i_1,\ldots,i_m}$$

En efecto, calculando

$$\begin{aligned} \sum a_{j_1,\ldots,j_m} f_{j_1,\ldots,j_m}(\sigma_{i_1}, \ldots, \sigma_{i_m}) &= a_{i_1,\ldots,i_m} \\ &= x(\sigma_{i_1}, \ldots, \sigma_{i_m}) \end{aligned}$$

Por tanto toda $x \in X_m$ se puede expresar como

$$(*) \qquad x = \sum_{(i_1,\ldots,i_m)} x(\sigma_{i_1},\ldots,\sigma_{i_m}) f_{i_1,\ldots,i_m} \in X_m$$

con $(1 \leq i_k \leq n)$, es decir, $\dim_K X_m = n^m$.

Se afirma que toda forma lineal $\wedge$ sobre $X_m$:

$$\wedge: X_m \to K_{\text{sep}}$$

se puede escribir como

$$\wedge(x) = \sum \gamma_{i_1,\ldots,i_m} x(\sigma_{i_1},\ldots,\sigma_{i_m})$$

donde $\gamma_{i_1,\ldots,i_m} \in K_{\text{sep}}$. En efecto, calculando y por $(*)$

$$\begin{aligned} \wedge(x) &= \wedge\left(\sum_{(i_1,\ldots,i_m)} x(\sigma_{i_1},\ldots,\sigma_{i_m}) f_{i_1,\ldots,i_m}\right) \\ &= \sum x(\sigma_{i_1},\ldots,\sigma_{i_m}) \wedge (f_{i_1,\ldots,i_m}) \end{aligned}$$

si definimos $\gamma_{i_1,\ldots,i_m} = \wedge(f_{i_1,\ldots,i_m})$ podemos escribir

$$\wedge(x) = \sum_{(i_1,\ldots,i_m)} \gamma_{i_1,\ldots,i_m} x(\sigma_{i_1},\ldots,\sigma_{i_m})$$

Y así la afirmación está demostrada.

Demostración por inducción sobre $m$.

Para $m = 1$ el lema 1 implica que $X_1$ como espacio vectorial sobre $K$, es isomorfo a $L$:

$$X_1 \cong L$$

y como $n = [\mathcal{G}:\mathcal{H}]$ se tiene que

$$[L:K] = n = \dim_K L = \dim X_1$$

Se afirma que $X_1' = X_1 \otimes_K K_{\text{sep}}$, es decir $X_1$ está generado por $X_1$. Supongamos que este no es el caso

$$\langle X_1 \rangle \subsetneq \{0\}$$

$$\therefore \qquad X_1'/\langle X_1\rangle \neq \{0\}$$

entonces existe una forma lineal.

$\wedge: X_1'/\langle X_1\rangle \to K_{\text{sep}}$ distinta de 0, como $\tilde{0} \in X_i/\langle X_1\rangle$

$$\wedge(\langle X_1\rangle) = \wedge(\tilde{0}) = 0$$

en particular

$$\wedge(X_1) = 0$$

es decir, para toda $x \in X_1$

$$\begin{aligned} \wedge(x) &= \sum \gamma_i x(\sigma_i) = 0 \\ &= \sum_{i=1}^{n} \gamma_i \xi^{\sigma_i} = \sum_{i=1}^{n} \gamma_i \sigma_i(\xi) \quad \text{con} \quad \xi \in L \\ &= \sum_{i=1}^{n} \gamma_i \lambda_i(\xi) \end{aligned}$$

o sea

$$0 = (\sum \gamma_i \lambda_i)(\xi) \qquad \forall \xi \in L$$

es decir

$$\sum \gamma_i \lambda_i = 0$$

como las restricciones $\lambda_i$ de $\sigma_i$ a $L$ son linealmente indpendientes

$$\gamma_i = 0 \qquad \forall 1 \leq i \leq n$$

esto implica que $\wedge = 0$ lo cual es una contradicción.

Por consiguiente

$$X_1' = X_1 \otimes_K K_{\text{sep}}$$

$\dim_{K_{\text{sep}}} X_1' = \dim_K X_1 = n$

Sea $m > 1$ y supongamos que se ha demostrado para $m - 1$.

$$\begin{aligned} Y_m &= X_1 \otimes_K \cdots \otimes_K X_1 \quad m\text{-factores iguales a } X_1 \\ Y_m' &= X_1' \otimes_{K_{\text{sep}}} \cdots \otimes_{K_{\text{sep}}} X_1' \\ &= (X_1 \otimes_{K_{\text{sep}}}) \otimes_{K_{\text{sep}}} (X_1 \otimes_K K_{\text{sep}}) \otimes_{K_{\text{sep}}} \cdots \otimes_{K_{\text{sep}}} (X_1 \otimes K_{\text{sep}}) \end{aligned}$$

usando asociatividad y conmutatividad del producto tensorial se obtiene

$$Y'_m = Y_m \otimes_K K_{\text{sep}}$$

Consideremos ahora la aplicación

$$\Phi: Y'_m \to X'_m$$

definida por la correspondencia

$$\begin{aligned} x_1 \otimes \cdots \otimes x_m &\longmapsto \Phi(x_1 \otimes \cdots \otimes x_m)(\sigma_{i_1}, \ldots, \sigma_{i_m}) \\ &= x_1(\sigma_{i_1}) x_2(\sigma_{i_2}) \cdots x_m(\sigma_{i_m}) \end{aligned}$$

*Afirmación:* $\Phi$ es suprayectiva. Supongamos que no, es decir, $\phi(Y'_m) \subset X'_m$ propiamente, es decir

$$X_m/\Phi(Y'_m) \neq \{0\}$$

Sea $\wedge: X_m/\Phi(Y'_m) \to K_{\text{sep}}$ una forma lineal distinta de cero $\wedge \neq \{0\}$ es decir $\Phi(Y'_M) = \tilde{0}$, $\tilde{0} \in X'_m/\Phi(Y'_m)$, es decir

$$\wedge(\Phi(Y'_m)) = \wedge(\tilde{0}) = 0$$

en otras palabras $\wedge$ se anula sobre $\Phi(Y'_m)$ sea $\Phi(x_1 \otimes \cdots \otimes x_m) \in \Phi(Y'_m)$ por tanto

$$\begin{aligned} 0 &= \wedge(\Phi(x_1 \otimes \cdots \otimes x_m)) \\ &= \sum \gamma_{i_1 \ldots i_m} \Phi(x_1 \otimes \cdots \otimes x_m)(\sigma_{i_1} \ldots \sigma_{i_m}) \\ &= \sum \gamma_{i_1 \ldots i_m} x_1(\sigma_{i_1}) x_2(\sigma_{i_2}) \cdots x_m(\sigma_{i_m}) \end{aligned}$$

$$\Rightarrow \gamma_{i_1 \ldots i_m} = 0 \qquad \forall\, (i_1, \ldots, i_m) \Rightarrow \wedge = 0$$

lo cual contradice la elección de $\wedge$.

Por lo anterior $\Phi$ es suprayectiva.

Ahora se afirma que $\Phi$ es un isomorfismo.

Se sabe que la dimensión

$$\dim_{K_{\text{sep}}} X'_m = n^m \tag{2}$$

y del acuerdo con el caso $m = 1$

$$\dim_{K_{\text{sep}}} X'_1 = \dim_K X_1 = n$$

Esto implica que

$$\dim_{K_{\text{sep}}} Y'_m = n^m \tag{3}$$

(2) y (3) implican $\dim_{K_{\text{sep}}} Y'_m = \dim_{K_{\text{sep}}} X'_m$.

Y así la afirmación está demostrada.

Consideremos finalmente una base sobre $K$

$$\{f_1, \ldots, f_n\}$$

de $X_1$. Entonces la familia

$$\{f_{i_1} \otimes f_{i_2} \otimes \cdots \otimes f_{i_m}\}_{(i_1,\ldots,i_m)}$$

es una base de $Y'_m$ sobre $K_{\text{sep}}$ y como $\Phi$ es un isomorfismo la familia

$$\{\Phi(f_i \otimes \cdots \otimes f_{i_m})\}_{(i_1,\ldots,i_m)}$$

es una base de $X'_m$ sobre $K_{\text{sep}}$.

