Universitat de Barcelona
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

TEORÍA DE PSEUDO-REPRESENTACIONES Y REPRESENTACIONES ASOCIADAS

Autor: Paula Sarrado Cortadellas

Director: Dr. Luis V. Dieulefait
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 21 de junio de 2020

Abstract

We study in this work the concept of pseudo-representation and its relevance in the Theory of Representations. In particular, we work with pseudo-representations induced by representations of algebras; and we give the necessary conditions so that, given a pseudo-representation, we can build a representation associated with it.

Resumen

Estudiamos en este trabajo el concepto de pseudo-representación y su relevancia en la Teoría de Representaciones. En particular trabajamos las pseudo-representaciones inducidas por representaciones de álgebras; y damos las condiciones necesarias para que, dada una pseudo-representación, podamos construir una representación asociada a ella.

2010 Mathematics Subject Classification. 20C15, 16H05

Agradecimientos

Me gustaría agradecer, en primer lugar, a mi tutor, el Dr. Luis Dieulefait, que me propusiera este trabajo y la pasión que me transmitió por él desde el primer momento. También querría agradecer a mis amigos (a los de la facultad y a los de antes, a los que entienden lo que estudio y a los que no entienden ni porqué lo estudio) su presencia y acompañamiento a lo largo de toda la carrera. Ellos han hecho que sea (un poco) más fácil y sobre todo una experiencia inolvidable. Finalmente, me gustaría agradecer a mi familia, y en especial a mi madre, su apoyo incondicional y su paciencia.

Índice

1. Introducción

Cuando la estructura de un grupo es muy compleja o cuando el grupo es muy grande, habitualmente es más fácil estudiar representaciones de dicho grupo que el grupo en sí. Sin embargo, estudiar representaciones no es sencillo y es por ello que necesitamos caracterizarlas.

Es A. Wiles quien primero introduce en [16] el concepto de pseudo-representación de grado 2, y lo hace con la finalidad de estudiar las representaciones de grupos de Galois en casos en los que el uso directo de la geometría algebraica no es posible. Así pues, las pseudo-representaciones juegan un papel crucial en la construcción, utilizando congruencias entre formas modulares, de algunas representaciones p-ádicas de Galois. Será R.Taylor quien defina pseudo-representaciones de grado n y desarrolle su estudio.

Más adelante, R. Rouquier da en [13] una definición de pseudo-representación que se corresponde con una ligera modificación de la definición dada por Taylor en [15] y que nos permite además definir la noción de dimensión de una pseudo-representación. Trabajaremos pues en este proyecto con tal definición y nos centraremos en la relación entre pseudo-representaciones y representaciones con el objetivo de entender su aportación a la Teoría de Representaciones. Veremos, por ejemplo, que el caracter de una representación de dimensión n es una pseudo-representación de dimensión menor o igual a n.

Considerando álgebras sobre un cuerpo, estableceremos una biyección entre representaciones absolutamente irreducibles sobre un álgebra simple central y pseudo-representaciones absolutamente irreducibles; biyección que viene dada por la traza reducida.

Siendo A un anillo conmutativo, estudiaremos también las representaciones de una A-álgebra R en una A-álgebra de Azumaya Σ y daremos las condiciones necesarias para que una pseudo-representación sea el caracter de una representación de R en Σ. En particular demostraremos que si f es una pseudo-representación de R cuyas pseudo-representaciones residuales asociadas son absolutamente irreducibles y de dimensión igual a la de f entonces dicha pseudo-representación es el caracter de una representación de R en una cierta álgebra de Azumaya.

1.1. Estructura de la memoria

La memoria está estructurada en cinco secciones, la primera de las cuales aporta todas las definiciones y nociones necesarias en lo que a representaciones de grupos se refiere.

La segunda sección pretende introducir el concepto de pseudo-representación de igual forma en que surgió en el tiempo: primeramente la pseudo-representación de Wiles, de grado 2; y en segundo lugar la pseudo-representación de Taylor, de grado n.

En la tercera sección proporcionamos la definición de pseudo-representación dada por Rouquier, la que utilizaremos en el resto del trabajo; y mostramos algunas de sus propiedades.

A continuación, en la cuarta sección, tratamos las pseudo-representaciones inducidas por representaciones y vemos, como resultado principal, que la traza de una representación es una pseudo-representación.

Finalmente, y trabajando tanto con álgebras sobre un cuerpo como con álgebras sobre un anillo, damos las condiciones necesarias para construir una representación a partir de una pseudo-representación.

2. Preliminares sobre representaciones de grupos

2.1. Definiciones y nociones esenciales

Definición 2.1. *Dado un grupo G y un anillo conmutativo unitario A, una representación de grado n de G es un homomorfismo de grupos*

$$\rho : G \longrightarrow GL_n(A),$$

donde $GL_n(A)$ denota el grupo de matrices $n \times n$ invertibles con coeficientes en A. Diremos que A es el anillo de coeficientes de la representación.

Decimos que dos representaciones ρ y ρ' son *equivalentes* o *isomorfas* si existe algún $x \in GL_n(A)$ tal que $\rho(\sigma) = x\rho'(\sigma)x^{-1}$ para todo $\sigma \in G$. Si ρ y ρ' son equivalentes escribimos $\rho \sim \rho'$.

Sea $\rho : G \longrightarrow GL_n(A)$ una representación de un grupo finito G sobre un anillo conmutativo A, llamaremos *caracter* (o *traza*) asociado a ρ a la función

$$\begin{array}{rccc} \chi : & G & \longrightarrow & A \\ & \sigma & \longmapsto & \mathrm{Tr}(\rho(\sigma)) \end{array}$$

donde Tr denota la traza de las matrices cuadradas con coeficientes en A.

Los caracteres de las representaciones de G se denominan también caracteres de G.

Dos representaciones equivalentes determinan el mismo caracter. Además,

$$\begin{aligned} \chi(\sigma^{-1}\tau\sigma) = {} & \mathrm{Tr}(\rho(\sigma^{-1}\tau\sigma)) = \mathrm{Tr}(\rho(\sigma)^{-1}\rho(\tau)\rho(\sigma)) = \mathrm{Tr}(\rho(\sigma)\rho(\sigma)^{-1}\rho(\tau)) = \\ = {} & \mathrm{Tr}(I \cdot \rho(\tau)) = \mathrm{Tr}(\rho(\tau)) = \chi(\tau), \end{aligned}$$

es decir, los caracteres son constantes sobre las clases de conjugación.

Sea G un grupo finito y A un anillo conmutativo, llamaremos $A[G]$ al A-módulo libre de base G, en el que consideramos la estructura de A-álgebra determinada por el producto siguiente:

$$(\sum_{\sigma \in G} \alpha_\sigma \sigma)(\sum_{\tau \in G} \beta_\tau \tau) = \sum_{\sigma, \tau \in G} \alpha_\sigma \beta_\tau \sigma\tau$$

Este producto es bilineal y extiende el producto de G. Así pues, se puede comprobar que $A[G]$ es una A-álgebra, cuya unidad es el elemento neutro de G.

Si $\rho : G \longrightarrow GL_n(A)$ es una representación, podemos extender ρ a un único homomorfismo de A-álgebras $\rho : A[G] \longrightarrow M_n(A)$ de modo que el siguiente diagrama conmuta:

$$\begin{tikzcd} A[G] \arrow[r, "\rho"] & M_n(A) \\ G \arrow[u] \arrow[r, "\rho"] & GL_n(A) \arrow[u] \end{tikzcd}$$

2.2. Representaciones con coeficientes en un cuerpo

Hemos observado en la sección anterior que dos representaciones equivalentes tienen igual traza. A continuación expondremos el resultado recíproco bajo ciertas hipótesis. Dicho resultado se puede encontrar con todo detalle en [6].

Sea $\rho : G \longrightarrow GL_n(A)$ una representación de G, consideramos $V(\rho)$ el anillo A^n de vectores columna equipado con la G-acción definida como

$$\begin{array}{ccc} G \times V(\rho) & \longrightarrow & V(\rho) \\ (\sigma, v) & \longmapsto & \sigma v = \rho(\sigma)v \end{array}.$$

Supongamos ahora que $A = K$ es un cuerpo. Decimos que ρ es una representación *reducible* si $V(\rho)$ tiene un subespacio no trivial invariante por G. Una representación es *irreducible* si no es reducible.

Además, si $\overline{K}$ denota la clausura algebraica de K, diremos que una representación $\rho : G \longrightarrow GL_n(K)$ es *absolutamente irreducible* si la representación inducida $\overline{\rho} : G \longrightarrow GL_n(\overline{K})$ es irreducible; es decir, si $V(\overline{\rho}) \cong V(\rho) \otimes_K \overline{K}$ no tiene subespacios no triviales invariantes por G.

Sea ρ una representación irreducible y $R(\rho)$ la K-subálgebra de $M_n(K)$ generada por $\mathrm{Im}(\rho)$, obtenemos el homomorfismo exhaustivo de K-álgebras $K[G] \longrightarrow R(\rho)$. Denotamos por $\hat{G}_K$ el conjunto de clases de isomorfía de representaciones irreducibles de G con coeficientes en K. Observamos entonces el siguiente resultado, probado en [6]:

Teorema 2.2. *El homomorfismo natural de álgebras*

$$K[G] \longrightarrow \bigoplus_{\rho \in \hat{G_K}} R(\rho)$$

es exhaustivo. Si además K es de característica 0 o la característica de K no divide a $|G|$ la aplicación anterior es un isomorfismo.

En todo caso, $\{Tr(\rho)\}_{\rho \in \hat{G}_K}$ son linealmente independientes como funciones de G.

De este Teorema se sigue el siguiente resultado:

Corolario 2.3. *[Teorema de Brauer - Nesbitt] Sea G un grupo finito. Si dos representaciones con coeficientes en un cuerpo K tienen la misma traza y una de ellas es absolutamente irreducible, entonces son equivalentes.*

Veamos la idea de su demostración, que pasa por suponer, primeramente, que K es algebraicamente cerrado. Sean entonces ρ y ρ' dos representaciones de G, supongamos que ρ' es absolutamente irreducible. Sea $\Omega = \{\rho' = \eta_1, ..., \eta_m\}$ el conjunto de representaciones absolutamente irreducibles de G. Sea $V = V(\rho)$, sabemos que existe un subespacio V_1 no trivial de V $K[G]$-estable minimal. Podemos encontrar entonces una cadena de subespacios vectoriales

$$0 \subset V_1 \subset V_2 \subset \cdots \subset V_r = V$$

de modo que $V_i/V_{i-1} = V(\rho_i)$ para cierta representación ρ_i y es absolutamente irreducible para todo $1 < i \leq r$. Escogiendo entonces para todo i una base de V_i que contenga una de V_{i-1}, tenemos que la matriz de ρ viene dada por

$$\begin{pmatrix} \rho_1 & * & \cdots & * \\ 0 & \rho_2 & & \vdots \\ \vdots & & \ddots & * \\ 0 & \cdots & 0 & \rho_r \end{pmatrix}.$$

De este modo tenemos

$$\mathrm{Tr}(\rho) = \sum_{i=1}^{r} \mathrm{Tr}(\rho_i) = \sum_{\eta \in \Omega} m_\eta \mathrm{Tr}(\eta),$$

es decir, entre $\rho_1, ..., \rho_r$ encontramos η m_η veces. Finalmente, como $\{\mathrm{Tr}(\eta)\}_{\eta \in \Omega}$ son linealmente independientes, la igualdad

$$\mathrm{Tr}(\eta_1) = \mathrm{Tr}(\rho') = \mathrm{Tr}(\rho) = \sum_{\eta \in \Omega} m_\eta \mathrm{Tr}(\eta)$$

implica que $\rho \sim \eta_1 \sim \rho'$.

2.3. Representaciones con coeficientes en un anillo artiniano

Veremos a continuación que el resultado anterior se generaliza también en el caso de anillos artinianos. Para ello destacaremos previamente la definición de anillo artiniano y algunas otras definiciones y nociones relevantes que podemos encontrar en [1]:

Se dice que un anillo A es *artiniano* (resp. *noetheriano*) si toda cadena descendente (resp. ascendente) de ideales de A estaciona.

Sea A un anillo artiniano, en [1] se prueba que A tiene un número finito de ideales maximales y que el nilradical de A, que coincide en este caso con su radical de Jacobson, es nilpotente. De estas propiedades se sigue que un anillo artiniano A es también noetheriano.

Sea M un módulo sobre un anillo cualquiera A, dada una cadena de submódulos de M de la forma

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots M_n = M$$

decimos que n es la longitud de la cadena. Una serie de composición de M es una cadena maximal, es decir, una cadena en la que cada cociente M_i/M_{i-1} es simple.

Se demuestra en [1] que todas las series de composición de un módulo tienen igual longitud y se define entonces la *longitud de* M, $l(M)$, como la longitud de cualquiera de sus series de composición. Si M no tiene series de composición decimos que tiene longitud infinita.

Observamos también que la longitud $l(M)$ es una función aditiva en la clase de todos los A-módulos de longitud finita.

Decimos que un anillo A tiene longitud finita si la tiene como A-módulo.

Observamos ahora que si A es un anillo artiniano, entonces tiene una serie de composición, que podemos construir del siguiente modo: Como A es también noetheriano, $M_0 = A$ tiene un submódulo maximal $M_1 \subset M_0$. De forma similar, M_1 tiene un submódulo maximal $M_2 \subset M_1$, y así sucesivamente. Tenemos entonces una cadena estrictamente descendiente $M_0 \supset M_1 \supset M_2 \supset \cdots$, que, al ser A artiniano, debe estacionar y que, por lo tanto, es una serie de descomposición.

De esta observación se sigue directamente que todo anillo artiniano tiene longitud finita.

Considerando estos resultados previos podemos tratar ahora la generalización del Teorema de Brauer - Nesbitt en el caso de anillos artinianos, que se corresponde con el resultado de Carayol y Serre siguiente:

Sea A un anillo local de ideal maximal $\mathfrak{m}_A$. Si $\rho : G \longrightarrow GL_n(A)$ es una representación, podemos considerar la representación $\overline{\rho} : G \longrightarrow GL_n(A/\mathfrak{m}_A)$.