Esto último significa que todo elemento $x$ de $X'_m$: $x \in X'_m$ se puede expresar como

$$\begin{aligned} x &= \sum \gamma_{i_1,\ldots,i_m} \Phi(f_{i_1} \otimes \cdots \otimes f_{i_m}) \\ x(\sigma_1\lambda \cdots \sigma_m\lambda) &= (x(\sigma_1, \ldots, \sigma_m))^\lambda \\ &= \sum (\gamma_{(i_1\ldots i_m)})^\lambda (\Phi(f_{i_1} \otimes \cdots \otimes f_{i_m})(\sigma_1, \ldots, \sigma))^\lambda \\ &= \sum \gamma_{i_1\ldots i_m} f_{i_1}^\lambda(\sigma_{i_1}) \cdots f_{i_m}^\lambda(\sigma_{i_m}) \end{aligned}$$

$$\begin{aligned} x(\sigma_1\lambda, \ldots, \sigma_m\lambda) &= \sum \gamma_{i_1\cdots i_m} \Phi(f_{i_1} \otimes \cdots \otimes f_{i_m})(\sigma_1\lambda, \ldots, \sigma_m\lambda) \\ &= \sum \gamma_{i_1\cdots i_m} f_{i_1}(\sigma_1\lambda) \cdot f_{i_m}(\sigma_m\lambda) \\ &= \sum \gamma_{i_1\cdots i_m} f_{i_1}^\lambda(\sigma_1) \cdots f_{i_m}^\lambda(\sigma_m) \end{aligned}$$

por tanto

$$\sum \gamma_{i_1\cdots i_m} f^{\lambda}_{i_1}(\sigma_1)\cdots f^{\lambda}_{i_m}(\sigma_m) = \sum \gamma^{\lambda}_{i_1\cdots i_m} f^{\lambda}_{i_1}(\sigma_1)\cdots f^{\lambda}_{i_m}(\sigma_m)$$

Como $(\sigma_1,\ldots,\sigma_m)$ se eligío arbitrariamente en $\mathcal{G}^{(m)}$ se obtiene

$$\sum \gamma_{i_1\cdots i_m} f_{i_1}(\sigma_1\lambda)\cdots f_{i_m}(\sigma_m\lambda) = \sum \gamma^{\lambda}_{i_1\cdots i_m} f_{i_1}(\sigma_1\lambda)\cdots f_{i_m}(\sigma_m\lambda)$$

Así

$$\sum(\gamma_{i_1\cdots i_m} - \gamma^{\lambda}_{i_1\cdots i_m}) f_{i_1}(\sigma_1)\cdots f_{\sigma i_m}(\sigma_m)$$

este es el resultado de calcular

$$\sum(\gamma_{i_1\cdots i_m} - \gamma^{\lambda}_{i_1\cdots i_m}) f_{i_1}\otimes\cdots\otimes f_{i_m}(\sigma_1,\ldots,\sigma_m$$

$$\forall\ (\sigma_1,\ldots,\sigma_m)\in\mathcal{G}^{(m)}$$

$$\Rightarrow\ \sum(\gamma_{i_1\ldots i_m} - \gamma^{\lambda}_{i_1\ldots i_m}) f_{i_1}\otimes\cdots f_{i_m} = 0$$

y como $\{f_{i_1\cdots i_m}\}_{(i_1,\ldots,i_m)}$ es una base de $Y'_m$ se tiene $\gamma_{i_1,\ldots,i_m} = \lambda(\gamma_{i_1\cdots i_m})\ \forall\ \lambda\in\mathcal{H}$

$$\Rightarrow\ \gamma_{i_1\cdots i_m}\in K,$$

es decir, $\Phi$ es un isomorfismo sobre $K$;

$$\begin{aligned}\dim_K Y'_m &= \dim_K X'_m = n^m\\ \dim_{K_{\text{sep}}} X'_m &= n^m\end{aligned}$$

y como $\dim_K X'_m = \dim_K X_m \Rightarrow \dim_K X_m = n^m \ \dim_{K_{\text{sep}}} X'_m$.

Sea $K'$ cualquier campo que contiene a $K$ y sea $\overline{K}'$, $K'_{\text{sep}}$ $\mathcal{G}$ definidas para $K'$ como $\overline{K}$, $K_{\text{sep}}$, $\mathcal{G}$ han sido definidas para $K$. Como $\overline{K}$ está determinado unicamente salvo isomorfismo, siempre asumiremos, en esta situación, que tomamos $\overline{K}$ como la cerradura algebraica de $K$ en $\overline{K}'$. Es obvio que $K_{\text{sep}}\subset K'_{\text{sep}}$. Todo automorfismo $\sigma'$ de $\overline{K}'$ sobre $K'$ induce en $\overline{K}$ un automorfismo $\sigma$ de $\overline{K}$ sobre $K$ (más precisamente, sobre $\overline{K}\cap K'$); claramente la correspondencia $\sigma'\to\sigma$ induce un morfismo continuo $\rho$ de $\mathcal{G}'$ en $\mathcal{G}$; éste se llamará el *morfiso restricción*; este morfismo es inyectivo si $K'$ es algebraico sobre $K$, entonces $\overline{K}' = \overline{K}$; en este caso identificaremos $\mathcal{G}'$ con su imagen en

$\mathcal{G}$, que es siempre un subgrupo cerrado de $\mathcal{G}$ y es abierto en $\mathcal{G}$ cuando $K'$ es de grado finito sobre $K$.

Si $\mathcal{H}$ es cualquier subgrupo abierto de $\mathcal{G}$ y $L$ es el subcampo correspondiente de $K_{\text{sep}}$, es decir aquél que consiste de los elementos invariantes bajo $\mathcal{H}$, el subgrupo $\mathcal{H}' = \rho^{-1}\mathcal{H}$ de $\mathcal{G}'$ es abierto y el subcampo correspondiente de $K'_{\text{sep}}$ es el generado por $L$ sobre $K'$.

Sea $f$ como en la definición 2, es decir, un mapeo de $\mathcal{G}^{(m)}$ en algún conjunto $S$.

Escribiremos $f \circ \rho$ para el mapeo

$$f \circ \rho : \mathcal{G}'^{(m)} \to S$$

definido por la correspondencia

$$(\sigma'_1, \cdots, \sigma'_m) \to f(\rho(\sigma_1), \ldots, \rho(\sigma'_m))$$

Este es obviamente continuo, es decir, localmente constante, si $f$ lo es; si $f$ es $\mathcal{H}$-regular, éste es $\mathcal{H}'$-regular, con $\mathcal{H}' = \rho^{-1}(\mathcal{H})$; Si $S = \mathcal{M}_n(K_{\text{sep}})$ y $f$ es covariante, $f \circ \rho$ es covariante. Si $K'$ es algebráico sobre $K$, $\mathcal{G}'$ es un subgrupo de $\mathcal{G}$ y $\rho$ es su inyección natural sobre $\mathcal{G}$; entonces $f \circ \rho$ es la restricción de $f$ a $\mathcal{G}'^{(m)}$.

Después de estas preliminares, podemos regresar a nuestro tópico principal.

**Teorema 2.** *Sea $A$ un álgebra simple sobre $K$. Sea $\mathcal{H}$ un subgrupo abierto de $\mathcal{G}$, $L$ el subcampo correspondiente de $K_{sep}$ y sea $F$ una $L$-representación de $A$. Entonces existe un mapeo covariante $\mathcal{H}$-regular*

$$Y : \mathcal{G} \times \mathcal{G} \to \mathcal{M}_n(K_{sep})^x$$

*tal que*

$$F^\sigma = Y(\rho, \sigma)^{-1} F^\rho Y(\rho, \sigma) \qquad \rho, \sigma \in \mathcal{H}$$

*Si existe tal $Y$ entonces existe un mapeo covariante*

$$f : \mathcal{G} \times \mathcal{G} \times \mathcal{G} \to K_{sep}$$

*tal que para todo* $\rho, \sigma, \tau$ *en* $\mathcal{G}$ *se tiene*

$$(A) \qquad f(\rho,\sigma,\tau)f(\nu,\rho,\tau) = f(\nu,\sigma,\tau)f(\nu,\rho,\sigma)$$

*Demostración:* Por hipótesis

$$F_L: A_L \cong \mathcal{M}_n(L)$$

lo cual implica que la aplicación

$$F: A \to \mathcal{M}_n(L)$$

es un homomorfismo, esto es a su vez significa que para toda $\lambda \in \mathcal{G}$

$$F^\lambda: A \to \mathcal{M}_n(K_{\text{sep}})$$

también es un homomorfismo, por consiguiente

$$F^\lambda_{K_{\text{sep}}}: A_{K_{\text{sep}}} \cong \mathcal{M}_n(K_{\text{sep}})$$

es decir, $F^\lambda$ es una $K_{\text{sep}}$-representación de $A$, además sabemos que $F^\lambda$ se puede expresar como

$$F^\lambda = Z(\lambda)^{-1} F Z(\lambda) \qquad Z(\lambda) \in \mathcal{M}_n(K_{\text{sep}})$$

es fácil ver que $F^\lambda$ no depende más que de la clase $\mathcal{H}\lambda$ lo cual significa que la aplicación

$$\begin{aligned} Z: \mathcal{G} &\to \mathcal{M}_n(K_{\text{sep}}) \\ \lambda &\longmapsto Z(\lambda) \end{aligned}$$

es $\mathcal{H}$-regular. Esto nos permite definir la aplicación

$$Y: \mathcal{G} \times \mathcal{G} \to \mathcal{M}_n(K_{\text{sep}})$$

definido por la correspondencia

$$(\rho,\sigma) \longmapsto Y(\rho,\sigma) = Z(\sigma\rho^{-1})^\rho$$

Calculando

$$F^{\sigma\rho^{-1}} = Z(\sigma\rho^{-1})^{-1}F^{\rho}Z(\sigma\rho^{-1})$$

como $\rho$ es homomorfismo y $Z$ matriz

$$F^{\rho\sigma\rho^{-1}} = (Z(\sigma\rho^{-1})^{\rho})^{-1}F^{\rho}Z(\sigma\rho^{-1})\rho$$

como $\mathcal{G}$ es conmutativo

$$F^{\sigma} = Y(\rho,\sigma)^{-1}F^{\rho}Y(\rho,\sigma) \qquad \forall\rho,\sigma \in \mathcal{G}$$

Sea $A$ un sistema completo de representantes de las clases residuales dobles $\mathcal{G}\,\mathrm{mod}\mathcal{H}$

$$\{\mathcal{H}\times\mathcal{H}\}_{\lambda\in\Lambda}$$

observemos que $F$ y $F^{\lambda}$ son $L$-representaciones de $A$ donde $L' = L(L^{\lambda}) = L\cdot L^{\lambda}$ para todo $\lambda \in \mathcal{G}$. En efecto, como

$$F{:}A \rightarrow \mathcal{M}_n(L') \qquad \text{y}$$

$$F^{\lambda}{:}A \rightarrow \mathcal{M}_n(L')$$

son homomorfismos, la proposición asegura que

$$\begin{aligned} F_{L'}{:}A_{L'} &\cong \mathcal{M}_n(L') \quad \text{y} \\ F^{\lambda}_{L'}{:}A_{L'} &\cong \mathcal{M}_n(L') \quad \text{con} \quad K \subset L \subset L' \\ L^{\lambda} &= \lambda L \end{aligned}$$

Elijamos a $Z(\lambda) \in \mathcal{M}_n(L')^x$ tal que

$$F^{\lambda} = Z(\lambda)^{-1}FZ(\lambda)$$

Como $F^{\lambda}$ es una $L'$-repressentación, podemos expresarla como

$$F^{\lambda} = Z(\lambda)^{-1}FZ(\lambda)$$

con $Z(\lambda) \in \mathcal{M}_n(L')$

Por otro lado, como todo elemento $\rho \in \mathcal{G}$ se puede expresar como

$$\rho = \alpha\lambda\beta^{-1} \qquad \text{con} \qquad \alpha,\beta \in \mathcal{H}$$

y $\lambda$ unívocamente determinada: supongamos que se tiene otra representación de $\rho$

$$\rho = \alpha' \lambda \beta'^{-1}$$

es decir

$$\begin{aligned} \alpha' \lambda \beta'^{-1} &= \alpha \lambda \beta^{-1} \implies \lambda \beta'^{-1} = \alpha'^{-1} \alpha \lambda \beta^{-1} \\ \implies \beta'^{-1} \beta &= \lambda^{-1} (\alpha'^{-1} \alpha) \lambda \\ \gamma \in \lambda^{-1} \mathcal{H} \lambda \cap \mathcal{H} &\implies \gamma \in \lambda^{-1} \delta \lambda \quad \text{con} \quad \delta \in \mathcal{H} \end{aligned}$$

*Afirmación:* $\gamma$ deja fijos a $L$ y $L^\lambda$. En efecto, calculando: sea $\lambda \ell \in L^\lambda$

$$(\lambda \ell)^{\lambda^{-1} \delta \lambda} = ((\lambda^{-1} \lambda) \ell)^{\delta \lambda} = \ell^{\delta \lambda} = (\delta \ell)^\lambda = \ell^\lambda = \lambda \ell$$

Si $\mathcal{H}$ es normal entonces $\gamma$ deja fijo también a $L$.

Por consiguiente la aplicación

$$\begin{aligned} Z : \mathcal{G} &\longmapsto \mathcal{M}_n(L')^\times \\ \rho &\longmapsto Z(\rho) = Z(\lambda)^\rho \end{aligned}$$

no depende de la representación (1) de $\rho$ esto demuestra que la aplicación

$$Y : \mathcal{G} \times \mathcal{G} \to \mathcal{M}_n(K_{\text{sep}})$$

definida por la correspondencia

$$(\rho, \sigma) \longmapsto Y(\rho, \sigma) = Z(\sigma, \rho^{-1})^\rho$$

es localmente constante.

*Afirmación:* $Y$ es covariante. En efecto, si calculamos

$$\begin{aligned} Y(\rho\lambda, \sigma\lambda) &= Z(\sigma\lambda(\rho\lambda)^{-1})^{\rho\lambda} = \\ &= Z(\sigma\rho^{-1})^{\rho\lambda} = \\ &= ((Z(\sigma\rho^{-1})^\rho)^\lambda = \\ &= Y(\rho, \sigma)^\lambda \end{aligned}$$

obtenemos

$$Y(\rho\lambda, \sigma\lambda) = (Y(\rho, \sigma))^{\lambda} \qquad \forall\ \lambda \in \mathcal{G}$$

Y así la afirmación está demostrada.

Consideremos ahora los elementos $\rho, \sigma, \tau \in \mathcal{G}$ fijos pero arbitrarios. Si calculamos

$$F^{\tau} = Y(\sigma,\tau)^{-1} F^{\sigma} Y(\sigma,\tau) = Y(\sigma,\tau)^{-1} Y(\rho,\sigma)^{-1} F^{\rho} Y(\rho,\sigma) Y(\sigma,\tau)$$

y por otro lado se tiene

$$F^{\tau} = Y(\rho,\tau)^{-1} F^{\rho} Y(\rho,\tau)$$

obtenemos

$$Y(\rho,\tau)^{-1} F^{\rho} Y(\rho,\tau) = Y(\sigma,\tau)^{-1} Y(\rho,\sigma)^{-1} F^{\rho} Y(\rho,\sigma) Y(\sigma,\tau)$$

Por el corolario de la proposición 4 esto significa que $Y(\rho,\sigma)Y(\sigma,\tau)$ difiere de $Y(\rho,\tau)$ es un factor escalar $f(\rho,\sigma,\tau)$

$$Y(\rho,\sigma)Y(\sigma,\tau) = f(\rho,\sigma,\tau)Y(\rho,\tau)$$

Para demostrar la fórmula (A) calculamos para todo $\nu, \rho, \sigma, \tau \in \mathcal{H}$

$$\begin{aligned} f(\rho,\sigma,\tau) f(\nu,\rho,\tau) Y(\nu,\tau) &= f(\rho,\sigma,\tau) Y(\nu,\rho) Y(\rho,\tau) \\ &= Y(\nu,\rho) f(\rho,\sigma,\tau) Y(\rho,\tau) \\ &= Y(\nu,\rho) Y(\rho,\sigma) Y(\sigma,\tau) \\ &= f(\nu,\rho,\sigma) Y(\nu,\sigma) Y(\sigma,\tau) \\ &= f(\nu,\sigma,\tau) f(\nu,\rho,\sigma) Y(\nu,\tau) \end{aligned}$$

$$\therefore \qquad f(\rho.\sigma,\tau) f(\nu,\rho,\tau) = f(\nu,\sigma,\tau) f(\nu,\rho,\sigma)$$

**Corolario:** *Mismas hipótesis y notación del teorema 2. Si* $K'/K$, $\mathcal{G} = Gal(K'_{sep}/K)$.

*Sea*

$$\tilde{\rho}: \mathcal{G}' \to \mathcal{G}$$

*el homomorfismo restricción y sea*

$$F_{K'} = A_{L'} \to \mathcal{M}_n(L')$$

*la extensión $K'$-lineal de $F$ a $A_{K'}$. Entonces $Y \circ \tilde{\rho}$ y $f \circ \tilde{\rho}$ están relacionado a $F_{K'}$ de la misma manera que $Y$ y $f$ están relacionados con $F$.*

*Demostración:* Como $\mathcal{H} \subset \mathcal{G}$ y como se sabe que $\tilde{\rho}$ es sobre y continuo $\mathcal{H}' = \tilde{\rho}^{-1}(\mathcal{H})$ es un subgrupo abierto de $\mathcal{G}'$: $\mathcal{H}' \subset \mathcal{G}'$ entonces su correspondiente subcampo $L'$ del campo $K'_{\text{sep}}$: $L' \subset K'_{\text{sep}}$ es el subcampo generado por $L$ sobre $K'$.

Como $A_{K'} = A \otimes_K K'$ y $\mathcal{M}_n(L) \otimes_k K' = \mathcal{M}_n(L')$ entonces $F$ (del teorema 2) induce la extensión $K'$-lineal

$$F_{K'}: A_{K'} \cong \mathcal{M}_n(L')$$

La hipótesis sobre $F$ implica que $F_{K'}$ es una $L'$-representación.

Se afirma que

$$Y' = Y \circ \tilde{\rho}: \mathcal{G}' \times \mathcal{G}' \to \mathcal{M}_n(K'_{\text{sep}})$$

definida por la correspondecia

$$(\rho, \sigma) \longmapsto Y'(\rho, \sigma) = Y \circ \tilde{\rho}(\rho, \sigma) = Y(\tilde{\rho}(\rho, \sigma))$$

satisface los requerimientos del teorema 2.