Proposición 2.4. *[Carayol, Serre] Sea A un anillo local artiniano con cuerpo residual $A/\mathfrak{m}_A$ finito. Sea $R = A[G]$ para un grupo finito G. Si dos representaciones*

$$\rho : R \longrightarrow M_n(A) \;\; y \;\; \rho' : R \longrightarrow M_{n'}(A)$$

tienen la misma traza y $\overline{\rho}$ o $\overline{\rho'}$ es absolutamente irreducible, entonces ρ y ρ' son equivalentes.

Esta proposición se prueba en [6] y se hace por inducción sobre la longitud de A, $l(A)$. La idea es la siguiente: Como las representaciones inducidas

$$\overline{\rho} : G \longrightarrow M_n(A/\mathfrak{m}_A) \;\; \text{y} \;\; \overline{\rho'} : G \longrightarrow M_{n'}(A/\mathfrak{m}_A)$$

tienen imagen finita, factorizan por un grupo cociente finito G' de G. Aplicando entonces el Teorema de Brauer - Nesbitt al grupo finito G', si $l(A) = 1$, la afirmación es cierta y, por lo tanto, $n = n'$. Se supone entonces que $l(A) > 1$ y se considera una serie de composición

$$0 \subset I_1 \subset \cdots \subset I_l = A.$$

Así, $I = I_1$ es un ideal de A tal que $I \cong A/\mathfrak{m}_A$ como $A/\mathfrak{m}_A$-espacios vectoriales y $l(A/I) = l(A) - 1$. De este modo las representaciones $\rho \bmod I$ y $\rho' \bmod I$, que tienen valores en $M_n(A/I)$ y igual traza, por hipótesis de inducción son equivalentes; es decir, existe un $x \in GL_n(A)$ tal que $\rho = x\rho' x^{-1} \bmod I$. Por lo tanto, podemos suponer que $\rho'(\sigma) = \rho(\sigma) + \delta(\sigma)$ para un cierto $\delta : R \longrightarrow M_n(I) \cong M_n(A/\mathfrak{m}_A)$ con $\mathrm{Tr}(\delta(\sigma)) = 0$. Puede probarse entonces también que $\mathrm{Im}(\overline{\rho}) = M_n(A/\mathfrak{m}_A)$ y que existe $U \in M_n(I)$ tal que $\rho'(\sigma) = (1 - U)\rho(\sigma)(1 + U)$. Esto concluye que ρ y ρ' son equivalentes.

3. Introducción a las pseudo-representaciones

En esta sección introducimos el concepto de pseudo-representación de grado 2 dado por A. Wiles y tratamos unos primeros resultados considerando las hipótesis concretas sobre las cuales Wiles trabaja. Introducimos también la definición de pseudo-representación de Taylor, que extiende la anterior a pseudo-representaciones de grado n cualquiera.

3.1. Pseudo-representaciones de Wiles

Sea A un anillo local con ideal maximal $\mathfrak{m}_A$, A. Wiles describe primeramente y de forma detallada la traza de una representación 2-dimensional $\rho : G \longrightarrow GL_2(A)$ cuando 2 invertible en A y G es tal que existe un elemento $c \in G$ con $c^2 = 1$ y $\det\rho(c) = -1$.

Recordamos que $V = V(\rho)$ es el anillo A^2 de vectores columna con la G-acción $\sigma v = \rho(\sigma)v$. Entonces, como 2 es invertible en A, podemos escribir

$$V = V_+ + V_- = \frac{1+c}{2}V + \frac{1-c}{2}V, \text{ con } V_+ = \frac{1+c}{2}V \text{ y } V_- = \frac{1-c}{2}V.$$

De hecho, vemos a continuación que se trata de una suma directa:

Claramente, $V_+ \oplus V_- \subseteq V$. Por otro lado, dados $v, v' \in V$ tales que $\frac{1+c}{2}v = \frac{1-c}{2}v'$ tenemos $(1+c)v = (1-c)v'$, y multiplicando por c la parte derecha de la igualdad, como $c^2 = 1$, es $(1-c)(1+c)v' = (1-c^2) = 0$. De este modo,

$$0 = (1+c)^2 v = (1 +^2 c + c^2)v = (2+2c)v = 2(1+c)v \Rightarrow \frac{1+c}{2}v = 0.$$

Sea $\overline{\rho} : G \longrightarrow GL_2(A/\mathfrak{m}_A)$ la representación inducida por ρ módulo $\mathfrak{m}_A$, de manera similar a la anterior escribimos $\overline{V} = K^2$ como

$$\overline{V} = V(\overline{\rho}) = \overline{V} = \overline{V_+} \oplus \overline{V_-}, \text{ con } \overline{V_+} = V_+/\mathfrak{m}_A V_+ \text{ y } \overline{V_-} = V_-/\mathfrak{m}_A V_-.$$

Dado que la dimensión de V sobre $A/\mathfrak{m}_A$ es 2 y $\overline{V} = \overline{V_+} \oplus \overline{V_-}$, tenemos que V_+ y V_- tienen dimensión 1 sobre $A/\mathfrak{m}_A$. Esto prueba que $\overline{V_+} = K \cdot \overline{v_+}$ y $\overline{V_-} = K \cdot \overline{v_-}$ para ciertos $\overline{v_+} \in \overline{V_+}$ y $\overline{v_-} \in \overline{V_-}$ no nulos. Observamos pues que $\{\overline{v_-}, \overline{v_+}\}$ es una base de $\overline{V}$.

Veremos a continuación que $\{v_-, v_+\}$ es una base de V:

Definimos las aplicaciones

$$\begin{array}{cccc} \phi_+ : & A & \longrightarrow & V_+ \\ & a & \longmapsto & av_+ \end{array} \quad \text{y} \quad \begin{array}{cccc} \phi_- : & A & \longrightarrow & V_- \\ & a & \longmapsto & av_- \end{array}.$$

Entonces las aplicaciones

$$\begin{array}{cccc} \overline{\phi}_+ : & A/\mathfrak{m}_A & \longrightarrow & \overline{V_+} \\ & \overline{a} & \longmapsto & \overline{av_+} \end{array} \quad \text{y} \quad \begin{array}{cccc} \overline{\phi}_- : & A/\mathfrak{m}_A & \longrightarrow & \overline{V_-} \\ & \overline{a} & \longmapsto & \overline{av_-} \end{array}$$

son exhaustivas y, por el Lema de Nakayama, ϕ_+ y ϕ_- también lo son.

Definimos ahora

$$\begin{array}{cccc} \phi : & A^2 & \longrightarrow & V = V_+ \oplus V_- \\ & (a,b) & \longmapsto & \phi_+(a) + \phi_-(b) = av_+ + bv_- \end{array}$$

y observamos que es una aplicación A-lineal exhaustiva.

Identificando V con A^2 podemos mirar $\phi : A^2 \longrightarrow A^2$ como una aplicación A-lineal exhaustiva. Supongamos que $av_+ + bv_- = 0$. Entonces $\overline{av_+} + \overline{bv_-} = 0$ con $\overline{a}, \overline{b} \in A/\mathfrak{m}_A$ y, como $\{\overline{v_-}, \overline{v_+}\}$ es base de $\overline{V}$, tenemos $\overline{a} = \overline{b} = 0$, es decir a, $b \in \mathfrak{m}_A$. Así pues, $\mathrm{Ker}(\phi) \subset \mathfrak{m}_A \times \mathfrak{m}_A$.

Sea ahora $\{u, v\}$ base de V como A-módulo, cogemos $x, y \in A^2$ tales que $\phi(x) = u$ y $\phi(y) = v$ y definimos

$$\begin{array}{cccc} \psi : & V & \longrightarrow & A^2 \\ & au + bv & \longmapsto & ax + by \end{array}$$

Entonces $\phi \circ \psi = id_V$.

Observamos ahora que para todo $t \in A^2$, $t \in \psi(V) + \mathrm{Ker}(\phi)$, dado que podemos escribir

$$t = \psi(\phi(t)) + t - \psi(\phi(t)), \quad \text{con} \quad \psi(\phi(t)) \in \psi(V) \quad \text{y} \quad t - \psi(\phi(t)) \in \mathrm{Ker}(\phi).$$

Además, $\psi(V) \cap \mathrm{Ker}(\phi) = \emptyset$, ya que si $ax+by \in \psi(V)$ y $\phi(ax+by) = 0$, es $au+bv = 0$ y, por lo tanto, $a, b = 0$. Así pues, $A^2 = \psi(V) \oplus \mathrm{Ker}(\phi)$. En particular, $\mathfrak{m}_A\psi(V) \oplus \mathfrak{m}_A\mathrm{Ker}(\phi) = \mathfrak{m}_A A^2$ y $\mathfrak{m}_A\mathrm{Ker}(\phi) = \mathrm{Ker}(\phi)$.

Ahora, $\mathrm{Ker}(\phi) = A^2/\psi(V)$ implica que $\mathrm{Ker}(\phi)$ es un A-módulo finitamente generado, y de nuevo por el Lema de Nakayama, $\mathrm{Ker}(\phi) = 0$. Vemos pues que $\phi : A^2 \longrightarrow V = V_+ \oplus V_-$ es un isomorfismo y, por lo tanto, que $\phi_+ : A \longrightarrow V_+$ y $\phi_- : A \longrightarrow V_-$ son isomorfismos. En otras palabras, hemos visto que $\{v_-, v_+\}$ es una base de V sobre A.

Escribimos ahora, en esta base,

$$\rho(r) = \begin{pmatrix} a(r) & b(r) \\ c(r) & d(r) \end{pmatrix}.$$

Utilizando que $V = \frac{1+c}{2}V \oplus \frac{1-c}{2}V$, en particular tenemos $(1+c)v_- = 0$ y $(1-c)v_+ = 0$. Por lo tanto, si escribimos $\rho(c)$ en esta base, tenemos

$$\rho(c) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Definimos ahora la aplicación

$$\begin{array}{cccc} x : & G \times G & \longrightarrow & A \\ & (r, s) & \longmapsto & b(r)c(s) \end{array}.$$

Entonces se cumple:

(W1) $a(rs) = a(r)a(s) + x(r, s)$,
$d(rs) = d(r)d(s) + x(s, r)$ y
$x(rs, tu) = a(r)a(u)x(s, t) + a(u)d(s)x(r, t) + a(r)d(t)x(s, u) + d(s)d(t)x(r, u)$;

(W2) $a(1) = d(1) = d(c) = 1$,
$a(c) = -1$ y
$x(r, s) = x(s, t) = 0$ si $s = 1, c$;

(W3) $x(r, s)x(t, u) = x(r, u)x(t, s)$.

Veámoslo:

Como una representación ρ es un morfismo de grupos, $\rho(r)\cdot\rho(s)=\rho(r\cdot s)$ para todo $r,s\in G$, es decir,

$$\begin{pmatrix} a(r) & b(r) \\ c(r) & d(r) \end{pmatrix}\begin{pmatrix} a(s) & b(s) \\ c(s) & d(s) \end{pmatrix}=\begin{pmatrix} a(rs) & b(rs) \\ c(rs) & d(rs) \end{pmatrix}$$

Por lo tanto,

$$a(rs)=a(r)a(s)+b(r)c(s)=a(r)a(s)+x(r,s) \text{ y}$$

$$d(rs)=c(r)b(s)+d(r)d(s)=d(r)d(s)+x(s,r).$$

De forma similar tenemos

$$b(rs)=a(r)b(s)+b(r)d(s) \text{ y}$$

$$c(rs)=c(r)a(s)+d(r)c(s),$$

y, de este modo,

$$\begin{aligned} x(rs,tu) &= b(rs)c(tu)=(a(r)b(s)+b(r)d(s))(c(r)a(s)+d(r)c(s))= \\ &= a(r)a(u)x(s,t)+a(u)d(s)x(r,t)+a(r)d(t)x(s,u)+d(s)d(t)x(r,u). \end{aligned}$$

Por otro lado, claramente, $a(1)=d(1)=1$, $a(c)=-1$ y $d(c)=1$. Y como $b(s)=c(s)=0$ si $s=1$ o $s=c$, entonces $x(r,s)=x(s,t)=0$ para $s=1,c$. Finalmente,

$$x(r,s)x(t,u)=b(r)c(s)b(t)c(u)=b(r)c(u)b(t)c(s)=x(r,u)x(t,s). \quad \square$$

A partir de estas propiedades Wiles define el concepto de pseudo-respresentación de grado 2 del siguiente modo:

Definición 3.1. *Fijado un elemento $c\in G$, una pseudo-representación de Wiles de grado 2 de (G,c) es un triplete $\pi=\{a,d,x\}$, donde $a:G\longrightarrow A$, $d:G\longrightarrow A$ y $x:G\times G\longrightarrow A$ son aplicaciones que satisfacen las propiedades $(W1)$, $(W2)$ y $(W3)$.*

Para cada pseudo-representación $\pi=\{a,d,x\}$ definimos

$$\mathrm{Tr}(\pi)(r)=a(r)+d(r) \quad \text{ y } \quad \det(\pi)(r)=a(r)d(r)-x(r,r).$$

Y si A es un anillo en el cual 2 es invertible, usando $(W1)$, $(W2)$ y $(W3)$, vemos que:

$$a(r)=\frac{1}{2}(\mathrm{Tr}(\pi)(r)-\mathrm{Tr}(\pi)(rc)), \quad d(r)=\frac{1}{2}(\mathrm{Tr}(\pi)(r)+\mathrm{Tr}(\pi)(rc)) \quad \text{y}$$

$$x(r,s)=a(rs)-a(r)a(s), \quad \det(\pi)(rs)=\det(\pi)(r)\det(\pi)(s).$$

Esto nos dice que, si 2 es invertible en A, toda pseudo-representación π queda determinada por su traza.

Proposición 3.2. *[A. Wiles, 1988] Sea G un grupo y $R=A[G]$. Sea $\pi=\{a,d,x\}$ una pseudo-representación (de Wiles) de (G,c). Supongamos además que existe al menos un par $(r,s)\in G\times G$ tal que $x(r,s)\in A^*$ o que $x(r,s)=0$ para todo $r,s\in G$. Entonces existe una representación $\rho:R\longrightarrow M_2(A)$ tal que $Tr(\rho)=Tr(\pi)$ y $det(\rho)=det(\pi)$ en G.*

Si A es un anillo topológico, G es un grupo topológico y todas las aplicaciones de π son continuas en G, entonces ρ es una representación continua de G en $GL_2(A)$ bajo la topología de $GL_2(A)$ inducida por la topología producto de $M_2(A)$.

Demostración. Si $x(r,s)=0$ para todo $r,s\in G$, usando $(W1)$ vemos que $a,d:G\longrightarrow A$ satisfacen $a(rs)=a(r)a(s)$ y $d(rs)=d(r)d(s)$, de modo que a y d son representaciones de dimensión 1 de G. Definimos entonces

$$\begin{array}{rccc} \rho: & G & \longrightarrow & GL_2(A) \\ & g & \longmapsto & \begin{pmatrix} a(g) & 0 \\ 0 & d(g) \end{pmatrix}, \end{array}$$

que satisface

$$\mathrm{Tr}(\rho)(g)=a(g)+d(g)=\mathrm{Tr}(\pi)(g) \text{ y } \det(\rho)(g)=a(g)d(g)=\det(\pi)(g).$$

Extendemos ρ a $R=A[G]$ por linealidad.

Por otro lado, si tenemos $x(r,s)\in A^*$ para ciertos $r,s\in G$, definimos $b(g)=\frac{x(g,s)}{x(r,s)}$ y $c(g)=x(r,g)$ para $g\in G$. Luego, por $(W3)$, $b(g)c(h)=\frac{x(r,h)x(g,s)}{x(r,s)}=x(g,h)$. Escribimos

$$\rho(g)=\begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}.$$

Por $(W2)$ vemos que $\rho(1)$ es la matriz identidad y que

$$\rho(c)=\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Y calculando, obtenemos

$$\rho(g)\rho(h)=\begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}\begin{pmatrix} a(h) & b(h) \\ c(h) & d(h) \end{pmatrix}=\begin{pmatrix} a(g)a(h)+b(g)c(h) & a(g)b(h)+b(g)d(h) \\ c(g)a(h)+d(g)c(h) & d(g)d(h)+c(g)b(h) \end{pmatrix}.$$

Usando a continuación $(W1)$, vemos que

$$a(gh)=a(g)a(h)+x(g,h)=a(g)a(h)+b(g)c(h) \text{ y}$$

$$d(gh)=d(g)d(h)+x(h,g)=d(g)d(h)+b(h)c(g).$$

Además, $c(g)a(h)+d(g)c(h)=x(r,g)a(h)+d(g)x(r,h)$, y de nuevo por $(W1)$,

$$\begin{aligned} c(gh)= &\ a(1)a(h)x(r,g)+a(h)d(r)x(1,g)+a(1)d(g)x(r,h)+d(r)d(g)x(1,h)= \\ = &\ a(h)x(r,g)+d(g)x(r,h) \end{aligned}$$

ya que $a(1)=1$ y $x(1,g)=x(1,h)=0$. Por lo tanto, $c(g)c(h)=c(gh)$.

Finalmente, como $(a(g)b(h)+b(g)d(h))x(r,s)=a(g)x(h,s)+x(g,s)d(h)$ y, a su vez,

$$\begin{aligned} b(gh)x(r,s)= &\ a(g)a(s)x(h,1)+a(s)d(h)x(g,1)+a(g)d(1)x(h,s)+d(h)d(1)x(g,s)= \\ = &\ a(g)x(h,s)+d(h)x(g,s) \end{aligned}$$

obtenemos que $b(g)b(h)=b(gh)$.

Tenemos entonces que $\rho(gh)=\rho(g)\rho(h)$ y extendiendo ρ linealmente a $R=A[G]$ hemos demostrado la primera afirmación. La continuidad de π nos da la continuidad de cada elemento de la matriz $\rho(g)$ y de ella se sigue la continuidad de ρ. $\square$

Observemos, a continuación, la biyección que existe entre ciertas representaciones y pseudo-representaciones de Wiles:

Fijemos una representación absolutamente irreducible $\overline{\rho} : G \longrightarrow GL_2(A/\mathfrak{m}_A)$ con $\det(\overline{\rho})(c) = -1$. Si tenemos una representación $\rho : G \longrightarrow GL_2(A)$ tal que $\rho \bmod \mathfrak{m}_A \sim \overline{\rho}$, entonces $\det(\rho(c)) = -1 \bmod \mathfrak{m}_A$. Como $c^2 = 1$, si 2 es invertible en A (es decir, si la característica de $A/\mathfrak{m}_A$ es diferente de 2), $\det(\rho(c)) = -1$. Entonces tenemos una pseudo-representación de Wiles π_ρ asociada a ρ. Como $\overline{\rho}$ es absolutamente irreducible, existen $r, s \in G$ tales que $b(r) \neq 0 \bmod \mathfrak{m}_A$ y $c(s) \neq 0 \bmod \mathfrak{m}_A$, de modo que π_ρ satisface la Proposición 3.2.

Por otro lado, si tenemos una pseudo-representación $\pi : G \longrightarrow A$ con $\pi = \overline{\pi} \bmod \mathfrak{m}_A$ para $\overline{\pi} = \pi_{\overline{\rho}}$ existen de nuevo $r, s \in G$ tales que $x(r, s) \in A^*$. La correspondencia entre ρ y π_ρ induce una biyección:

$$\{\rho : G \longrightarrow GL_2(A) \text{ representación} \mid \rho \bmod \mathfrak{m}_A \sim \overline{\rho}\}/\sim\ \longleftrightarrow$$

$$\{\pi : G \longrightarrow A \text{ pseudo-representación de Wiles} \mid \pi \bmod \mathfrak{m}_A = \overline{\pi}\}$$

La aplicación es exhaustiva por la Proposición 3.2 y biyectiva por la Proposición 2.4, ya que una representación queda determinada por su traza.

3.2. Pseudo-representaciones de Taylor

Como hemos observado, cualquier representación de grupos $\rho : G \longrightarrow GL_n(A)$ es inducida por una representación de A-álgebras $\rho : A[G] \longrightarrow M_n(A)$, es decir, por un homomorfismo de A-álgebras. Por lo tanto, sin pérdida de generalidad, podemos restringirnos a representaciones $\rho : R \longrightarrow M_n(A)$ donde R es una A-álgebra.

Sean pues A un anillo conmutativo y R una A-álgebra, Taylor define el concepto de pseudo-representación (de Taylor) de grado n del siguiente modo:

Definición 3.3. *Una pseudo-representación de Taylor de grado n es una función $T : R \longrightarrow A$ que satisface las siguientes propiedades:*

(T1) $T(1) = n$;

(T2) $T(rs) = T(sr)$ *para todo* $r, s \in G$;

(T3) $\displaystyle\sum_{\sigma \in \mathfrak{S}_{n+1}} sgn(\sigma) T_\sigma(r_0, r_1, ..., r_n) = 0$ *para todo* $r, s \in G$.

donde T_σ está definida de la siguiente manera: Si descomponemos σ en producto de cíclos disjuntos (incluyendo todos los 1-cíclos):

$$\sigma = (i_{1,1} i_{1,2} \cdots i_{1,k_1}) \cdots (i_{m,1} i_{m,2} \cdots i_{m,k_m}),$$

$$T_\sigma(r_0, \cdots, r_n) = \prod_j T(r_{i_{j,1}} r_{i_{j,2}} \cdots r_{i_{j,k_j}}).$$

Podemos ver que la traza de una representación de grado n es una pseudo-representación de igual dimensión: Sea $\rho : R \longrightarrow M_n(A)$ una representación de grado n, primero vemos que, como ρ envía la identidad a la matriz identidad, $\mathrm{Tr}(1) = 1$. Claramente, para dos matrices X, Y $n \times n$ es $\mathrm{Tr}(XY) = \mathrm{Tr}(YX)$. Más generalmente, para n matrices $X_1, ..., X_n$,

$$\mathrm{Tr}(X_1 X_2 \cdots X_n) = \mathrm{Tr}(X_n X_1 X_2 \cdots X_{n-1})$$

y para cualquier permutación cíclica $\sigma \in \mathfrak{S}_\mathfrak{n}$,

$$\mathrm{Tr}(X_1 X_2 \cdots X_n) = \mathrm{Tr}(X_{\sigma(1)} X_{\sigma(2)} \cdots X_{\sigma(n)}).$$

Esto prueba que $\mathrm{Tr}(rs) = \mathrm{Tr}(sr)$ y que, para $\sigma = (1, 2..., n)^k$ una permutación cíclica,

$$\mathrm{Tr}(r_1 r_2 \cdots r_n) = \mathrm{Tr}(r_{\sigma(1)} r_{\sigma(2)} \cdots r_{\sigma(n)}).$$

C. Procesi prueba en [11] que para todo $r, s \in G$,

$$\sum_{\sigma \in \mathfrak{S}_{\mathfrak{n}+1}} \mathrm{sgn}(\sigma) \mathrm{Tr}_\sigma(r_0, r_1, ..., r_n) = 0.$$

Es decir, que dada una representación $\rho : R \longrightarrow M_n(A)$, su traza $T = \mathrm{Tr}(\rho)$ es una pseudo-representación de R de grado n.

El resultado recíproco es probado por R. Taylor y L. Nyssen. Concretamente, Taylor prueba en [15] que, siendo K un cuerpo algebraicamente cerrado de característica 0 y $R = K[G]$ para un grupo G; dada una pseudo-representación de Taylor $T : R \longrightarrow K$ de grado n, entonces existe una representación $\rho : G \longrightarrow M_n(K)$ con $T = \mathrm{Tr}(\rho)$.

En [10] Nyssen demuestra que siendo A un anillo artiniano y $T : R \longrightarrow A$ una pseudo-representación de Taylor de grado n, si existe una representación absolutamente irreducible $\overline{\rho} : R \longrightarrow M_n(A/\mathfrak{m}_A)$ tal que $T \bmod \mathfrak{m}_A = \mathrm{Tr}(\overline{\rho})$, entonces existe una única representación $\rho : R \longrightarrow M_n(A)$ tal que $T = \mathrm{Tr}(\rho)$.

Fijada $\overline{\rho} : R \longrightarrow GL_n(A/\mathfrak{m}_A$ una representación absolutamente irreducible, por los resultados anteriores la correspondencia $\rho \longmapsto Tr(\rho)$ induce una biyección:

$$\{\rho : G \longrightarrow GL_n(A) \text{ representación} \mid \rho \bmod \mathfrak{m}_A \sim \overline{\rho}\}/\sim \;\longleftrightarrow$$

$$\{T : G \longrightarrow A \text{ pseudo-representación de Taylor de grado } n \mid T \bmod \mathfrak{m}_A = \mathrm{Tr}(\overline{\rho})\}$$

En este trabajo presentaremos los resultados de R. Rouquier que cubren tales resultados.

4. Pseudo-representaciones. Definición y propiedades elementales

Consideramos A un anillo conmutativo y R una A-álgebra.

Sean $f \in \mathrm{Hom}_A(R, A)$ una función central (es decir, un homomorfismo tal que $f(xy) = f(yx)$ para todo $x, y \in R$) y n un entero positivo. Sea $\mathfrak{S}_n$ el grupo simétrico de orden n, y ε el carácter signatura de $\mathfrak{S}_n$. Definimos la aplicación $S_n(f) : R^n \longrightarrow A$ como

$$S_n(f)(x) = \sum_{\sigma \in \mathfrak{S}_\mathbf{n}} \varepsilon(\sigma)(\sigma \cdot f)(x)$$

donde si $x = (x_1, ..., x_n) \in R^n$, $\sigma = \sigma_1 \cdots \sigma_k$ es la descomposición en cíclos disjuntos de $\sigma \in \mathfrak{S}_n$ (incluyendo todos los 1-cíclos) y $\sigma_i = (j_1, ..., j_m)$, entonces $\sigma_i(x) = x_{j_1} \cdots x_{j_m}$ y

$$(\sigma \cdot f)(x) = f(\sigma_1(x)) \cdots f(\sigma_k(x)).$$

Además, sea $\tau \in \mathfrak{S}_n$, la descomposición de $\tau^{-1}\sigma\tau$ en producto de cíclos disjuntos es $\tau^{-1}\sigma\tau = (\tau^{-1}\sigma_1\tau) \cdots (\tau^{-1}\sigma_n\tau)$ y si $\sigma_i = (j_1, ..., j_m)$, entonces $\tau^{-1}\sigma_i\tau = (\tau(j_1), ..., \tau(j_m))$. Por lo tanto, $(\sigma \cdot f)(\tau \cdot x) = ((\tau^{-1}\sigma\tau) \cdot f)(x)$. Luego, $S_n(f)(\tau \cdot x) = S_n(f)(x)$, es decir, S_n es una aplicación simétrica.

Para $f \in \mathrm{Hom}_A(R, A)$ una función central, definimos $S_0(f) = 1$ y observamos, por ejemplo, que para $n = 1, 2, 3$ tenemos

$$S_1(f)(x_1) = f(x_1) \ ,$$

$$S_2(f)(x_1, x_2) = f(x_1) \cdot f(x_2) - f(x_1x_2) \quad \text{y}$$

$$\begin{aligned} S_3(f)(x_1, x_2, x_3) = \ & f(x_1) \cdot f(x_2) \cdot f(x_3) - f(x_1x_2) \cdot f(x_3) - f(x_1x_3) \cdot f(x_2) - \\ & - f(x_2x_3) \cdot f(x_1) + f(x_1x_2x_3) + f(x_1x_3x_2). \end{aligned}$$

Definición 4.1. *Sea d un entero positivo, decimos que $f \in Hom(R, A)$ es una pseudo-representación de dimensión d de R en A (y notamos $dimf = d$) si:*

1. *$f(xy) = f(yx)$ para todo $x, y \in R$,*
2. *d es el entero positivo k más pequeño tal que $S_{k+1}(f) = 0$.*

Diremos que f es *irreducible* si no existen dos pseudo-representaciones f_1, f_2 tales que $f = f_1 + f_2$ y $\dim f = \dim f_1 + \dim f_2$.