En efecto, calculando para $\rho, \sigma, \tau \in \mathcal{G}' \implies \tilde{\rho}\rho$ y $\tilde{\rho}\sigma \in \mathcal{G}$

$$\begin{aligned} F^{\tilde{\rho}\sigma} &= Y(\tilde{\rho}\rho, \tilde{\rho}\sigma)^{-1} F^{\tilde{\rho}\rho} Y(\tilde{\rho}\rho, \tilde{\rho}\sigma) \\ &= Y \circ \tilde{\rho}(\rho, \sigma)^{-1} F^{\tilde{\rho}\rho} Y \circ \tilde{\rho}(\rho, \sigma) \\ &= Y'(\rho, \sigma)^{-1} F^{\tilde{\rho}\rho} Y'(\rho, \sigma) \end{aligned}$$

En seguida se extiende $K'$-linealmente este mapeo y se obtiene

$$F^{\sigma}_{K'} = Y'(\rho, \sigma)^{-1} F^{\rho}_{K'} Y'(\rho, \sigma) \qquad \forall \rho, \sigma \in \mathcal{G}'$$

calculando para todo $\rho, \sigma, \tau \in \mathcal{G}'$

$$\begin{aligned} Y'(\rho, \sigma) \cdot Y'(\sigma, \tau) &= Y(\tilde{\rho}\rho, \tilde{\rho}\sigma) Y(\tilde{\rho}\sigma, \tilde{\rho}\tau) \\ &= f(\tilde{\rho}\rho, \tilde{\rho}\sigma, \tilde{\rho}\tau) Y(\tilde{\rho}\rho, \tilde{\rho}\tau) \\ &= f \circ \tilde{\rho}(\rho, \sigma, \tau) Y'(\rho, \sigma) \end{aligned}$$

obtenemos

$$Y'(\rho,\sigma)\cdot Y'(\sigma,\tau) = f'(\rho,\sigma,\tau) = f\circ\tilde{\rho}(\rho,\sigma,\tau)$$

para todo $\rho,\sigma,\tau \in \mathcal{G}'$ se tiene $\rho' = f\circ\tilde{\rho}$ por lo tanto $f'(\rho,\sigma,\tau)Y'(\rho,\tau) = Y'(\rho,\sigma)Y'(\sigma,\tau) \quad \forall\rho,\sigma,\tau \in \mathcal{G}'$ para la fórmula (A) calculamos

$$\begin{aligned} f'(\rho,\sigma,\tau)f'(\nu,\rho,\tau) &= f\cdot\tilde{\rho}(\rho,\sigma,\tau)f\cdot\tilde{\rho}(\nu,\rho,\tau) \\ &= f(\tilde{\rho}\rho,\tilde{\rho}\sigma,\tilde{\rho}\tau)f(\tilde{\rho}\nu,\tilde{\rho}\rho,\tilde{\rho}\tau) \\ &= f(\tilde{\rho}\nu,\tilde{\rho}\sigma,\tilde{\rho}\tau)f(\tilde{\rho}\nu,\tilde{\rho}\rho,\tilde{\rho}\sigma) \\ &= f\cdot\tilde{\rho}(\nu,\sigma,\tau)f\cdot\tilde{\rho}(\nu,\rho,\sigma) \\ &= f'(\nu,\sigma,\tau)f'(\nu,\rho,\sigma) \\ &= f'(\nu,\sigma,\tau)f'(\nu,\rho,\tau) \end{aligned}$$

así se cumple la fórmula (A) y el corolario.

**Definición.** Sea $f$ un mapeo covariante de $\mathcal{G}\times\mathcal{G}\times\mathcal{G}$ en $K^{\times}_{\text{sep}}$. Se dirá que $f$ es un conjunto factorial si satisface la siguiente condición

$$(A) \qquad f(\rho,\sigma,\tau)f(\nu,\rho,\tau) = f(\nu,\sigma,\tau)f(\nu\rho,\sigma) \qquad \forall\rho,\sigma,\tau\in\mathcal{G}$$

*Afirmación:* La clase de los conjuntos factoriales lo constituyen un grupo multiplicativo que se denotará $\mathcal{H}(K)$.

$\mathcal{H}(K) = \{f: \mathcal{G}^{(3)} \to K^{\times}_{\text{sep}} \mid$ i) $f$ es covariante ii) $f$ es un conjunto factorial$\}$

En efecto, si $f_1, f_2 \in \mathcal{H}(K)$. Calculando

$$f_1f_2(\rho,\sigma,\tau) = f_1(\rho,\sigma,\tau)f_2(\rho,\sigma,\tau)$$

este producto así definido es covariante y como $f_i$ satisface la igualdad (A) podemos escribir

$$\begin{aligned} &f_1f_2(\rho,\sigma,\tau)f_1f_2(\nu,\rho,\tau) = \\ &= f_1(\rho,\sigma,\tau)f_2(\rho,\sigma,\tau)f_1(\nu,\rho,\tau)f_2(\nu,\rho,\tau) \\ &= f_1(\rho,\sigma,\tau)f_1(\nu,\rho,\tau)f_2(\rho,\sigma,\tau)f_2(\nu,\rho,\tau) \\ &= f_1(\nu,\sigma,\tau)f_1(\nu,\rho,\sigma)f_2(\nu,\sigma,\tau)f_2(\nu,\rho,\sigma) \end{aligned}$$

$$\begin{aligned} &= f_1(\nu,\sigma,\tau)f_2(\nu,\sigma,\tau)f_1(\nu,\sigma,\tau)f_2(\nu,\rho,\sigma) \\ &= f_1 f_2(\nu,\sigma,\tau)f_1 f_2(\nu,\sigma,\tau) \end{aligned}$$

obtenemos

$$f_1 f_2(\rho,\sigma,\tau)f_1 f_2(\nu,\rho,\tau) = f_1 f_2(\nu,\sigma,\tau)f_1 f_2(\nu,\sigma,\tau)$$

esto demuestra que $f_1 f_2 \in \mathcal{H}(K)$, es decir, $\mathcal{H}(K)$ es un grupo.

**Lema.** *Sea $z$ un mapeo covariante*

$$z: \mathcal{G} \times \mathcal{G} \to K_{sep}^{\times}$$

*definido por la correspondencia*

$$(\rho,\sigma) \longmapsto z(\rho,\sigma)$$

*entonces el mapeo $f$ de $\mathcal{G} \times \mathcal{G} \times \mathcal{G}$ en $K_{sep}^{\times}$*

$$f: \mathcal{G} \times \mathcal{G} \times \mathcal{G} \longmapsto K_{sep}^{\times}$$

*definido por la correspondencia*

$$(\rho,\sigma,\tau) \longmapsto f(\rho,\sigma,\tau) = z(\rho,\sigma)z(\sigma,\tau)z(\rho,\tau)^{-1}$$

*es un conjunto factor.*

*Demostración:* Es evidente que $f$ es covariante, puesto que $z$ lo es, calculando:

$$f(\rho,\sigma,\tau)f(\nu,\rho,\tau) = z(\rho,\sigma)z(\sigma,\tau)z(\rho,\tau)^{-1}z(\nu,\rho)z(\rho,\tau)z(\nu,\tau)^{-1}$$

obtenemos

$$f(\rho,\sigma,\tau)f(\nu,\rho,\tau) = z(\rho,\sigma)z(\sigma,\tau)z(\nu,\rho)z(\nu,\tau)^{-1}$$

análogamente

$$\begin{aligned} f(\nu,\sigma,\tau)f(\nu,\rho,\sigma) &= z(\nu,\sigma)z(\sigma,\tau)z(\nu,\tau)^{-1} \cdot \\ &\quad \cdot z(\nu,\rho)z(\rho,\sigma)z(\nu,\sigma)^{-1} \\ &= z(\rho,\sigma)z(\sigma,\tau)z(\nu,\rho)z(\nu,\tau)^{-1} \end{aligned}$$

por consiguiente $f$ satisface (A).

**Definición:** Si $z$ es un mapeo covariante de $\mathcal{G} \times \mathcal{G}$ a $K_{\text{sep}}^{\times}$:

$$z: \mathcal{G} \times \mathcal{G} \longmapsto K_{\text{sep}}$$

al conjunto factorial $f$ determinado por el lema se llama la cofrontera de $z$ y se escribirá

$$f = \delta z$$

(también se le llama conjunto factorial trivial).