Esta definición de pseudo-representación, dada por Rouquier, es una ligera modificación de la noción original de pseudo-representación de grado d de Taylor, donde se pide, en lugar de 2., que $S_{d+1}(f) = 0$ y que $f(1) = d \cdot 1_A$. Esta nueva definición nos permite tener una noción de dimensión bien determinada para cada pseudo-representación. Hemos visto también que, previamente y para el caso $n = 2$, Wiles da una definición más restrictiva de pseudo-representación.

Observamos ahora que para $f \in \mathrm{Hom}_A(R, A)$ una función central, se satisface

$$S_1(f)(x_1) = f(x_1) \ ,$$

$$S_2(f)(x_1, x_2) = f(x_2) \cdot S_1(f)(x_1) - S_1(f)(x_1x_2) \quad \text{y}$$

$$S_3(f)(x_1, x_2, x_3) = f(x_3) \cdot S_2(f)(x_1, x_2) - S_2(f)(x_1x_3, x_2) - S_2(f)(x_1, x_2x_3) \ ;$$

relación que se puede extender, dando lugar al siguiente Lema:

Lema 4.2. *Sean n un entero positivo y $f \in Hom_A(R, A)$ una función central. Sean $x_1, ..., x_{n+1} \in R$, entonces:*

(1) Para todo n natural,

$$\begin{aligned} S_{n+1}(f)(x_1, ..., x_{n+1}) = \ & f(x_{n+1})S_n(f)(x_1, ..., x_n)- \\ & -\sum_{i=1}^{n} S_n(f)(x_1, ..., x_{i-1}, x_i x_{n+1}, x_{i+1}, ..., x_{n+1}). \end{aligned}$$

(2) Sea g una segunda función central y $E = \{1, ..., n\}$,

$$S_n(f+g)(x_1, ..., x_n) = \sum_{I \subset E} S_{|I|}(f)(\{x_i\}_{i\in I}) S_{|E-I|}(g)(\{x_i\}_{i\in E-I}),$$

donde I denota los subconjuntos de E.

Demostración. Veamos primero (1):

$$\begin{aligned} S_{n+1}(f)(x_1, ..., x_{n+1}) = \ & \sum_{i=1}^{n} \sum_{\substack{\sigma \in \mathfrak{S}_{\mathfrak{n}+1}, \\ \sigma(i)=n+1}} \varepsilon(\sigma)(\sigma \cdot f)(x_1, ..., x_{n+1}) + \\ & + \sum_{\substack{\sigma \in \mathfrak{S}_{\mathfrak{n}+1}, \\ \sigma(n+1)=n+1}} \varepsilon(\sigma)(\sigma \cdot f)(x_1, ..., x_{n+1}) \end{aligned}$$

donde

$$\sum_{\substack{\sigma \in \mathfrak{S}_{\mathfrak{n}+1}, \\ \sigma(n+1)=n+1}} \varepsilon(\sigma)(\sigma \cdot f)(x_1, ..., x_{n+1}) = f(x_{n+1})S_n(f)(x_1, ..., x_n).$$

y donde, como para todo $\sigma \in \mathfrak{S}_{\mathfrak{n}+1}$ con $\sigma(i) = n+1$ podemos escribir $\sigma = \sigma'(i\ n+1)$, entonces

$$\varepsilon(\sigma)(\sigma \cdot f)(x_1, ..., x_{n+1}) = -\varepsilon(\sigma')(\sigma' \cdot f)(x_1, ..., x_{i-1}, x_i \cdot x_{n+1}, x_{i+1}, ..., x_{n+1},$$

Por lo tanto, para $1 \leq i \leq n$ tenemos

$$\sum_{\substack{\sigma \in \mathfrak{S}_{\mathfrak{n}+1}, \\ \sigma(i)=n+1}} \varepsilon(\sigma)(\sigma \cdot f)(x_1, ..., x_{n+1}) - \sum_{i=1}^{n} S_n(f)(x_1, ..., x_{i-1}, x_i \cdot x_{n+1}, x_{i+1}, ..., x_{n+1}).$$

Probamos, a continuación, (2):

$$\begin{aligned} S_n(f+g)(\{x_i\}_{i\in E}) = \ & \sum_{\sigma \in \mathfrak{S}(E)} \sum_{\substack{I \subset E, \\ \sigma(I)=I}} \varepsilon(\sigma)(\sigma_{|I} \cdot f)(\{x_i\}_{i\in I})(\sigma_{|E-I} \cdot g)(\{x_i\}_{i\in E-I}) = \\ = \ & \sum_{I \subset E} \sum_{\substack{\sigma_1 \in \mathfrak{S}(I), \\ \sigma_2 \in \mathfrak{S}(E-I)}} \varepsilon(\sigma_1)\varepsilon(\sigma_2)(\sigma_1 \cdot f)(\{x_i\}_{i\in I})(\sigma_2 \cdot g)(\{x_i\}_{i\in E-I}), \end{aligned}$$

de donde se sigue la segunda igualdad. □

De la primera igualdad de este lema, se deduce directamente la siguiente proposición:

Proposición 4.3. *Si f es una pseudo-representación de dimensión n, entonces $S_k(f) = 0$ para todo $k > n$.*

Proposición 4.4. *Sea A un dominio de integridad. Si f es una pseudo-representación de dimensión n, entonces $f(1) = n \cdot 1_A$.*

Demostración. Si $n = 0$, el resultado es claro. Supongamos pues que $n > 0$. Entonces dados $x_1, ..., x_n \in R$, por la primera igualdad del Lema 4.2,

$$S_{n+1}(f)(x_1, ..., x_n, 1) = (f(1) - n \cdot 1_A)S_n(x_1, ..., x_n).$$

Finalmente, como $S_n(f) \neq 0$ y A es dominio de integridad, $f(1) = n \cdot 1_A$. □

Lema 4.5. *Dados k un entero y $\{1, ..., k\} = I_1 \cup \cdots \cup I_l$ una partición de $\{1, ..., k\}$. Sea $x = x_1 \times \cdots \times x_l$ donde $x_i \in R^{I_i}$. Supongamos que $yy' = y'y = 0$ para todas las componentes y, y' de x_i, x_j con $i \neq j$. Entonces, para $f \in Hom_A(R, A)$ una función central, tenemos*

$$S_k(f)(x) = \prod_{i=1}^{l} S_{|I_i|}(f)(x_i)$$

Demostración. Sea $\sigma \in \mathfrak{S}_k$ con una órbita cuya intersección con dos elementos distintos I_i, I_j de la partición es no vacía. Sea ahora σ' un cíclo de σ correspondiente a esta órbita. Entonces $\sigma'(x) = 0$ y, por lo tanto, $(\sigma \cdot f)(x) = 0$. De este modo obtenemos

$$S_k(f)(x) = \sum_{\sigma} \varepsilon(\sigma)(\sigma \cdot f)(x),$$

donde σ describe $\mathfrak{S}(I_1) \times \cdots \times \mathfrak{S}(I_l)$. □

Vemos, a continuación, un ejemplo para ilustrar dicha propiedad:

Sea $k = 3$ y $\{1, 2, 3\} = \{1\} \cup \{2, 3\}$ una partición, escribimos $x = (y_1, y_2, y_3)$ como $x = x_1 \times x_2$ donde $x_1 = y_1$ y $x_2 = (y_2, y_3)$. Entonces, suponiendo que $y_1y_2 = y_2y_1 = 0$ y que $y_1y_3 = y_3y_1 = 0$, tenemos

$$\begin{aligned} S_3(f)(y_1, y_2, y_3) = \;& f(y_1) \cdot f(y_2) \cdot f(y_3) - f(y_1y_2) \cdot f(y_3) - f(y_1y_3) \cdot f(y_2) - \\ & -f(y_2y_3) \cdot f(y_1) + f(y_1y_2y_3) + f(y_1y_3y_2) = \\ = \;& f(y_1) \cdot [f(y_2)f(y_3) - f(y_2y_3)] = \\ = \;& S_1(f)(y_1) \cdot S_2(f)(y_2y_3). \end{aligned}$$

Lema 4.6. *Sea f una pseudo-representación de R, para todo $x \in R$ nilpotente, $f(x)$ es nilpotente.*

Demostración. Observamos primero que si x es tal que $f(x^r)$ es nilpotente para algún $r \geq 2$, entonces $f(x)$ es nilpotente, ya que de la misma forma en que

$S_1(f)(x) = f(x)$,

$S_2(f)(x, x) = f(x)^2 - f(x^2)$ o

$S_3(f)(x, x, x) = f(x)^3 - 3f(x)f(x^2) + 2f(x^3)$,

$S_{1+\dim f}(f)(x,...,x)$ también tiene como sumando $f(x)^{1+\dim f}$. Y como por definición $S_{1+\dim f}(f)(x,...,x) = 0$, tenemos $f(x)^{1+\dim f} = 0$. Así, $f(x)^{1+\dim f}$ es nilpotente y, por lo tanto, $f(x)$ también.

Sea ahora $x \in R$ nilpotente y $r > 1$ tal que $x^r = 0$, entonces si $i \geq r$, $f(x^i)$ es nilpotente. En particular, para $i \geq 2$, $f((x^{r-1})^i)$ es nilpotente y, por la observación anterior, $f(x^{r-1})$ es nilpotente. Finalmente, y por recurrencia descendiente sobre r, $f(x)$ es nilpotente. $\square$

Lema 4.7. *Sea $f \in Hom_A(R,A)$ una función central y k un entero tal que $k!$ no es divisor de 0 en R, entonces*

$$S_k(f) = 0 \iff S_k(f)(x,...,x) = 0 \text{ para todo } x \in R.$$

Demostración. Sea $S^k(R)$ la potencia simétrica k-ésima de un A-módulo R, es decir, $S^k(R) = \frac{R\otimes\cdots\otimes R}{\{x\otimes y - y\otimes x\}}$, y φ la aplicación

$$\begin{array}{cccc} \varphi: & R^k & \longrightarrow & S^k(R) \\ & (x_1,...,x_k) & \longmapsto & x_1\cdots x_k \end{array},$$

por la propiedad universal de $S^k(R)$, y dado que $S_k(f)$ es k-lineal y simétrica, existe $g \in \mathrm{Hom}_A(S^k(R),A)$ tal que el siguiente diagrama conmuta:

$$\begin{tikzcd} R^k \arrow[r, "S_k(f)"] \arrow[d, "\pi"'] & A \\ S^k(R) \arrow[ur, "g"'] & \end{tikzcd}.$$

Sea ahora A' la localización de A en el conjunto multiplicativamente cerrado generado por $k!$. Sean $R' = A' \otimes_A R$ y $f' = id_{A'} \otimes f \in \mathrm{Hom}_{A'}(R',A')$. Dado que $k!$ no es divisor de 0 en R, tampoco lo es en A y, por lo tanto, los morfismos canónicos

$$\begin{array}{ccc} A & \longrightarrow & A' \\ a & \longmapsto & \frac{a}{1} \end{array} \quad \text{y} \quad \begin{array}{ccc} R & \longrightarrow & R' \\ r & \longmapsto & 1\otimes r \end{array}$$

son inyectivos.

Como $S_k(f') : (A' \otimes_A R)^k \longrightarrow A'$ es k-lineal, tenemos que $S_k(f') = 0$ si y solamente si $S_k(f) = 0$, y que $S_k(f')(x,...,x) = 0$ para todo $x \in R'$ si y solamente si $S_k(f)(x,...,x) = 0$ para todo $x \in R$. Por consiguiente, es suficiente demostrar el lema en el caso en que $k!$ es invertible en A. Así pues, suponiendo que $k!$ es invertible en A, el A-módulo $S^k(R)$ está generado por x^k con $x \in R$ y, por lo tanto, $S_k(f) = 0$ si y solo si $S_k(f)(x,...,x) = 0$ para todo $x \in R$. $\square$

Lema 4.8. *Sean f y g dos pseudo-representaciones, entonces $f+g$ es una pseudo-representación y $\dim(f+g) \leq \dim f + \dim g$.*

Además, si A es un dominio de integridad, $(\dim f+\dim g)! \cdot 1_A \neq 0$ y $(\dim f)!\cdot(\dim g)!$ no es divisor de 0 en R, entonces $\dim(f+g) = \dim f+\dim g$.

Del mismo modo, si A es un dominio de integridad y R es el producto directo de dos sub A-álgebras R_1 y R_2 tales que $f(R_2) = g(R_1) = 0$, entonces también tenemos $\dim(f+g) = \dim f+\dim g$.

Demostración. Sean $m = \dim f$ y $n = \dim g$, por la segunda igualdad del Lema 4.2 tenemos $S_{m+n+1}(f+g) = 0$. Luego, por el Lema 4.6, existen $x, y \in R$ tales que $S_m(f)(x,..,x) \neq 0$ y $S_n(g)(y,..,y) \neq 0$.

Sea ahora k el entero positivo más pequeño tal que $S_n(g)(\underbrace{x,...,x}_{n-k},\underbrace{y,...,y}_{k}) \neq 0$, por el Lema 4.2 tenemos que

$$S_{m+n}(f+g)(\underbrace{x,...,x}_{m+n-k},\underbrace{y,...,y}_{k}) = \binom{m+n-k}{n-k} S_m(f)(x,...,x)S_n(g)(\underbrace{x,...,x}_{n-k},\underbrace{y,...,y}_{k}) \neq 0.$$

Ahora, si $(m+n)! \cdot 1_A \neq 0$, $\;S_{m+n}(f+g) \neq 0$.

Si R es el producto directo de las sub A-álgebras R_1 y R_2 tales que $f(R_2) = g(R_1) = 0$, entonces necesariamente $k = n$ y, por lo tanto, $S_{m+n}(f+g) \neq 0$. $\square$

Observación 4.9. Si r es un entero positivo con $r \cdot 1_A \neq 0$, f es una pseudo-representación no nula y $g = (r-1)f$, entonces g es una pseudo-representación y $f+g = 0$ es una pseudo-representación nula, es decir, de dimensión nula.

Lema 4.10. *Sea A' una A-álgebra conmutativa. Sea $f \in Hom_A(R, A)$ y f' la extensión de f a $R \otimes_A A'$. Si f es una pseudo-representación, entonces f' es una pseudo-representación de $R \otimes_A A'$ y $\dim f' \leq \dim f$.*

Si además A' es un A-módulo fiel (es decir, si $Ann_A(A') = 0$), entonces f es una pseudo-representación si y solo si f' es una pseudo-representación. Y en este caso, $\dim f' = \dim f$.

Demostración. Primeramente, tenemos

$$\begin{array}{ccccc} R \otimes_A A' & \xrightarrow{f'} & A \otimes A' & \xrightarrow{\cong} & A' \\ x \otimes a' & \longmapsto & f(x) \otimes a' & \longmapsto & f(x)a' \end{array}$$

y como f es una función central, f' también lo es, ya que

$$f'((x \otimes a')(y \otimes b')) = f(xy)a'b' = f(yx)b'a' = f'((y \otimes b')(x \otimes a')).$$

Ahora, dado que $S_n(f) : R^n \longmapsto A\;$ y $\;S_n(f) \otimes_A Id_{A'} : R^n \otimes_A A' \longmapsto A'$ son aplicaciones A-multilineales y que

$$\begin{tikzcd} R^n \otimes_A A' \arrow[r, "S_n(f)\otimes Id_{A'}"] \arrow[d, "\cong"'] & A' \\ (R \otimes_A A')^n \arrow[ur, "S_n(f')"'] & \end{tikzcd}$$

es un diagrama conmutativo, $S_n(f') : (R \otimes_A A')^n \longrightarrow A'$ también es A-multilineal. Además, $S_{n+1}(f) = 0 \Rightarrow S_{n+1}(f') = 0$ y $\dim f' \leq \dim f$. Finalmente y si además A' es fiel, entonces $A \subset A'$ y, por lo tanto, f es una pseudo-representación si y solo si f' es una pseudo-representación. En este caso obtenemos también que $\dim f = \dim f'$. $\square$

Sea $f \in \mathrm{Hom}_A(R,A)$, denotamos por $\hat{f} \in \mathrm{Hom}_A(R, \mathrm{Hom}_A(R,A))$ la aplicación definida como:

$$\begin{array}{ccl} R & \xrightarrow{\hat{f}} & \mathrm{Hom}_A(R,A) \\ x & \longmapsto & \hat{f}(x) : R \ \to \ A \\ & & \qquad\qquad y \mapsto f(xy) \end{array}$$

Si f es una función central, entonces $\mathrm{Ker}\hat{f}$ es un ideal de R.

Definición 4.11. *Sea f una pseudo-representación, decimos que f es fiel si $Ker\hat{f} = 0$.*

Proposición 4.12. *Sean f una pseudo-representación fiel de R en A, A' una A-álgebra y f' la extensión de f a $R \otimes_A A'$. Si R es finitamente generado como A-módulo y A' es un A-módulo plano o proyectivo, entonces f' es fiel.*

Demostración. Dado que $\hat{f} : R \longrightarrow \mathrm{Hom}_A(R,A)$ es una aplicación inyectiva, si A' es A-plano, la aplicación obtenida por extensión de escalares

$$\hat{f} \otimes Id_{A'} : R \longrightarrow \mathrm{Hom}_A(R,A) \otimes_A A'$$

también es inyectiva. Por otro lado, dado que R es de tipo finito como A-módulo y A' es proyectivo sobre A, el homomorfismo canónico

$$\psi : \mathrm{Hom}_A(R,A) \otimes_A A' \longrightarrow \mathrm{Hom}_{A'}(R \otimes_A A', A')$$

también es inyectivo. Así pues, la aplicación $\widehat{f'} = (\hat{f} \otimes Id_{A'}) \circ \psi$ es inyectiva y, por lo tanto, f' es una pseudo-representación fiel. □

Lema 4.13. *Sea f una pseudo-representación fiel de dimensión n de R. Sean A' una A-álgebra conmutativa, $R' = R \otimes_A A'$ y f' la extensión de f a R'. Dados $x_1, ..., x_n \in R'$, entonces*

$$\sum_{I,\sigma} (-1)^{|I|} S_{n-|I|}(f')(\{x_i\}_{i \notin I}) x_{\sigma(1)} \cdots x_{\sigma(|I|)} = 0,$$

donde I recorre los subconjuntos de $\{1, ..., n\}$ y σ el conjunto de las biyecciones $\{1, ..., |I|\} \to I$.

Demostración. Como la identidad a probar es multilineal, es suficiente probarla para $A' = A$. Así pues, dado $y \in R$, tenemos

$$\begin{aligned} S_{n+1}(f)(x_1, ..., x_n, y) &= \sum_I (-1)^{|I|} S_{n-|I|}(f)(\{x_i\}_{i \notin I}) f(x_{\sigma(1)} \cdots x_{\sigma(|I|)} y) = \\ &= f\left(\left(\sum_I (-1)^{|I|} S_{n-|I|}(f)(\{x_i\}_{i \notin I}) x_{\sigma(1)} \cdots x_{\sigma(|I|)}\right) y\right) = 0. \end{aligned}$$

Finalmente,

$$\sum_I (-1)^{|I|} S_{n-|I|}(f)(\{x_i\}_{i \notin I}) x_{\sigma(1)} \cdots x_{\sigma(|I|)} \in \mathrm{Ker}\hat{f} = 0.$$

□

Lema 4.14. *Sea f una pseudo-representación fiel de dimensión n de R. Sean A' una A-álgebra conmutativa, $R' = R \otimes_A A'$ y f' la extensión de f a R'. Entonces todo elemento de R' se anula por un polinomio de grado n sobre A'. Para $x \in R'$, tenemos $P_x(x) = 0$, donde*

$$P_x(t) = \sum_{k=0}^{n} (-1)^k \frac{n!}{(n-k)!} S_{n-k}(f')(x, ..., x) t^k.$$

Demostración. Teniendo en cuenta que para cada $1 \leq k \leq n$ hay $\frac{n!}{(n-k)!}$ subconjuntos de $\{1, ..., n\}$ de k elementos contados juntamente con sus permutaciones, observamos que este lema es consecuencia directa del anterior. $\square$

Lema 4.15. *Sea f una pseudo-representación fiel de R. Sean A' una A-álgebra conmutativa, $R' = R \otimes_A A'$ y f' la extensión de f a R'. Si $e_1, ..., e_k$ son elementos idempotentes no nulos y ortogonales dos a dos de R', entonces $k \leq \dim f$.*

Demostración. Sea $n = \dim f$, supongamos $k > n$. Por la definición de $S_n(f')$, como $e_1, ..., e_{n+1}$ son ortogonales dos a dos, tenemos

$$S_{n+1}(f')(e_1, ..., e_{n+1}) = f'(e_1) \cdots f'(e_{n+1})$$

y, a su vez, como la dimensión de f' es n tenemos $S_{n+1}(f')(e_1, ..., e_{n+1}) = 0$. De este modo, $f'(e_1) \cdots f'(e_{n+1}) = 0$.

Notamos ahora que, siendo $P_x(t)$ el polinomio definido en el lema anterior, $P_{e_i}(e_i) = 0$. Sea i minimal tal que $f'(e_1) \cdots f'(e_i) = 0$. Vemos primero que $i \neq 1$ ya que si $i = 1$ entonces $P_{e_i}(t) = n!t^n$ y, en particular, $P_{e_i}(e_i) = n!e_i^n = n!e_i \neq 0$, que contradice la observación anterior. Entonces tenemos

$$f'(e_1) \cdots f'(e_{i-1}) P_{e_i}(t) = f'(e_1) \cdots f'(e_{i-1}) n!t^n,$$

ya que los coeficientes de t^m con $m < n$ del polinomio $f'(e_1) \cdots f'(e_{i-1}) P_{e_i}(t)$ son múltiplos de $f'(e_1) \cdots f'(e_i)$. Así pues,

$$f'(e_1) \cdots f'(e_{i-1}) P_{e_i}(1) = f'(e_1) \cdots f'(e_{i-1}) n!,$$

y como $P_{e_i}(1) = 0$ obtenemos $f'(e_1) \cdots f'(e_{i-1}) = 0$, que contradice la minimalidad de i. De este modo, $k \leq n$. $\square$

5. Pseudo-representaciones inducidas por representaciones

En esta sección consideraremos morfismos de A-álgebras $\rho : R \longrightarrow \Sigma$ y diremos entonces que ρ es una representación de R en Σ. Definiremos también la traza reducida de una representación de un álgebra en un álgebra de Azumaya y veremos que es una pseudo-representación.

Las álgebras de Azumaya son una generalización de las álgebras simples centrales a álgebras sobre A cuando A no es necesariamente un cuerpo. Fueron introducidas por G. Azumaya en [2] para A un anillo conmutativo local. Seguimos aquí la defincíón dada en [5]:

Definición 5.1. *Sea A un anillo conmutativo y Σ una A-álgebra. Decimos que Σ es un álgebra de Azumaya sobre A si y solo si:*

1. *Σ es un A-módulo fiel finito generado,*
2. *Para todo ideal maximal $\mathfrak{m}$ de A, la $A/\mathfrak{m}$-álgebra $\Sigma/\mathfrak{m}\Sigma$ es simple central (es decir, una $A/\mathfrak{m}$-álgebra simple cuyo centro es $A/\mathfrak{m}$).*

Notamos que si Σ es un álgebra de Azumaya sobre A, el A-módulo Σ es, de hecho, proyectivo.

Se demuestra en [3] que si Σ es una A-álgebra de Azumaya, existe $A \longrightarrow A'$ una extensión fielmente plana de A tal que $\Sigma \otimes_A A'$ es isomorfo a un álgebra de matrices $M_n(A')$. Decimos entonces que A' es una extensión neutralizante de A para Σ.

Sea ρ una representación de R en Σ observamos que tenemos:

$$\begin{array}{ccccccc} R & \longrightarrow & R \otimes_A A' & \xrightarrow{\rho\otimes 1_{A'}} & \Sigma \otimes_A A' & \xrightarrow{h} & M_n(A') \\ r & \longmapsto & r \otimes 1 & \longmapsto & \rho(r) \otimes 1 & \longmapsto & h(\rho(r) \otimes 1) \end{array}$$

donde h es un isomorfismo.

Se prueba también en [3] que la traza de $h(\rho(r)\otimes 1)$ es un elemento de A independiente de la extensión A' de A. Definimos entonces la *traza reducida de ρ* como la aplicación:

$$\begin{array}{rccc} \chi : & R & \longrightarrow & A \\ & r & \longmapsto & Tr(h(\rho(r) \otimes 1)) \end{array}.$$

Proposición 5.2. *Sea $\rho : R \longrightarrow \Sigma$ una representación de R en una A-álgebra de Azumaya Σ. Sea χ la traza reducida de ρ. Entonces, χ es una pseudo-representación.*

Si Σ es de rango n^2 en A, χ es de dimensión menor o igual a n.

Demostración. De la definición de traza reducida observamos que es suficiente tratar el caso en que $R = \Sigma$ y ρ es la identidad. Además, por el Lema 4.10, es suficiente probar la proposición para $A_\mathfrak{m}$ en lugar de A y $R \otimes A_\mathfrak{m}$ en lugar de R para todo ideal maximal $\mathfrak{m}$ de A. Por consiguiente podemos suponer que A es local. Extendiendo ahora los escalares de forma fielmente plana podemos suponer $R = M_n(A)$. Observamos también que podemos remplazar A por un anillo conmutativo íntegro de característica 0 del cual A es un cociente. Por lo tanto, podemos remplazar A por la clausura algebraica de su cuerpo de fracciones. Así, asumimos ahora que A es un cuerpo algebraicamente cerrado de característica 0 que denotaremos por K.

Sea ahora k un entero, $k > n$, queremos ver que $S_k(\chi) = 0$, es decir, que $S_k(\chi)(x_1,...,x_n) = 0$ para todo $x_1,...,x_n \in M_n(K)$. Por el Lema 4.7 es suficiente probar que $S_k(\chi)(x,...,x) = 0$ para todo $x \in M_n(K)$. Además, al ser K algebraicamente cerrado y de característica 0, tenemos que toda matriz es diagonalizable y, por lo tanto, es suficiente verificar que se anula para las matrices diagonalizables. De hecho, solo para las matrices diagonales, puesto que $S_k(\chi)(x,...,x) = S_k(\chi)(y,...,y)$ si x e y son conjugadas.

Sean pues x una matriz diagonal de $M_n(K)$ y $V = K^n$, vemos que x actúa sobre $V^{\otimes k}$ de manera que $x(a_1,...,a_n) = (xa_1,...,xa_n)$ para $(a_1,...,a_n) \in V$. Por otro lado, el grupo simétrico $\mathfrak{S}_k$ actúa sobre $V^{\otimes k}$ por permutación de los factores y esta acción conmuta con la de x.

Dado $\sigma \in \mathfrak{S}_k$, entonces, en la base canónica $\{e_{i_1} \otimes \cdots \otimes e_{i_k}\}_{1 \leq i_j \leq n}$ de $V^{\otimes k}$ inducida por la base $\{e_i\}_{1 \leq i \leq n}$ de V, la matriz del endomorfismo inducido por $x\sigma$ es monomial ya que la matriz del endomorfismo inducido por x es diagonal. Sea ahora $\sigma = \sigma_1 \cdots \sigma_m$ la descomposición de σ en producto de ciclos disjuntos, los vectores de la base fijados por σ son los $e_{i_1} \otimes \cdots \otimes e_{i_k}$ tales que $i_{\sigma(j)} = i_j$ para todo $1 \leq j \leq k$. Por consiguiente, la traza de $x\sigma$ en $V^{\otimes k}$ es $\chi(x^{c_1}) \cdots \chi(x^{c_m})$ donde $c_1,...,c_m$ denotan las longitudes de los cíclos de σ.