Se afirma que la familia de conjuntos factoriales que son cofronteras constituyen un subgrupo de grupo $\mathcal{H}(K)$ y se denotará

$$\xi(K): \xi(K) \subset \mathcal{H}(K)$$

En efecto, sean:

$$f_1 f_2 \in \xi(K), \qquad f_i = \delta z_i$$

Observemos en primer lugar que el mapeo

$$z_1 z_2: \mathcal{G} \times \mathcal{G} \longmapsto K_{\text{sep}}^{\times}$$

definido por la correspondencia

$$(\rho, \sigma) \longmapsto z_1 z_2(\rho, \sigma) = z_1(\rho, \sigma) z_2(\rho, \sigma)$$

es covariante. Calculando

$$\begin{aligned} f_1 f_2(\rho, \sigma, \tau) &= f_1(\rho, \sigma, \tau) f_2(\rho, \sigma, \tau) = \\ &= z_1(\rho, \sigma) z_1(\sigma, \tau) z_1(\rho, \tau)^{-1} z_2(\rho, \sigma) z_2(\sigma, \tau) z_2(\rho, \tau)^{-1} = \\ &= z_1(\rho, \sigma) z_2(\rho, \sigma) z_1(\sigma, \tau) z_2(\sigma, \tau) z_1(\rho, \tau)^{-1} z_2(\rho, \tau)^{-1} = \\ &\quad z_1 z_2(\rho, \sigma) z_1 z_2(\sigma, \tau) z_1 z_2(\rho, \tau)^{-1} \end{aligned}$$

obtenemos

$$f_1 f_2(\rho, \sigma, \tau) = z_1 z_2(\rho, \sigma) z_1 z_2(\sigma, \tau) z_1 z_2(\rho, \tau)^{-1}$$

Por el lema $f_1 f_2$ es un conjunto factorial por definición $f_1 f_2 = \delta(z_1 z_2)$ por consiguiente $\xi(K)$ es un subgrupo del grupo $\mathcal{H}(K)$

$$\xi(K) \subset \mathcal{H}(K)$$

El grupo cociente se denotará

$$H(K) = \mathcal{H}(K)/\xi(K)$$

Si $K'/K$ entonces se afirma que $\tilde{\rho}$ el mapeo de restricción induce un mapeo

$$\rho^*: H(K) \to H(K')$$

Para definir el mapeo $\tilde{\rho}$ es suficiente definir la aplicación

$$\tilde{\rho}^{\#}: \mathcal{H}(K') \to \xi(K')$$

ésta se define por la correspondencia

$$f \longmapsto f \circ \tilde{\rho}$$

donde $f = \delta z$.

Calculando para $\rho, \sigma, \tau \in \mathcal{G}'$

$$\begin{aligned} f \circ \tilde{\rho}(\rho, \sigma, \tau) &= f(\tilde{\rho}\rho, \tilde{\rho}\sigma, \tilde{\rho}\tau) = \\ &= z(\tilde{\rho}\rho, \tilde{\rho}\sigma) z(\tilde{\rho}\sigma, \tilde{\rho}\tau) z(\tilde{\rho}\rho, \tilde{\rho}\tau)^{-1} = \\ &= z\tilde{\rho}(\rho, \sigma) z\tilde{\rho}(\sigma, \tau) z\tilde{\rho}(\rho, \tau)^{-1} \end{aligned}$$

se obtiene

$$f \circ \tilde{\rho} = \delta z \tilde{\rho}$$

y de acuerdo con el lema

$$f \circ \tilde{\rho} \in \xi(K')$$

Es decir, la aplicación $\tilde{\rho}^{\#}$ está bien definida, por tanto pasando al cociente se obtiene $\overline{\tilde{\rho}}^{\#}$.

Se dirá que el conjunto factorial $f$ del teorema 2 pertenece al álgebra $A$ y a las clases residuales módulo $\mathcal{H}(K)$ de $H(K)$ se les llamará *Clases Factoriales* mod $\xi(K)$.

**Proposición 7.** *Sea $A$ un álgebra simple sobre $K$. Entonces la clase de conjuntos factoriales pertenecientes al álgebra $A$ constituyen una clase residual de $\mathcal{H}(K)$ mod$\xi(K)$.*

*Demostración:* Observemos que $f, f' \in \mathcal{H}(K)$ se dirá que

$$f \sim f' \iff ff'^{-1} = \delta z$$

Sea $\mathcal{H}, L, F, Y$ y $f$ como en el teorema 2

$$F: A \to \mathcal{M}_n(L)$$

una $L$-representación de $A$, sea

$$z: \mathcal{G} \times \mathcal{G} \to K_{\text{sep}}^{\times}$$

un mapeo covariante arbitrario. Sea $\mathcal{H}'$ un subgrupo de $\mathcal{H}$: $\mathcal{H}' \subset \mathcal{H}$ de tal suerte que $z$ sea $\mathcal{H}'$-regular y sea $L'$ su subgrupo correspondiente de $K_{\text{sep}}$. $L' \supset L$.

Esto último implica que

$$F: A \to \mathcal{M}_n(L')$$

es una $L$-representación de $A$.

Ahora consideremos la aplicación

$$Y': \mathcal{G} \times \mathcal{G} \to \mathcal{M}_n(K_{\text{sep}})^{\times}$$

definida por la correspondencia

$$\begin{aligned}(\rho, \sigma) \longmapsto Y'(\rho, \sigma) &= zY(\rho, \sigma) \\ &= z(\rho, \sigma)Y(\rho, \sigma)\end{aligned}$$

lo cual es claramente covariante y $\mathcal{H}'$-regular.

Se afirma que

$$f'(\rho,\sigma,\tau)Y'(\rho,\tau) = Y'(\rho,\sigma)Y'(\sigma,\tau) \qquad \forall \rho,\sigma,\tau \in \mathcal{G}$$

Calculando:

$$\begin{aligned} Y'(\rho,\sigma)Y'(\sigma,\tau) &= z(\rho,\sigma)Y(\rho,\sigma)z(\sigma,\tau)Y(\sigma,\tau) \\ &= z(\rho,\sigma)z(\sigma,\tau)z(\rho,\tau)^{-1}z(\rho,\tau)Y(\rho,\sigma)Y(\sigma,\tau) \\ &= f_0(\rho,\sigma,\tau)z(\rho,\tau)f(\rho,\sigma,\tau)Y(\rho,\tau) \\ &= f_0(\rho,\sigma,\tau)f(\rho,\sigma,\tau)Y'(\rho,\tau) \end{aligned}$$

obtenemos

$$f_0(\rho,\sigma,\tau)f(\rho,\sigma,\tau)Y'(\rho,\tau) = Y'(\rho,\sigma)Y'(\sigma,\tau)$$

Tomando $f' = f_0 f$ se tiene la afirmación.

Lo anterior significa que si $f$ es un conjunto factorial perteneciente a $A$ entonces todo conjunto factorial $f'$ que se derive de $f$, está en la misma clase factorial

$$f \sim f' \iff f'f^{-1} = \delta z$$

Dado otro sistema $\mathcal{H}'$, $L'$, $F'$, $Y'$ y $f'$ pertenecientes al álgebra $A$ definida por el teorema 2 entonces

$$f \sim f' \iff f'f^{-1} = \delta z$$

donde $f$ pertenece a $A$; es decir $\mathcal{H}, L, F, Y$, y $f$ pertencen al álgebra $A$.

Consideremos

$$\mathcal{H}'' = \mathcal{H}' \cap \mathcal{H}$$

y sea $L''$ su correspondiente subgrupo de $\mathcal{G}$, el cual es el compositum de los campos $L$ y $L'$: $L'' = L(L') \qquad L'' \supset L,\ L'' \supset L'$

Como todo sucede en $K_{\text{sep}}$ el conjunto de los $L''$-representaciones de $A$ no es vacío.

Por tanto, si $F$ y $F'$ son dos $L''$-representaciones del álgebra $A$, existe un elemento $Z \in \mathcal{M}_n(L'')^z$ tal que

$$F' = Z^{-1}FZ$$

En seguida se define el mapeo

$$W: \mathcal{G} \times \mathcal{G} \to K_{\text{sep}}$$

definido por la correspondencia

$$(\rho, \sigma) \mapsto W(\rho, \sigma) = (z^\rho)^{-1} Y(\rho, \sigma) z^\rho$$

*Afirmación:* $F'^\sigma = W^{-1} F'^\rho W$

Calculando; utilizando el teorema 2, reemplazando $F'^\rho$ y $F^\rho$:

$$\begin{aligned}
&W^{-1}(\rho,\sigma) F'^\rho W(\rho,\sigma) = \\
&= \left((Z^\rho)^{-1} Y(\rho,\sigma) Z^\sigma\right)^{-1} F'^\rho (Z^\rho)^{-1} Y(\rho,\sigma) Z^\sigma \\
&= (Z^\sigma)^{-1} Y^{-1}(\rho,\sigma) Z^\rho F'^\rho (Z^\rho)^{-1} Y(\rho,\sigma) Z^\sigma \\
&= (Z^\sigma)^{-1} Y^{-1}(\rho,\sigma) Z^\rho (z^\rho)^{-1} F^\rho Z^\rho (Z^\rho)^{-1} Y(\rho,\sigma) Z^\sigma \\
&= (Z^\sigma)^{-1} Y^{-1}(\rho,\sigma) F^\rho Y(\rho,\sigma)^{-1} Y(\rho,\sigma) Z^\sigma \\
&= (Z^\sigma)^{-1} F^\sigma Z^\sigma \\
&= (Z^{-1} F Z)^\sigma \\
&= F'^\sigma
\end{aligned}$$

obtenemos

$W^{-1}(\rho,\sigma) F'^\rho W(\rho,\sigma) = F'^\sigma$ para todo $\rho, \sigma \in \mathcal{H}$ es decir

$$F' = W^{-1} F'^\rho W$$

En resúmen, dados $F$ y $F'$ el corolario de la proposición 5 afirma que $Y'$ es único salvo por un factor constante en el centro $L''^x$ de $\mathcal{M}_n(L'')^x$, es decir

$$Y'(\rho,\sigma) = z(\rho,\sigma) W(\rho,\sigma)$$

para todo $\rho, \sigma \in \mathcal{G}$. Esto implica que el mapeo

$$z: \mathcal{G} \times \mathcal{G} \to K_{\text{sep}}^x$$

es covariante y $\mathcal{H}''$-regular.