De este modo, la traza de $x \sum\limits_{\sigma \in \mathfrak{S}_k} \varepsilon(\sigma)\sigma$ en $V^{\otimes k}$ es

$$\chi\left(x \sum_{\sigma \in \mathfrak{S}_k} \varepsilon(\sigma)\sigma\right) = \chi\left(\sum_{\sigma \in \mathfrak{S}_k} \varepsilon(\sigma)(x\sigma)\right) = \sum_{\sigma \in \mathfrak{S}_k} \varepsilon(\sigma)\chi(x\sigma) = \sum_{\sigma \in \mathfrak{S}_k} \varepsilon(\sigma)(\sigma \cdot \chi)(x,...,x),$$

es decir, $S_k(\chi)(x,...,x)$; y dado que la acción de x conmuta con la de S_k, la traza de $x \sum\limits_{\sigma \in \mathfrak{S}_k} \varepsilon(\sigma)\sigma$ en $V^{\otimes k}$ es igual a la de x en $(\sum\limits_{\sigma \in \mathfrak{S}_k} \varepsilon(\sigma)\sigma)V^{\otimes k}$, que es la k-ésima potencia exterior de V. Por lo tanto, y puesto que $k > n$, es 0. Así pues, $S_k(\chi)(x,...,x) = 0$. □

Ejemplificamos parte de la demostración anterior en el caso $n = 2$ y $k = 3$:

Después de habernos reducido al caso en que $A = K$ es un cuerpo algebraicamente cerrado de característica 0 y haber visto que es suficiente demostrar que $S_k(x,x) = 0$ para toda matriz diagonal $x \in M_2(K)$, probamos dicha igualdad:

Sea $x = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$, consideramos la acción de x sobre $(K^2)^{\otimes 3} = K^2 \otimes K^2 \otimes K^2$ dada de modo que

$$\begin{array}{ccc} K^2 & \longrightarrow & K^2 \\ (a_1, a_2) & \longmapsto & (d_1a_1, d_2a_2). \end{array}$$

Siendo $\{e_1, e_2\}$ la base canónica de K^2, consideramos en $(K^2)^{\otimes 3}$ la base

$$\{e_1\otimes e_1\otimes e_1,\ e_1\otimes e_1\otimes e_2,\ e_1\otimes e_2\otimes e_1,\ e_2\otimes e_1\otimes e_1,\ e_1\otimes e_2\otimes e_2,\ e_2\otimes e_1\otimes e_2,\ e_2\otimes e_2\otimes e_1,\ e_2\otimes e_2\otimes e_2\}.$$

Ahora fijémonos por ejemplo en $\sigma = (12)(3)$. Las imágenes de los elementos de la base de $(K^2)^{\otimes 3}$ anterior por $x\sigma$ son:

$$
\begin{aligned}
x\sigma(e_1 \otimes e_1 \otimes e_1) &= d_1e_1 \otimes d_1e_1 \otimes d_1e_1 = d_1^3 \cdot (e_1 \otimes e_1 \otimes e_1),\\
x\sigma(e_1 \otimes e_1 \otimes e_2) &= d_1e_1 \otimes d_1e_1 \otimes d_2e_2 = d_1^2d_2 \cdot (e_1 \otimes e_1 \otimes e_2),\\
x\sigma(e_1 \otimes e_2 \otimes e_1) &= d_2e_2 \otimes d_1e_1 \otimes d_1e_1 = d_1^2d_2 \cdot (e_2 \otimes e_1 \otimes e_1),\\
x\sigma(e_2 \otimes e_1 \otimes e_1) &= d_1e_1 \otimes d_2e_2 \otimes d_1e_1 = d_1^2d_2 \cdot (e_1 \otimes e_2 \otimes e_1),\\
x\sigma(e_1 \otimes e_2 \otimes e_2) &= d_2e_2 \otimes d_1e_1 \otimes d_2e_2 = d_1d_2^2 \cdot (e_2 \otimes e_1 \otimes e_2),\\
x\sigma(e_2 \otimes e_1 \otimes e_2) &= d_1e_1 \otimes d_2e_2 \otimes d_2e_2 = d_1d_2^2 \cdot (e_1 \otimes e_2 \otimes e_2),\\
x\sigma(e_2 \otimes e_2 \otimes e_1) &= d_2e_2 \otimes d_2e_2 \otimes d_1e_1 = d_1d_2^2 \cdot (e_2 \otimes e_2 \otimes e_1) \text{ y}\\
x\sigma(e_2 \otimes e_2 \otimes e_2) &= d_2e_2 \otimes d_2e_2 \otimes d_2e_2 = d_2^3 \cdot (e_2 \otimes e_2 \otimes e_2).
\end{aligned}
$$

De este modo vemos que las matrices de los endomorfismos $x\sigma$ para cada

$$\sigma \in \{Id = (1)(2)(3),\ (12)(3),\ (13)(2),\ (23)(1),\ (123),\ (132)\}$$

son respectivamente:

$$
\begin{pmatrix}
d_1^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & d_1^2d_2 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & d_1^2d_2 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & d_1^2d_2 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & d_1d_2^2 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & d_1d_2^2 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & d_1d_2^2 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & d_2^3
\end{pmatrix},
\begin{pmatrix}
d_1^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & d_1^2d_2 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & d_1^2d_2 & 0 & 0 & 0 & 0\\
0 & 0 & d_1^2d_2 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & d_1d_2^2 & 0 & 0\\
0 & 0 & 0 & 0 & d_1d_2^2 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & d_1d_2^2 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & d_2^3
\end{pmatrix},
$$

$$
\begin{pmatrix}
d_1^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & d_1^2d_2 & 0 & 0 & 0 & 0\\
0 & 0 & d_1^2d_2 & 0 & 0 & 0 & 0 & 0\\
0 & d_1^2d_2 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & d_1d_2^2 & 0\\
0 & 0 & 0 & 0 & 0 & d_1d_2^2 & 0 & 0\\
0 & 0 & 0 & 0 & d_1d_2^2 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & d_2^3
\end{pmatrix},
\begin{pmatrix}
d_1^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & d_1^2d_2 & 0 & 0 & 0 & 0 & 0\\
0 & d_1^2d_2 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & d_1^2d_2 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & d_1d_2^2 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & d_1d_2^2 & 0\\
0 & 0 & 0 & 0 & 0 & d_1d_2^2 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & d_2^3
\end{pmatrix},
$$

$$
\begin{pmatrix}
d_1^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & d_1^2d_2 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & d_1^2d_2 & 0 & 0 & 0 & 0\\
0 & d_1^2d_2 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & d_1d_2^2 & 0\\
0 & 0 & 0 & 0 & d_1d_2^2 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & d_1d_2^2 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & d_2^3
\end{pmatrix},
\begin{pmatrix}
d_1^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & d_1^2d_2 & 0 & 0 & 0 & 0\\
0 & d_1^2d_2 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & d_1^2d_2 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & d_1d_2^2 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & d_1d_2^2 & 0\\
0 & 0 & 0 & 0 & d_1d_2^2 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & d_2^3
\end{pmatrix}.
$$

Observamos pues que para todo $\sigma \in \mathfrak{S}_3$, los vectores de la base fijados por σ son los $e_{i_1} \otimes e_{i_2} \otimes e_{i_3}$ tales que $e_{i_j} = e_{i_k}$ para todo j, k perteneciente al mismo cíclo de σ, es decir, los $e_{i_1} \otimes e_{i_2} \otimes e_{i_3}$ tales que $i_{\sigma(j)} = i_j$ para todo $1 \leq j \leq 3$.

Así pues, del mismo modo en que para $\sigma = (12)(3)$

$$\chi(x\sigma) = d_1^3 + d_1^2d_2 + d_1d_2^2 + d_2^3 = (d_1^2 + d_2^2)(d_1 + d_2) = \chi(x^2) \cdot \chi(x),$$

para cada permutación $\sigma \in \mathfrak{S}_3$, si esta descompone en cíclos disjuntos como $\sigma = \sigma_1 \cdots \sigma_m$ tenemos $\chi(x\sigma) = \chi(x^{c_1}) \cdots \chi(x^{c_m})$ donde c_i denota la longitud del cíclo σ_i para cada $1 \leq i \leq m$.

Ahora, como hemos visto en el caso general, $\chi\left(x \sum\limits_{\sigma \in \mathfrak{S}_3} \varepsilon(\sigma)\sigma\right) = S_3(\chi)(x, x, x)$ y, como el caracter de los endomorfismos

$$(K^2)^{\otimes 3} \xrightarrow{x \sum_{\sigma\in\mathfrak{S}_3} \varepsilon(\sigma)\sigma} (K^2)^{\otimes 3} \quad \text{y} \quad \sum_{\sigma\in\mathfrak{S}_3} \varepsilon(\sigma)\sigma(K^2)^{\otimes 3} \xrightarrow{x} \sum_{\sigma\in\mathfrak{S}_3} \varepsilon(\sigma)\sigma(K^2)^{\otimes 3}$$

es igual, y $\sum_{\sigma\in\mathfrak{S}_3} \varepsilon(\sigma)\sigma)(K^2)^{\otimes 3}$ es la tercera potencia exterior de K^2, que es nula porque $k = 3 > n = 2$, tenemos que $S_3(\chi)(x, x, x) = 0$.

Continuando con el caso $n = 2$ y $k = 3$, fijémonos ahora en la matriz identidad $I \in M_2(K)$. Observamos que para $\sigma = (12) = (12)(3)$,

$$(\sigma \cdot \chi)(I, I, I) = \chi\left((12)(I, I, I)\right) \cdot \chi\left((3)(I, I, I)\right) = \mathrm{Tr}(I^3) \cdot \mathrm{Tr}(I^3) = 2^2.$$

Del mismo modo podemos observar que, en general, para cualquier permutación $\sigma \in \mathfrak{S}_3$, $(\sigma \cdot \chi)(I, I, I) = (\mathrm{Tr}(I^3))^{c_\sigma} = 2^{c_\sigma}$ donde c_σ es el número de órbitas de σ. Así pues,

$$S_3(I, I, I) = \sum_{\sigma\in\mathfrak{S}_3} \varepsilon(\sigma)(\sigma \cdot \chi)(I, I, I) = \sum_{\sigma\in\mathfrak{S}_3} \varepsilon(\sigma)2^{c_\sigma} = 0$$

De esta última observación se sigue el siguiente corolario:

Corolario 5.3. *Sean k un entero positivo y P_k el polinomio dado por $P_k(t) = \sum_{\sigma\in\mathfrak{S}_k} \varepsilon(\sigma)t^{c_\sigma}$ donde c_σ designa el número de órbitas de σ, entonces*

$$P_k(t) = (t - k + 1)(t - k + 2)\cdots(t - 1)t.$$

Demostración. Con las hipótesis y las notaciones de la proposición que le precede, y fijándonos en la última observación, tenemos $P_k(n) = S_k(\chi)(1, ..., 1) = 0$ para todo $k > n$. Por consiguiente, los enteros $0, ..., k - 1$ son las raíces de P_k. Ahora, como P_k es un polinomio mónico y de grado k, obtenemos el resultado. □

Corolario 5.4. *Sea R un álgebra de matrices de dimensión n^2 sobre un cuerpo K. Sea $\alpha > 0$ un entero, con $\alpha < p$ en caso de que K sea un cuerpo de característica $p > 0$. Entonces, la pseudo-representación αTr es de dimensión αn.*

Demostración. Sea $1 = e_1 + \cdots + e_n$ una descomposición de la unidad de R en idempotentes primitivos (idempotentes tales que si $e_i = e_{i_1} + e_{1_2}$ con e_{i_1}, e_{i_2} ortogonales, entonces $e_{i_1} = 0$ o $e_{i_2} = 0$) ortogonales dos a dos. Por el Lema 4.5, tenemos

$$S_{\alpha n}(\alpha Tr)(\underbrace{e_1, ..., e_1}_{\alpha}, ..., \underbrace{e_n, ..., e_n}_{\alpha}) = \prod_{i=1}^{n} S_\alpha(\alpha Tr)(e_i, ..., e_i) = \prod_{i=1}^{n} P_\alpha(\alpha Tr(e_i)) = P_\alpha(\alpha)^n \neq 0.$$

De este modo, $\dim(\alpha\mathrm{Tr}) \geq \alpha n$. Por otro lado, y debido a la Proposición 5.2, $\dim(\mathrm{Tr}) = n$ y, como por el Lema 4.8 tenemos $\dim(\alpha\mathrm{Tr}) \leq \alpha \dim(\mathrm{Tr})$, obtenemos el resultado. □

6. Representaciones asociadas a pseudo-representaciones

Nos ocupamos ahora del problema recíproco al planteado en la sección anterior.

Consideraremos primero pseudo-representaciones sobre un cuerpo y demostraremos que toda pseudo-representación absolutamente irreducible es la traza reducida de una representación en una álgebra simple central.

En general, considerando pseudo-representaciones sobre un anillo, veremos que toda pseudo-representación f, cuyas pseudo-representaciones residuales asociadas son absolutamente irreducibles y de dimensión igual a la de f, es la traza de una representación en una cierta álgebra de Azumaya.

6.1. Construcción de representaciones sobre un cuerpo

Consideramos en esta sección R un anillo arbitrario. Enunciamos, a continuación, ciertos resultados necesarios para demostrar el primer resultado que nos ocupa.

Lema 6.1. *[Schur] Sea M un R-módulo simple, entonces el anillo de endomorfismos de M, $End_R(M)$, es un cuerpo.*

Demostración. Sea f un endomorfismo de M no nulo, entonces $\mathrm{Ker} f \subsetneq M$ es un submódulo de M con $\mathrm{Im} f \neq \{0\}$. Como M es simple, no tiene submódulos no triviales y, por lo tanto $\mathrm{Ker} f$=0. Entonces, claramente, $\mathrm{Im} f = M$ y, por lo tanto, f es biyectiva. Finalmente, como f^{-1} es una aplicación R-lineal, f tiene inversa en $\mathrm{End}_R(M)$. □

Los siguientes son resultados generales sobre módulos simples que utilizaremos a lo largo de esta sección y la demostración de los cuales podemos encontrar en [3]:

Teorema 6.2. *[Teorema de densidad de Jacobson] Sean M un R-módulo semisimple y $D = End_R(M)$. Entonces R es denso para M como D-espacio vectorial, es decir, dada una secuencia finita $m_1, ..., m_n$ de elementos de M D-linealmente independientes y dada una secuencia $m'_1, ..., m'_n$ de elementos de M, existe $r \in R$ tal que $m_1 r = m'_1, ..., m_n r = m'_n$.*

Denotamos por $H_R(M)$ el subanillo de $\mathrm{End}_R(M)$ formado por sus homotecias, y por h_r la homotecia de $H_R(M)$ que, fijado $r \in R$, se define vía $m \longmapsto rm$.

Corolario 6.3. *Sean $M_1, ..., M_n$ R-módulos simples no isomorfos dos a dos. Sean $r_1, ..., r_n$ elementos de R. Entonces existe $r \in R$ tal que $(h_i)_{r_i} = (h_i)_r$ para todo $1 \leq i \leq n$.*

Teorema 6.4. *[Teorema de Burnside] Sean K un cuerpo conmutativo algebraicamente cerrado y R una K-álgebra. Sea M un R-módulo simple de dimensión finita sobre K, entonces $H_R(M) = End_K(M)$.*

Corolario 6.5. *Sea K un cuerpo conmutativo algebraicamente cerrado y R una K-álgebra. Sean $M_1, ..., M_n$ R-módulos simples dos a dos no isomorfos y de dimensiones finitas sobre K. Sea $f_1 \in End_K(M_i)$ para todo $1 \leq i \leq n$. Entonces existe un $r \in R$ tal que $(h_i)_r = f_i$ para todo $1 \leq i \leq n$.*

Consideramos ahora K un cuerpo conmutativo y R una K-álgebra.

Lema 6.6. *Sea f una pseudo-representación de R en K, entonces $R/Ker(\hat{f})$ es un álgebra semisimple. Además, los centros de los factores simples de $R/Ker(\hat{f})$ son extensiones separables de K.*

Demostración. Podemos remplazar R por $R/\mathrm{Ker}\hat{f}$ y suponer $\mathrm{Ker}\hat{f} = 0$. Entonces, por el Lema 4.14, sabemos que todo elemento de R se anula por un polinomio de grado $\dim f$ en K.

Sea M un R-módulo simple y $D = \mathrm{End}_R(M)$, D es un cuerpo de centro contenido en K, por el Lema 6.1. Siendo S la imagen de R en $\mathrm{End}_K(M)$, observamos que S se identifica con $H_R(M)$ (el subanillo de $\mathrm{End}_R(M)$ formado por sus homotecias). Así pues, por el Teorema 6.2 S es un subanillo denso de $\mathrm{End}_D(M)$. Por [3, §4, exercice 9] vemos que si M es de dimensión infinita sobre D, entonces para todo entero $n > 0$ existe un morfismo exhaustivo de un subanillo de S en $M_n(D^\circ)$, donde D° denota el cuerpo opuesto a D. Ahora, como todo elemento de R, y por lo tanto de S, se anula por un polinomio de grado $\dim f$ en K; todo elemento de $M_n(D^\circ)$ se anula por un polinomio de grado $\dim f$ en K. Pero esto es imposible, puesto que $n > \dim f$. Así pues, M es de dimensión finita sobre D.

Sean ahora k un entero, $M_1, ..., M_k$ R-módulos simples no isomorfos dos a dos y $M = M_1 \oplus \cdots \oplus M_k$, entonces por el Corolario 6.5 la imagen de R en $\mathrm{End}_K(M)$ es igual a $\prod_{i=1}^{k} \mathrm{End}_{D_i}(M_i)$ donde $D_i = \mathrm{End}_R(M_i)$. De este modo, R tiene un cociente isomorfo a $\prod_{i=1}^{k} M_{n_i}(D_i^\circ)$, siendo $n_i = \dim_{D_i}(M_i)$.

Notamos que si S es una subálgebra de R y S' un cociente de S, entonces todo idempotente de S' es la imagen de un idempotente de S: En efecto, sea $e \in S'$ un idempotente y $x \in S$ de imagen e. Entonces la K-subálgebra de S generada por x es de dimensión finita, ya que x se anula por un polinomio sobre K. De este modo, y por [3, §4, exercice 5], tenemos que existe un idempotente de la subálgebra generada por x de imagen e.

Sean ahora $1_1, ..., 1_k$ las unidades de $\mathrm{End}_{D_1}(M_1), ..., \mathrm{End}_{D_k}(M_k)$, estos son elementos idempotentes no nulos y ortogonales dos a dos. Así pues, por [3, §4, exercice 5], existen idempotentes dos a dos ortogonales $e_1, ..., e_k$ de R tales que la imagen de e_i en $\mathrm{End}_K(M)$ es 1_i para todo $1 \leq i \leq k$. Ahora, debido al Lema 4.15, tenemos $k \leq \dim f$ y, por consiguiente, R tiene como mucho $\dim f$ clases de isomorfía de módulos simples.

Veamos a continuación que el radical de Jacobson de R, $J(R)$, es 0: Sean $x \in R$ y P un polinomio de grado $\dim f$ tal que $P(x) = 0$. Sean $r \geq 0$, $a \in K$ y Q un polinomio tales que $P = aX^r(1 + XQ)$. Como $x \in J(R)$, $1 + xQ(x)$ es invertible por la derecha. Ahora, $P(x) = ax^r(1 + xQ(x)) = 0$ implica que $x^r = 0$ y $r > 0$, es decir, x es nilpotente de orden $r \leq \dim f$. Por consiguiente, el ideal $J(R)$ es nilpotente. De este modo, y por el Lema 4.6, tenemos que $J(R) = 0$, ya que f es una pseudo-representación fiel. El álgebra R, que tiene un número finito de clases de isomorfía de módulos simples, los cuales son de dimensión finita, y que tiene un radical nulo, es entonces producto finito de álgebras simples. Esto prueba la primera parte del Lema.

Sea ahora S una subálgebra simple de R, de la cual es un factor directo; la restricción f' de f en S es una pseudo-representación fiel de R. Denotando por $Z(S)$ el centro de S, por la Proposición 4.12, la aplicación

$$f' \otimes 1_{Z(S)} : S \otimes_K Z(S) \longrightarrow Z(S)$$

es una pseudo-representación fiel de $S \otimes_K Z(S)$. Por la primera parte del Lema, el álgebra $S \otimes_K Z(S)$ es semisimple y, por consiguiente, $Z(S)$ es una extensión separable de K. $\square$

Recordamos que una pseudo-representación f es irreducible si no existen dos pseudo-representaciones f_1, f_2 tales que $f = f_1 + f_2$ y $\dim f = \dim f_1 + \dim f_2$. Diremos entonces que una pseudo-representación f de R en K es *absolutamente irreducible* si para toda extensión L de K la pseudo-representación $f \otimes 1_L$ de $R \otimes_K L$ en L es irreducible.

Teorema 6.7. *Sea f una pseudo-representación absolutamente irreducible de dimensión n de R en K. Entonces, $R/Ker\hat{f}$ es un álgebra simple central sobre K de dimensión n^2 y f es la traza reducida de la representación absolutamente irreducible $R \longrightarrow R/Ker\hat{f}$.*

Demostración. Podemos suponer que f es fiel. Entonces, por el Lema 6.6 podemos suponer también que R es isomorfo a un producto de álgebras simples sobre K cuyos centros son extensiones separables de K. Sea K_S la clausura separable de K, entonces, por [3, §10, Corollaire 3], $R \otimes_K K_S$ es isomorfo a un producto de álgebras de matrices sobre K_S. Además, por la Proposición 4.12, la extensión f' de f a $R \otimes_K K_S$ es una pseudo-representación fiel e irreducible ya que f es irreducible. Si $R \otimes_K K_S$ es isomorfo a un álgebra de matrices de dimensión n^2 sobre K_S y f' es la traza correspondiente, entonces R es isomorfo a un álgebra simple central de dimensión n^2 sobre K y f es la traza reducida correspondiente. Así pues, es suficiente demostrar el Teorema cuando R es isomorfo a un producto de álgebras de matrices sobre K. El Teorema resulta entonces del lema que veremos a continuación. $\square$

Lema 6.8. *Sean $n_1, ..., n_s$ enteros positivos y $R = \prod_{i=1}^{s} R_i$ donde $R_i \simeq M_{n_i}(K)$ para todo $1 \leq i \leq s$. Dada f una pseudo-representación de R, entonces existen $\alpha_1, ..., \alpha_s$ enteros positivos, con $\alpha_i \leq p-1$ para todo $1 \leq i \leq s$ en caso que K sea de característica $p > 0$, tales que $f = \sum_{i=1}^{s} \alpha_i Tr_i$, donde Tr_i es el caracter de la proyección $R \longrightarrow R_i$. Tenemos entonces $dim f = \sum_{i=1}^{s} \alpha_i n_i$.*

Demostración. Sea e_i un idempotente primitivo de R_i para cada $1 \leq i \leq s$, es decir, un idempotente $e_i \neq 0$ tal que si $e_i = e_{i_1} + e_{i_2}$ con e_{i_1}, e_{i_2} ortogonales, entonces $e_{i_1} = 0$ o $e_{i_2} = 0$. Como f es una función central, tenemos $f = \sum_{i=1}^{s} f(e_i) Tr_i$. Sabemos también que

$$S_{k+1}(f)(e_i, ..., e_i) = P_{k+1}(f(e_i)) = 0.$$

Así pues, por el Corolario 5.3, tenemos $f(e_i) \in \{0, ..., 1_K \cdot \dim f\}$.

Sea p la característica de K. Dados los enteros $\alpha_1, ..., \alpha_s$ tales que para todo $1 \leq i \leq s$, $f(e_i) = 1_K \cdot \alpha_i$ y $0 \leq \alpha_i \leq p-1$ si $p > 0$. Por el Lema 4.8 tenemos

$$\dim f = \sum_{i=1}^{s} \dim(\alpha_i Tr_i).$$

Por el Corolario 5.4 tenemos además que $\dim(\alpha_i Tr_i) = \alpha_i n_i$, de donde se sigue el resultado. $\square$

Corolario 6.9. *Supongamos que toda álgebra simple central sobre K es isomorfa a un álgebra de matrices (por ejemplo, suponiendo K algebraicamente cerrado). Sea f una pseudo-representación absolutamente irreducible de dimensión n de R en K. Entonces $R/Ker\hat{f}$ es isomorfo a un álgebra de matrices de dimensión n^2 sobre K y f es el caracter de la representación absolutamente irreducible $R \longrightarrow R/Ker\hat{f}$.*

Observamos que, considerando el caso particular en que K es un cuerpo algebraicamente cerrado de característica nula, este corolario recupera el resultado de Taylor mencionado en la Sección 3.2 y cuya demostración podemos encontrar en [15].

6.2. Construcción de representaciones sobre un anillo

Supondremos en esta subsección que A es un anillo conmutativo.

Si Σ es una A-álgebra de Azumaya y ρ, ρ' son dos representaciones de R en Σ, decimos que ρ y ρ' son equivalentes si existe un A-automorfismo τ de Σ tal que $\rho' = \tau\rho$.

El siguiente resultado demuestra que en el caso de álgebras de Azumaya, la definición de representaciones equivalentes dada aquí se corresponde con la noción clásica de equivalencia dada en la sección 2. Este generaliza, para álgebras de Azumaya, el Teorema de Skolem - Noether, que nos dice que todo K-automorfismo τ de álgebras de matrices sobre K es interior (es decir, de la forma $\tau(r) = xrx^{-1}$ para cierto x invertible).

Teorema 6.10. *Sea Σ un álgebra de Azumaya sobre un anillo semi-local A. Si τ es un A-automorfismo de Σ, entonces τ es un automorfismo interno.*

Demostración. Sea τ un A-automorfismo de Σ. Sea Σ° el álgebra opuesta de Σ y $\Sigma^e := \Sigma \otimes_A \Sigma^\circ$. Entonces Σ es un Σ^e-módulo por la izquierda con las multiplicaciones

$$\begin{array}{rccc} \mu_1 : & \Sigma^e \times \Sigma & \longrightarrow & \Sigma \\ & (x \otimes y, r) & \longmapsto & xry \end{array} \quad \text{y} \quad \begin{array}{rccc} \mu_2 : & \Sigma^e \times \Sigma & \longrightarrow & \Sigma \\ & (x \otimes y, r) & \longmapsto & \tau(x)ry \end{array}$$

Denotaremos por Σ_1 y Σ_2 a Σ con la estructura de Σ^e-módulo dada por μ_1 y μ_2 respectivamente. Observamos que Σ^e es una A-álgebra de Azumaya y que Σ_1 y Σ_2 son Σ^e-módulos proyectivos finitamente generados de igual rango. De ello se deduce que existe un isomorfismo de Σ^e-módulos por la izquierda $\pi : \Sigma_1 \longrightarrow \Sigma_2$. Entonces para todo $r \in \Sigma$, $\pi(r) = \pi((r \otimes 1) \cdot 1) = \pi((1 \otimes r) \cdot 1)$, por lo tanto, $(r \otimes 1) \cdot \pi(1) = (1 \otimes r) \cdot \pi(1)$. Esto implica que $\tau(r) \cdot \pi(1) = \pi(1) \cdot r$. Además, como π es un isomorfismo, existe un elemento $s \in \Sigma_1$ tal que $\pi(s) = 1$. Así pues, $\pi(s) = \pi(1) \cdot s = 1 = \tau(s) \cdot \pi(1)$. Entonces $\pi(1)$ es una unidad en Σ tal que $\tau(r) = \pi(1)r(\pi(1))^{-1}$ para todo $r \in \Sigma$. Esto concluye que τ es un A-automorfismo interno de Σ. □

En el Teorema siguiente utilizaremos la henselización de anillos locales. Decimos que un anillo local A es *henseliano* si toda A-álgebra finita es producto de anillos locales. Decimos que A es estrictamente henseliano si además su cuerpo residual K es separablemente cerrado, es decir, si todas las extensiones finitas separables de K son triviales.

Sea A un anillo local, llamamos *henselización de* A a una pareja (A', i) donde A' es un anillo local henseliano y i es un morfismo local $i : A \longrightarrow A'$ tales que para todo anillo local henseliano B y para todo morfismo local $u : A \longrightarrow B$, existe un único morfismo local $u' : A' \longrightarrow B$ tal que $u = u'i$.

De forma similar existe una henselización estricta de A. Sin embargo esta no es del todo universal, sino que es única excepto isomorfismo. Concretamente, depende de la elección de la clausura algebraica separable del cuerpo residual de A; y los automorfismos de dicha clausura algebraica separable corresponden a los automorfismos de la correspondiente henselización estricta. Se puede probar que el henselizado estricto de A es una extensión fielmente plana.