Calculando y aplicando el teorema 2

$$\begin{aligned} Y'(\rho,\sigma)Y'(\sigma,\tau) &= z(\rho,\sigma)W(\rho,\sigma)z(\sigma,\tau)W(\sigma,\tau) \\ &= z(\rho,\sigma)z(\sigma,\tau)W(\rho,\sigma)W(\sigma,\tau) \\ &= z(\rho,\sigma)z(\sigma,\tau)(z^{\rho})^{-1}Y(\rho,\sigma)z^{\sigma}(z^{\sigma})^{-1}Y(\sigma,\tau)z^{\tau} \\ &= z(\rho,\sigma)z(\sigma,\tau)(z^{\rho})^{-1}Y(\rho,\sigma)Y(\sigma,\tau)z^{\tau} \\ &= z(\rho,\sigma)z(\sigma,\tau)f(\rho,\sigma,\tau)(z^{\rho})^{-1}Y(\rho,\tau)z^{\tau} \\ &= z(\rho,\sigma)z(\sigma,\tau)f(\rho,\sigma,\tau)W(\rho,\tau) \\ &= z(\rho,\sigma)z(\sigma,\tau)z(\rho,\tau)^{-1}f(\rho,\sigma,\tau)z(\rho,\tau)W(\rho,\tau) \\ &= \delta zf(\rho,\sigma,\tau)Y'(\rho,\tau) \end{aligned}$$

Obtenemos

$$\delta zf(\rho,\sigma,\tau)Y'(\rho,\tau) = Y'(\rho,\sigma)Y'(\sigma,\tau)$$

Si definimos $f'(\rho,\sigma,\tau) = \delta zf(\rho,\sigma,\tau)$ entonces

$$f'(\rho,\sigma,\tau)Y'(\rho,\sigma) = Y'(\rho,\sigma)Y'(\sigma,\tau)$$

$\forall\ \rho,\sigma,\tau \in \mathcal{G}$ es decir

$$f' = \delta zf$$

$$f'f^{-1} = \delta z \iff f' \sim f$$

Por lo tanto, una clase residual está compuesta de todos los conjuntos factoriales.

**Corolario.** *Sea $K'$ un campo que contiene a $K$: $K'/K$ entonces una clase factorial determinante por el álgebra simple*

$$A_{K'} = A \otimes_K K'$$

*definida sobre $K'$, es la imágen de la clase factorial determinada por el álgebra simple $A$ sobre $K$ bajo el mapeo $\tilde{\rho}^{\#}$:*

$$\tilde{\rho}^{\#}: H(K') \to H(K)$$

*definido por la correspondencia*

$$\{f\} \to \tilde{\rho}^{\#}\{f\} = \{f \circ \tilde{\rho}\}$$

**Definición.** Se dirá que una clase factorial de $K$ formada por los conjuntos factoriales pertenecientes al álgebra simple $A$ sobre $K$, **pertenece** al álgebra o está *asociada* al álgebra $A$.

**Teorema.** *La aplicación*

$$\Psi: B(K) \to \mathbf{H}(K)$$

*definida por la correspondencia*

$$\{A\}_B \longmapsto \psi(\{A\}_B) = \{A\}_{Fac}$$

*es un isomorfismo. (Donde* $\{A\}_B$ *es un elemento arbitrario del Grupo de Brauer:* $\{A\}_B \subset B(\overline{K})$ *y* $\{A\}_{Fac}$ *es la clase factorial de la perteneciente al álgebra A).*

*Demostración:* En primer lugar se demuestra que $\psi$ es un homomorfismo. Para este próposito se consideran las álgebras simples sobre $K$, $A$ y $A'$ de $\dim_K A = n^2$, $\dim_K A = n'^2$.

Sean

$$L, F, Y \text{ y } f$$

los objetos asociados con $A$ como lo establece el teorema 2.

Sea $L''$ el compositum de $L$ y $L'$: $L'' = L(L')$ y observemos que

$$\mathcal{M}_n(L'') \times \mathcal{M}_{n'}(L'') = \mathcal{M}_{nn'}(L'').$$

En seguida se define el álgebra simplde sobe $K$

$$A'' = A \otimes_K A'$$

y el mapeo

$$F'' = F \otimes_K F'$$

como $F$ y $F'$ son $L''$-representaciones de $A$ se obtiene que el mapeo

$$Y'' : \mathcal{G} \times \mathcal{G} \to \mathcal{M}_{nn'}(K_{\text{sep}})$$

definido por la correspondencia

$$(\rho, \sigma) \longmapsto Y''(\rho, \sigma) = Y(\rho, \sigma) \otimes Y'(\rho, \sigma)$$

satisface los requerimientos del teorema 2.

En efecto, calculando

$$\begin{aligned} Y''(\rho,\sigma)Y''(\sigma,\tau) &= Y(\rho,\sigma) \otimes Y'(\rho,\sigma)Y(\sigma,\tau) \otimes Y'(\sigma,\tau) = \\ &= Y(\rho,\sigma)Y(\sigma,\tau) \otimes Y'(\rho,\sigma)Y'(\sigma,\tau) = \\ &= f(\rho,\sigma,\tau)Y(\rho,\tau) \otimes f'(\rho,\sigma,\tau)Y'(\rho,\tau) = \\ &= ff'(\rho,\sigma,\tau)Y(\rho,\tau) \otimes Y'(\rho,\tau) = \\ &= f''Y''(\rho,\tau) = \\ f''(\rho,\sigma,\tau)Y''(\rho,\tau) &= Y''(\rho,\sigma)Y''(\sigma,\tau) \end{aligned}$$

para toda $\rho, \sigma, \tau \in \mathcal{G}$ donde $f'' = f \cdot f'$. Además se satisfacen las propiedades

(i) $F''^{\rho} = Y''(\rho,\sigma)^{-1} F''^{\sigma} Y''(\rho,\sigma)$ para toda $\rho, \sigma \in \mathcal{G}$

(ii) $f''(\rho,\sigma,\tau) \cdot f''(\nu,\rho,\tau) = f'(\nu,\sigma,\tau) \cdot f''(\nu,\rho,\sigma)$

En efecto, calculando

$$\begin{aligned} Y''(\rho,\sigma)^{-1} F''^{\sigma} Y''(\rho,\tau) &= (Y''(\rho,\sigma))^{-1}(F \otimes F')^{\sigma} Y(\rho,\sigma) \otimes Y'(\rho,\sigma) = \\ &= (Y''(\rho,\sigma))^{-1}(F^{\sigma} \otimes F'^{\sigma}) Y(\rho,\sigma) \otimes Y'(\rho,\sigma) = \\ &= (Y''(\rho,\sigma))^{-1} F^{\sigma} Y(\rho,\sigma) \otimes F'^{\sigma} Y'(\rho,\sigma) = \\ &= Y''(\rho,\sigma)^{-1}(Y(\rho,\sigma) \cdot F^{\rho} \otimes Y'(\rho,\sigma) F'^{\rho}) = \\ &= Y''(\rho,\sigma)^{-1}(Y(\rho,\sigma) \otimes \otimes Y'(\rho,\sigma))(F^{\rho}) \otimes F'^{\rho}) = \\ &= Y''(\rho,\sigma)^{-1} Y''(\rho,\sigma)(F \otimes F')^{\rho} = \\ &= F''^{\rho} \end{aligned}$$

y así se obtiene la afirmación para (i) calculando para obtener (ii)

$$f''(\rho,\sigma,\tau) f''(\nu,\rho,\tau) = f(\rho,\sigma,\tau) f'(\rho,\sigma,\tau) f(\nu,\rho,\tau) f'(\nu,\sigma,\tau) =$$

$$
\begin{aligned}
&= f(\rho,\sigma,\tau)f(\nu,\rho,\tau)f'(\rho,\sigma,\tau)f'(\nu,\rho,\tau) = \\
&= f(\nu,\sigma,\tau)f(\nu,\rho,\tau)f'(\nu,\sigma,\tau)f'(\nu,\rho,\sigma) = \\
&= f(\nu,\sigma,\tau)f'(\nu,\sigma,\tau)f(\nu,\rho,\sigma)f'(\nu,\rho,\sigma) = \\
&= f''(\nu,\sigma,\tau)f''(\nu,\rho,\sigma)
\end{aligned}
$$

resultando la afirmación para (ii).

Por lo tanto la clase factorial asociada al álgebra $A'' = A \otimes_K A'$ es el producto de las clases factoriales asociadas a las álgebras $A$ y $A'$ respectivamente.

$$
\begin{aligned}
\{f''\}_{\mathrm{Fac}} &= \{f\}_{\mathrm{Fac}}\{f'\}_{\mathrm{Fac}} \\
\Psi(\{A\}_B\{A'\}_B) &= \Psi(\{A\}_B)\Psi(\{A'\}_B)
\end{aligned}
$$

*Afirmación:* $\Psi(\{\mathcal{M}_n(K)\}) = \{1\}_{\mathrm{Fac}} \in \mathbf{H} = \mathcal{H}(K)/\xi(K)$

Consideremos el álgebra simple

$$A = \mathcal{M}_n(K)$$

el mapeo

$$F: A \to \mathcal{M}_n(K)$$

definido por la correspondencia

$$a \longmapsto F(a) = a$$

y el mapeo

$$Y: \mathcal{G} \times \mathcal{G} \to \mathcal{M}_n(K_{\mathrm{sep}})$$

definido por la correspondencia

$$(\rho,\sigma) \longmapsto Y(\rho,\sigma) = \mathrm{I}_n = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ & & \ddots \\ 0 & & 1 \end{pmatrix}$$

Como $f$ esta dada por la fórmula

$$f(\rho,\sigma,\tau)Y(\rho,\tau) = Y(\rho,\sigma)Y(\sigma,\tau) \qquad \forall\, \rho,\sigma,\tau \in \mathcal{G}$$

Esto implica que

$$f = 1$$

Para obtener en este caso

1. $F''$ asociada al álgebra

$$\begin{aligned} A'' &= A \otimes_K A' = \mathcal{M}_n(K) \otimes_K A' \\ A'' &= \mathcal{M}_n(A') \end{aligned}$$

Sabemos $f'' = f \cdot f' = 1 \cdot f' = f' \Rightarrow \{f''\} = \{f'\}$ es decir la clase factorial asociada a

$$A''$$

es la misma que la clase factorial asociada a

$$A'$$

Es decir, se demostró que $\Psi$ es homomorfismo, ahora se demostrará que es biyectivo.

**Lema 3.** *Sea $\mathcal{H}$ un subgrupo abierto del grupo $\mathcal{G}$ y sea $L$ un subcampo de $K_{sep}$ correspondiente al grupo $\mathcal{H}$ y sea $Y$ un mapeo $\mathcal{H}$-regular y covariante de $\mathcal{G} \times \mathcal{G}$ en $\mathcal{M}_n(L)$*

$$Y: \mathcal{G} \times \mathcal{G} \to \mathcal{M}_n(L)$$

*definido por la correspondencia*

$$(\rho, \sigma) \longmapsto Y(\rho, \sigma)$$

*satisfaciendo la propiedad*

$$Y(\rho, \tau) = Y(\rho, \sigma)Y(\sigma, \tau) \quad \textit{para todo} \quad \rho, \sigma, \tau \in \mathcal{G}$$

*Entonces existe una matriz $Z \in \mathcal{M}_n(L)^x$ tal que*

$$Y(\rho, \sigma) = (Z^\rho)^{-1}(Z^\sigma)$$

*Demostración:* Sea

$$\alpha = \{\alpha_1, \ldots, \alpha_n\}$$

un sisema coompleto de representantes de las clases $\mathcal{H}\sigma \bmod \mathcal{H}$ del grupo $\mathcal{G}$. Sabemos que este sistema de representantes induce sobre $L$ todos los isomorfismos $K$-lineales de $L$ en $K_{\text{sep}}$ linealmente independientes sobre el campo $L$.

Sean

$$\begin{aligned} \mathcal{M}_{1,n}(L) &= \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in L\} \\ \mathcal{M}_{n,1}(L) &= \left\{ \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \mid b_1, \ldots, b_n \in L \right\} \end{aligned}$$

y consideremos las aplicaciones

$$\mathcal{M}_{1,n}(L) \times \mathcal{M}_n(L) \to \mathcal{M}_{1,n}(L)$$

definida por la correspondencia

$$((a_1, \ldots, a_n), (b_{ij})) \longmapsto \left( \sum_i a_i b_{ij} \right)$$

$$\mathcal{M}_n(L) \times \mathcal{M}_{n,1}(L) \longmapsto \mathcal{M}_{n,1}(L)$$

definida por la correspondencia

$$(a_{ij}) \times \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \longmapsto \begin{pmatrix} \sum a_{i_1} b_1 \\ \vdots \\ \sum a_{i_n} b_n \end{pmatrix}$$

Consideremos la aplicación

$$\varphi: \mathcal{M}_{1,n}(L) \to \mathcal{M}_{1,n}(L)$$

definida por la correspondencia

$$u \longmapsto \varphi(u) = \sum_i u^{\alpha i} Y(\alpha_i, \epsilon)$$

se afirma que esta aplicación así definia está bien definida. En efecto, es suficiente demostrar que $\varphi(u) = z$ es invariante bajo la acción del grupo $\mathcal{H}$: $z^\rho = z$ para todo $\rho \in \mathcal{H}$ lo cual se demuestra observando que el sistema

$$\alpha\rho = (\alpha_1\rho, \ldots, \alpha_n\rho)$$

es otro sistema de representantes de las clases $\mathcal{H}\alpha \bmod \mathcal{H}$ en $\mathcal{G}$ puesto que si $i \neq j$

$$\alpha_i\rho(\alpha_j\rho)^{-1} \in \mathcal{H} \Rightarrow \alpha_i\alpha_j^{-1} \in \mathcal{H}.$$

Esta contradicción demuestra que efectivamente $\alpha\rho$ es otro sistema de representantes. Calculando para todo $\rho \in \mathcal{H}$

$$\begin{aligned} z^p &= \sum_i u^{\alpha_i\rho} Y^\rho(\alpha_i, \epsilon) = \sum u^{\alpha_i\rho} Y(\alpha_i\rho, \epsilon\rho) \\ &= \sum u^{\alpha_i\rho}(\alpha_i\rho, \epsilon) \\ &= z \end{aligned}$$

obtenemos

$$z^p = z \qquad \text{para todo} \qquad \rho \in \mathcal{H}$$

Se afirma que esta aplicación así definida está bien definida. A continuación se demuestra la

*Afirmación:* Existen $n$ vectores en $\mathcal{M}_{1,n}$:

$$u_1, \ldots, u_n \in \mathcal{M}_{1,n}$$

cuyas imágenes bajo el mapeo $\varphi$:

$$\varphi(u_1), \ldots, \varphi(u_n) \in \mathcal{M}_{1,n}$$

son linealmente independientes sobre $L$.

En efecto, supongamos por un instante que esto no sucede, en particular esta situación debe darse para la base canónica del espacio vectorial $\mathcal{M}_{1,n}(L)$:

$$e_1e_2, \ldots, e_n \in \mathcal{M}_{1,n}(L)$$

es decir, existe una relación no trivial

$$\varphi(e_1)\tilde{\ell}_1 + \cdots + \varphi(e_n)\tilde{\ell}_n = 0 \quad \text{con} \quad \tilde{\ell}_1, \ldots, \tilde{\ell}_n \in L$$

Si ahora calculamos

$$\begin{aligned} 0 &= \sum_i \varphi(e_i)\tilde{\ell}_i \\ &= \sum_i \left( \sum_j \ell_{ij} e_j \right) \tilde{\ell}_j \\ &= \sum_j \left( \sum_i \ell_{ij} \tilde{\ell}_j \right) e_j \end{aligned}$$

obtenemos

$$\begin{aligned} \sum_j \left( \sum_i \ell_{ij} \tilde{\ell}_j \right) e_j &= 0 \qquad (4) \\ &\Rightarrow \sum_j \ell_{ij} \tilde{\ell}_j = 0 \\ &\quad (1 \leq j \leq n) \end{aligned}$$

Por otro lado, si $u \in \mathcal{M}_{1,n}$ es un vector fijo pero arbitrario y si calculamos

$$\begin{aligned} \varphi(u) &= \varphi\left( \sum \ell'_i e_i \right) \\ &= \sum_i \ell'_i \varphi(e_i) \\ &= \sum \ell'_i \left( \ell_{ij} e_j \right) \\ &= \sum_i \sum_j \ell'_i \ell_{ij} e_j \\ &= \sum_j \left( \sum_i \ell'_i \ell_{ij} \right) e_j \end{aligned}$$

obtenemos

$$\begin{aligned} \varphi(u) &= \sum_j \left( \sum_i \ell'_j \ell_{ij} \right) e_j \\ &= \left( \sum_i \ell'_i \ell_{ij}, \ldots, \sum_i \ell'_i \ell_{in} \right) \end{aligned}$$

o sea $\varphi(u) = \left(\sum_i \ell_i' \ell_{i1}, \ldots, \sum_i \ell_i' \ell_{in}\right)$

Ahora multipliquemos este vector por la derecha por el vector

$$v = \begin{pmatrix} \tilde{\ell}_1 \\ \vdots \\ \tilde{\ell}_n \end{pmatrix} \in \mathcal{M}_{n,1}(L), \quad v \neq 0$$

$$\begin{aligned} \varphi(u) \cdot v &= \sum_i' \ell_i' \ell_{i1} \tilde{\ell}_1 + \cdots + \sum_i \ell_i' \ell_{in} \tilde{\ell}_n \\ &= \sum_j \sum_i \ell_i' \ell_{ij} \tilde{\ell}_j \\ &= \sum_i \ell_i' \left(\sum \ell_{ij} \tilde{\ell}_j\right) \end{aligned}$$