Teorema 6.11. *Sea f una pseudo-representación de R tal que para todo ideal maximal $\mathfrak{m}$ de A, si $f_{\mathfrak{m}}$ designa la pseudo-representación correspondiente de $R \otimes_A A/\mathfrak{m}$, entonces $f_{\mathfrak{m}}$ es absolutamente irreducible y $dim f_{\mathfrak{m}} = dim f$. Entonces $R/Ker\hat{f}$ es un álgebra de Azumaya de rango $(dim f)^2$ sobre A y f es la traza reducida de la representación $\rho_f : R \longrightarrow R/Ker\hat{f}$. Además, si ρ es una representación de R en un álgebra de Azumaya de rango $(dim f)^2$ sobre A y de traza reducida f, entonces ρ es equivalente a ρ_f.*

Demostración. Podemos suponer $\mathrm{Ker}\hat{f} = 0$. Sea $n = \dim f$.

Sea $\mathfrak{m}$ un ideal maximal de A y K el cuerpo residual de $A_{\mathfrak{m}}$, es decir, $K = A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}}$. Sea $A'_{\mathfrak{m}}$ una henselización estricta de $A_{\mathfrak{m}}$; $A'_{\mathfrak{m}}$ es un anillo local henseliano, que es una extensión local fielmente plana de $A_{\mathfrak{m}}$ y de cuerpo residual K' una clausura separable de K. Sea $\mathfrak{m}'$ su ideal maximal. Sean $R' = R \otimes A_{\mathfrak{m}}$ y

$$f' : R' \xrightarrow{f \otimes id_{A_{\mathfrak{m}}}} A \otimes A_{\mathfrak{m}}$$

la pseudo-representación de R' que extiende f. Por el Lema 4.10, tenemos $\dim f' = \dim f$ y $\dim \overline{f'} = \dim \overline{f}$, donde $\overline{f}$ y $\overline{f'}$ denotan respectivamente las pseudo-representaciones

$$\overline{f} : \overline{R} = R \otimes K \longrightarrow A \otimes K \quad \text{ y } \quad \overline{f'} : \overline{R'} = R \otimes K' \longrightarrow A \otimes K'.$$

Ahora, como $K = A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}} \cong A/\mathfrak{m}$, tenemos que el diagrama

$$\begin{tikzcd} R \otimes K \arrow[r, "\overline{f}"] \arrow[d, "\cong"] & A \otimes K \arrow[d, "\cong"] \\ R \otimes A/\mathfrak{m} \arrow[r, "f_{\mathfrak{m}}"] & A \otimes A/\mathfrak{m} \end{tikzcd}$$

es conmutativo y que, por lo tanto, $\overline{f}$ es absolutamente irreducible. Entonces, por el Teorema 6.7, la K-álgebra $\overline{R}/Ker\hat{\overline{f}}$ es simple central de dimensión n^2 y, de este modo, $(\overline{R}/Ker\hat{\overline{f}}) \otimes_K K'$ es un álgebra de matrices de dimensión n^2 sobre K'. Además, por la Proposición 4.12 tenemos

$$\overline{R'}/Ker\hat{\overline{f'}} \cong (\overline{R}/Ker\hat{\overline{f}}) \otimes_K K'.$$

Sean $e_1, ..., e_n$ idempotentes de R' dos a dos ortogonales con imágenes en $\overline{R'}/Ker\hat{\overline{f'}}$ idempotentes no nulos ortogonales dos a dos. Entonces tenemos $1 = e_1 + \cdots + e_n$, ya que en caso contrario, $e_1, ..., e_n, 1 - (e_1 + \cdots + e_n)$ serian $n + 1$ idempotentes no nulos de R' ortogonales dos a dos y, por el Lema 4.15 esto no puede ocurrir.

Ahora, de acuerdo con [3, §4, exercice 5], existen elementos $\{e_{ij}\}_{1 \leq i,j \leq n}$ de R' tales que $e_{ij}e_{kl} = \delta_{jk}e_{il}$ y $e_{ii} = e_i$. Sea S la subálgebra de R' generada por los e_{ij}. Si $n = 1$, por el Lema 4.14, tenemos $x = f'(x)1_{R'}$ para todo $x \in R'$, es decir, $R' = S$. Sino, si $n > 1$, para

$i \neq j$ tenemos $e_{ij}^2 = 0$ y, por el Lema 4.6, $f'(e_{ij})$ es nilpotente. Sea I el ideal de A generado por los $f'(e_{ij})$ con $i \neq j$, este es un ideal nilpotente, pues está generado por un número finito de elementos nilpotentes. Sean $x \in R'$ y $i_1, ..., i_n$ tales que $\{i_1, ..., i_n\} = \{1, ..., n\}$ y $x_1 = e_{i_1 i_2}$, ..., $x_{n-1} = e_{i_{n-1} i_n}$, $x_n = x e_{i_1}$. Por el Lema 4.13 tenemos

$$\sum_{j=2}^{n-1} e_{i_j i_n} x e_{i_1 i_j} + x e_{i_1 i_n} + \sum_{j=1}^{n-1} (-1)^j f'(x e_{i_1 i_j}) e_{i_j i_n} \in IR'$$

de donde, multiplicando por $e_{i_n i_1}$ por la derecha, obtenemos:

$$x e_{i_1} + \sum_{j=1}^{n-1} (-1)^j f'(x e_{i_1 i_j}) e_{i_j i_n} \in IR'.$$

Por consiguiente, $x e_{i_1} \in S + IR'$ y, de este modo tenemos $R' = S + IR'$. Finalmente, como I es nilpotente, tenemos $R' = S$, es decir que R' es un álgebra de matrices de dimensión n^2 sobre $A'_{\mathfrak{m}}$. Por consiguiente, $R \otimes A_{\mathfrak{m}}$ es un álgebra de Azumaya, puesto que se vuelve isomorfa a un álgebra de matrices tras una extensión fielmente plana de escalares [8, Chapitre III, théorème 6.6].

Hemos probado de este modo que para todo ideal maximal $\mathfrak{m}$ de A, la $A_{\mathfrak{m}}$-álgebra $R \otimes A_{\mathfrak{m}}$ es un álgebra de Azumaya de rango n^2. Por lo tanto, R es un álgebra de Azumaya de rango n^2 sobre A.

Para la última parte del Teorema podemos suponer que R es un álgebra de Azumaya sobre A de rango n^2 y que f es una pseudo-representación fiel de R. Entonces, siendo también Σ una A-álgebra de Azumaya de rango n^2, $\rho : R \longrightarrow \Sigma$ es inyectiva, puesto que $\mathrm{Trd}(\rho) = f$ es fiel.

Ahora, por [8, Chapitre III, corollaire 5.3], tenemos que para todo A-monomorfismo φ entre dos álgebras de Azumaya Σ_1 y Σ_2 de igual rango,

$$\begin{array}{ccc} \varphi(\Sigma_1) \otimes (\Sigma_2)^{\varphi(\Sigma_1)} & \longrightarrow & \Sigma_2 \\ a \otimes b & \longmapsto & ab \end{array}$$

es un isomorfismo; y como $(\Sigma_2)^{\varphi(\Sigma_1)} = Z(\Sigma_2) = A$, obtenemos que $\varphi(\Sigma_1) = \Sigma_2$, es decir, que φ es un isomorfismo. De este modo queda probado el Teorema. □

En el caso particular en que A es un anillo local henseliano, se obtiene el siguiente corolario, que fue probado (de forma no constructiva) por L. Nyssen en [10] en respuesta a una cuestión de J. - P. Serre:

Corolario 6.12. *Sea A un anillo local henseliano de cuerpo residual K y sea f una pseudo-representación de R tal que la pseudo-representación residual $\overline{f}$ de $R \otimes K$ es el caracter de una representación absolutamente irreducible $\overline{\rho}$ de $R \otimes K$ en un álgebra de matrices sobre K. Entonces, el álgebra $R/Ker\hat{f}$ es isomorfa a un álgebra de matrices sobre A y la representación $R \longrightarrow R/Ker\hat{f}$ tiene caracter f y eleva la representación $\overline{\rho}$.*

Veremos a continuación dos corolarios más del Teorema 6.11, cuya demostración podemos encontrar en [14]. En ambos consideramos ρ una representación absolutamente irreducible de R en una A-álgebra de Azumaya Σ de rango n^2.

Corolario 6.13. *Sea ρ' una representación de R en una A-álgebra de Azumaya Σ' de rango n^2. Si ρ y ρ' tienen la misma traza reducida, entonces existe un isomorfismo de $\Sigma \longrightarrow \Sigma'$ que envía ρ a ρ'.*

Corolario 6.14. *Sea A' un subanillo de A tal que todo ideal maximal de A' es de la forma $\mathfrak{m} \cap A'$ donde $\mathfrak{m}$ es un ideal maximal de A. Sea R' una A'-subálgebra de R tal que $R = AR'$. Si $Trd(\rho)(x) \in A$ para todo $x \in R'$, entonces la restricción de ρ a R' es una representación absolutamente irreducible de R' en una A'-álgebra de Azumaya Σ' de rango n^2 tal que $\Sigma' \otimes_{A'} A \cong \Sigma$.*

7. Conclusiones. Aplicación en Teoría de Representaciones

Las pseudo-representaciones son una herramienta importante dentro de la Teoría de Representaciones. Estas, al ser funciones que satisfacen las propiedades formales de la traza de las representaciones, permiten, por ejemplo, recuperar representaciones completamente reducibles a partir de su traza.

Uno de los grandes problemas estudiados en la Teoría de Representaciones es construir y estudiar representaciones de grupos de Galois, y concretamente de $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, el grupo de $\mathbb{Q}$-automorfismos del cuerpo de los números algebraicos $\overline{\mathbb{Q}}$. Además, las representaciones de Galois p-ádicas a menudo se dan en términos de trazas de automorfismos de Frobenius, es decir, de pseudo-representaciones.

Entre los autores que han estudiado este problema se encuentran por ejemplo Shimura, Serre, Carayol, Mazur, Wiles, Taylor y Hida. Una de las estrategias más utilizadas por estos autores para construir representaciones de Galois es el uso de formas modulares y operadores de Hecke. La introducción de las pseudo-representaciones de Wiles y Taylor supone una nueva técnica en esta teoría.

Las pseudo-representaciones fueron utilizadas por Taylor para construir representaciones de Galois asociadas a formas modulares a través de argumentos de congruencia; argumentos que resultan eficaces en los casos en los que el uso directo de la geometría algebraica no es posible. La idea es comenzar con una forma modular f a la que se quiere asociar una representación l-ádica, y encontrar congruencias módulo potencias arbitrariamente grandes de l a otras formas modulares en espacios extendidos por formas a las que se puede asociar una representación l-ádica. Si las formas congruentes con f son formas propias del álgebra de Hecke, no es dificil juntar las representaciones módulo potencias de l para construir la representación l-ádica deseada. Pero esto, en general, es dificil de lograr. Sin embargo, usando pseudo-representaciones se puede probar que es suficiente utilizar congruencias con formas que no son valores propios del álgebra de Hecke. Taylor explica en [15] dicho argumento.

En relación a la Teoría de Deformaciones el uso de pseudo-representaciones en la construcción de representaciones de Galois es relevante en trabajos como [9], en el cual Mazur estudia el posible conjunto de representaciones p-ádicas $\rho' : \mathrm{Gal}(L/\mathbb{Q}) \longrightarrow GL_2(\mathbb{Z}_p)$ que levantan una representación dada $\rho : \mathrm{Gal}(L/\mathbb{Q}) \longrightarrow GL_2(\mathbb{F}_p)$, donde L es una cierta extensión algebraica de $\mathbb{Q}$.

Hida también utiliza en [6] el concepto de pseudo-representación para construir representaciones de Galois $\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(K)$ donde K es el cuerpo residual de un ideal primo P de una cierta álgebra de Hecke.

Referencias

[1] Atiyah, M. F.; Macdonald, I. G. Introduction to commutative algebra. *Addison - Wesley Publishing Co.*, 1969.

[2] Azumaya, G. On maximally central algebras. *Nagoya Math. J. 2* (1951), 119 - 150.

[3] Bourbaki, N. Éléments de mathématique. Àlgèbre. Chapitre 8. Modules et anneaux semi-simples. *Nouveau tirage février*, 1973.

[4] Bourbaki, N. Éléments de mathématique. Algèbre commutative. Chapitres 1 à 4. *Springer, Berlin*, 1985.

[5] Braun, A. On the defining axioms of Azumaya algebras. *J.Algebra* 109 (1987), no. 1, 166-171.

[6] Hida, H. Modular Forms and Galois Cohomology. *Cambridge Studies in Advanced Mathematics, 69. Cambridge University Press*, 2000.

[7] Hida, H. Big Galois representations and p-adic L-functions. *Compos. Math.* 151 (2015), no. 4, 603–664.

[8] Knus, M. A., M. Ojanguren. Théorie de la descente et algèbres d'Azumaya. *Lecture Notes in Mathematics*, Vol 389. Springer - Verlag, Berlin - New York, 1974.

[9] Mazur, B. Deforming Galois representations. Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), 385–437. *Math. Sci. Res. Inst. Publ.*, 16, Springer, New York, 1989.

[10] Nyssen, L. Pseudo-représentations. *Math. Ann.* 306 (1996), no 2., 257-283.

[11] Procesi, C. The invariant theory of $n \times n$ matrices. *Advances in Math.* 19 (1976), 306-381.

[12] Raynaud, M. Anneaux locaux Henséliens. *Lecture Notes in Mathematics* Vol. 169, Springer - Verlag, Berlin - New York, 1970.

[13] Rouquier, R. Caractérisation des caractères et pseudo-caractères, *Journal of Algebra* 180 (1996), no. 2, 571-586.

[14] Serre, J.-P. Linear representations of finite groups. *Graduate Texts in Mathematics*, Vol. 42. Springer - Verlag, New York - Heidelberg, 1977.

[15] Taylor, R. Galois representations associated to Siegel modular forms of low weight. *Duke Math. J.* 63 (1991), no. 2, 281–332.

[16] Wiles, A. On ordinary λ-adic representations associated to modular forms. *Invent. Math.* 94 (1988), no. 3, 529–573.