Si ahora utilizamos la relación (4) obtenemos

$$\varphi(u) \cdot v = 0$$

Ahora veremos que $v = 0$.

$${}^t v \, {}^t\varphi(u) = 0$$

Calculando

$$\begin{aligned} 0 &= {}^t v \, {}^t\varphi(u) = \\ &= {}^t v \, {}^t\left(\sum u^{\alpha_i} Y(\alpha_i, \epsilon)\right) = \\ &= {}^t v \sum_i {}^t Y(\alpha_i, \epsilon) \, {}^t u^{\alpha_1} = \\ &= \sum_i {}^t v \, {}^t Y(\alpha_i, \epsilon) \alpha_i \, {}^t u \end{aligned}$$

Obtenemos

$$\left(\sum_i {}^t v \, {}^t Y(\alpha_i, \epsilon) \alpha_i\right) {}^t u = 0$$

Como $u$ se eligió arbitrariamente en $\mathcal{M}_{1,n}$ se obtiene

$$\sum_i {}^t v \, {}^t Y(\alpha_i, \epsilon) \alpha_i = 0$$

lo cual implica, por la independencia lineal de $\alpha_i$ en $L$, que $v\ {}^tY(\alpha_i,\epsilon)=0$ $(1\leq i\leq n)$

$$Y(\alpha_i,\epsilon)v=0 \qquad (1\leq i\leq n)$$

como $Y(\alpha_i,\epsilon)\in\mathcal{M}_n^{\times}(L)$ implica que $v=0$.

Esto último contradice la elección del vector $v=\begin{pmatrix}\tilde{\ell}_1\\ \vdots\\ \tilde{\ell}_n\end{pmatrix}\neq 0$. Y así la afirmación esta demostrada.

Sean $n$ vectores $u_1,\ldots,u_n\in\mathcal{M}_{1,n}(L)$ donde $u_i=\left(u_1^{(i)},\ldots,u_n^{(i)}\right)$ con $u_j^{(i)}\in L$ $(1\leq i\leq n)$ con la propiedad de la afirmación. En seguida se define la mattriz

$$Z=\sum_i u^{\alpha_i}Y(\alpha_i,\epsilon)$$

donde

$$u=\begin{pmatrix}u_1^{(1)} & \cdots & u_n^{(1)}\\ & \vdots & \vdots\\ u_1^{(n)} & \cdots & u_n^{(n)}\end{pmatrix}$$

por tanto, para obtener la matriz

$$u^{\alpha}Y(\alpha_i,\epsilon)$$

se multiplica la matriz $Y(\alpha_i,\epsilon)$ por la izquierda por el vector

$$\sum_{i=1}^{n}\begin{pmatrix}u_1^{\alpha_i}Y(\alpha_i,\epsilon)\\ u_2^{\alpha_i}Y(\alpha_i,\epsilon)\\ \vdots\\ u_n^{\alpha_i}Y(\alpha_i,\epsilon)\end{pmatrix}=\sum_i u^{\alpha_i}Y(\alpha_i,\epsilon)$$

Esto último implica

$$\begin{pmatrix}\sum_i u_1^{\alpha_i}Y(\alpha_i,\epsilon)\\ \vdots\\ \sum_i u_n^{\alpha_i}Y(\alpha_i,\epsilon)\end{pmatrix}=\sum_i u^{\alpha_i}Y(\alpha_i,\epsilon)$$

Por lo tanto $\sum_i u^{\alpha_i} Y(\alpha_i, \epsilon) = \begin{pmatrix} \varphi(u_1) \\ \vdots \\ \varphi(u_n) \end{pmatrix}$ donde cada hilera es linealmente independiente de acuerdo con la elección de los vectores $u_1, \ldots, u_n \in \mathcal{M}_{1,n}(L)$ la matriz

$$Z = \sum u^{\alpha_i} Y(\alpha_i, \epsilon) \quad \text{es invertible}$$

Calculando

$$\begin{aligned} Z^\rho Y(\rho, \sigma) &= \sum_i u^{\alpha_i \rho} Y^\rho(\alpha_i, \epsilon) Y(\rho, \sigma) = \\ &= \sum_i u^{\alpha_i} Y(\alpha_i, \rho) Y(\rho, \sigma) = \\ &= \sum_i u^{\alpha_i} Y(\alpha_i, \sigma) = \\ &= Z^\sigma \end{aligned}$$

Esto implica que

$$\begin{aligned} Z^\rho Y(\rho, \sigma) &= Z^\rho \\ \Rightarrow Y(\rho, \sigma) &= (Z^\rho)^{-1} Z^\sigma \end{aligned}$$

*Afirmación:* La aplicación

$$\Psi : B(K) \to \mathbf{H}(K)$$

definida por la correspondencia

$$\{A\}_B \longmapsto \mu(\{1\}) = \{A\}_{CF}$$

es una inyección. En efecto, supongamos que $\mu(\{A\}_B)$ es la clase factorial trivial de $A$ es decir

$$\mu(\{A\}_B) = \{\delta z\}_{CF}$$

donde $z$ es un mapeo covariante de $\mathcal{G} \times \mathcal{G}$ en $K^\times_{\text{sep}}$

$$z : \mathcal{G} \times \mathcal{G} \to K^\times_{\text{sep}}$$

definido por la correspondencia

$$(\rho,\sigma) \longmapsto z(\rho,\sigma)$$

y donde $\delta z$ es el mapeo covariante de $\mathcal{G}\times\mathcal{G}\times\mathcal{G}$ es $K_{\text{sep}}^{\times}$

$$\delta z\colon \mathcal{G}\times\mathcal{G}\times\mathcal{G} \to K_{\text{sep}}^{\times}$$

definida por la correspondencia

$$(\rho,\sigma,\tau) \longmapsto \delta z(\rho,\sigma,\tau) = z(\rho,\sigma)z(\sigma,\tau)z(\rho,\tau)^{-1}$$

es fácil ver que $z$ así definida es un conjunto factorial

$$f = \delta z$$

es decir, $f$ es la cofrontera de $z$.

La hipótesis implica que, de acuerdo con la proposición 7, se puede elegir $\mathcal{H}, L$ y $Y$ tal que $f = 1$ y como en general

$$f(\rho,\sigma,\tau)Y(\rho,\tau) = Y(\rho,\sigma)Y(\sigma,\tau)$$

entonces

$$Y(\rho,\sigma) = Y(\rho,\sigma)Y(\sigma,\tau)$$

esto último nos permite aplicar el lema 3; por tanto, existe una matriz $Z \in \mathcal{M}_n(L)^{\times}$ tal que

$$Y(\rho,\sigma) = (Z^{\rho})^{-1}Z^{\sigma}$$

Con esta matriz definimos la aplicación

$$F^{\prime} = ZFZ^{-1}$$

Calculando

$$\begin{aligned} F^{\prime\sigma} &= Z^{\sigma}F^{\sigma}(Z^{\sigma})^{-1} \\ &= Z^{\rho}Y(\rho,\sigma)F^{\sigma}Y(\rho,\sigma)^{-1}(Z^{\rho})^{-1} \\ &= Z^{\rho}F^{\sigma}(Z^{\rho})^{-1} \\ &= F^{\prime\rho} \end{aligned}$$

Obtenemos

$$F^{l\sigma} = F^{l\rho}$$

es decir

$$F^{l\sigma\rho^{-1}} = F^{l} \qquad \forall\, \rho, \sigma \in \mathcal{H}$$

Observemos

$$A_L \overset{F_L}{\cong} \mathcal{M}_n(L), \quad \therefore \mathcal{M}_n(L)^{\times} \overset{Z^{-1}}{\hookrightarrow} \mathcal{M}_n(L)^{\times}$$

$$\mathcal{M}_n(L) \overset{Z^{-1}}{\hookrightarrow} \mathcal{M}_n(L) \overset{F_1 Z^{-1}}{\hookrightarrow} \mathcal{M}_n \overset{Z}{\hookrightarrow} \mathcal{M}$$

$$F'_L = ZF_LZ^{-1}:$$

$$\mathcal{M}_n(L) \overset{F'_L}{\hookrightarrow} \mathcal{M}_n(L) \xrightarrow{F'_L=(F'_L)^{\sigma\rho^{-1}}} \mathcal{M}_n(L)$$

$$\Rightarrow\ F'_L: A_L \cong \mathcal{M}_n(K)\ \Rightarrow F': A \cong \mathcal{M}_n(K)$$

$$\Rightarrow\ F'_L: A \cong \mathcal{M}_n(K)$$

esto significa que $\Psi(\{A\}_B) = \{A\}_{CF} = \{\delta z\} = \{A\}_B$ es la clase trivial, $\therefore$ es inyectiva.

# Bibliografía

[1] *Basic Number Theory.* Andre Weil.

[2] *Algebra.* B. L. van der Waerden. Vol 2

[3] *Algebra.* P. M. Cohn. Second Edition. Vol. 3