Teoría de Galois para anillos graduados

Ferrero, Miguel Angel

1969

Tesis presentada para obtener el grado de Doctor en Ciencias Matemáticas de la Universidad de Buenos Aires

UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE CIENCIAS EXACTAS Y NATURALES

TEORIA DE GALOIS PARA ANILLOS GRADUADOS

Miguel A. Ferrero

Tesis presentada para optar al título de Doctor en Ciencias Matemáticas

Año 1969

RESUMEN

En este trabajo se deducen resultados para la teoría de Galois de anillos graduados con parte de grado cero conmutativa y grupo de automorfismos homogéneos de grado cero.

Está dividido en tres capítulos:

I.- Resultados previos.

II.- Sobre teoría de Galois de anillos no conmutativos.

III.- Teoría de Galois para anillos graduados.

En el primer párrafo del capítulo I se deducen algunas propiedades, generalizaciones triviales, de las extensiones separables de anillos no conmutativos.

En el segundo párrafo, se estudian los monoides sobre los cuales se supone dada la graduación, que se denominan monoides admisibles. Un monoide admisible es un submonoide del monoide de los elementos positivos de un grupo totalmente ordenado.

Suponemos ahora, para el resto de esta introducción, que todos los monoides son admisibles. No obstante, algunas propiedades no necesitan de esta hipótesis.

Si $A = \bigoplus_{i\in I} A_i$ es un anillo graduado sobre el monoide I, $M = \bigoplus_{i\in I} M_i$ es un A-módulo a derecha graduado, en el párrafo 3 se demuestra que:

a) Si M es finitamente generado (proyectivo, playo) sobre A, M_o es finitamente generado (respectivamente proyectivo, playo) sobre A_o.

b) Si M es un A-anillo homogéneo (es decir, M es un anillo y existe un homomorfismo homogéneo de grado cero $A \longrightarrow M$) separable (fielmente proyectivo) sobre A, entonces M_o es separable (respectivamente fielmente proyectivo) sobre A_o.

En el párrafo 4 se estudian algunas propiedades de anillos graduados. Se obtiene así el resultado fundamental de este capítulo: "Sean $B \longrightarrow A$ un B-anillo graduado homogéneo con $A_o \subset Z(A)$ (Z(A) es el centro de A), C un B-subanillo homogéneo de A el cual es separable sobre B y $f: C \longrightarrow A$ un homomorfismo homogéneo de grado cero de B-anillos. Entonces $f/C_o = 1_{C_o}$ si y solo si $f = 1_C$". En particular,

si A es B-separable y σ es un automorfismo homogéneo de grado cero de A que deja fijo B, entonces $\sigma/A_o = 1_{A_o}$ si y solo si σ = id. Por lo tanto, si G(A/B) es el grupo de todos los B-automorfismos homogéneos de grado cero de A y $G(A_o/B_o)$ el grupo de todos los B_o-automorfismos de A_o, entonces $G(A/B) \subset G(A_o/B_o)$ por la aplicación $\sigma \longmapsto \sigma/A_o$

En el quinto párrafo se extienden los resultados de Villamayor y Zelinski (Galois theory with infinitely many idempotents), referentes al espectro booleano de un anillo.

El capítulo termina con un teorema sobre separabilidad de álgebras universales: "Si A es un anillo conmutativo, F el funtor álgebra tensorial, simétrica o exterior (más generalmente, un funtor de la categoría de A-módulos en la categoría de A-álgebras graduadas que cumple ciertas condiciones), M un A-módulo y G $\neq$ {id} un grupo de automorfismos de M entonces F(M) no es $F(M)^G$-separable".

En el capítulo II se desarrolla una teoría de Galois de anillos no conmutativos, que generaliza la teoría de Chase, Harrison y Rosenberg (Galois theory and Galois cohomology of commutative rings) para el caso de anillos sin idempotentes.

Si S es un anillo, G un grupo finito de automorfismos de S y $R = S^G$, se considera el caso en que S es Galois sobre R en el sentido de Chase, Harrison y Rosenberg (Galois fuerte). Suponemos que S verifica la condición (H) siguiente:

Para cada familia finita x_i, y_i, en S, $\sum_{i,j} x_i.x_j.y_j.y_i = \sum_i x_i.y_i \Longrightarrow \sum_i x_i.y_i = 0$ ó $\sum_i x_i.y_i = 1$.

Esta condición es mas restrictiva que la no existencia de idempotentes no triviales.

En el párrafo 2 se prueba que, bajo estas suposiciones, S es Galois fuerte sobre R si y solo si S es R-separable.

Para este caso, en el párrafo 3 se deduce el siguiente teorema de Galois: "Si S es Galois fuerte sobre R con grupo G, S verifica (H) y la aplicación traza de S en R es suryectiva, entonces existe una correspondencia biunívoca entre subgrupos de G y subanillos de S que contienen a R y son R-separables".

En el párrafo 4 se estudia cierta conexión de nuestra teoría con la de Miyashita (Finite outer Galois theory of non commutative rings).

Finalmente, en el último párrafo se obtienen propiedades relativas a los homomorfismos, endomorfismos y automorfismos de extensiones de Galois (fuerte). El teorema fundamental establece una representación de los homomorfismos, que generaliza la obtenida para anillos conmutativos por Chase, Harrison y Rosenberg.

En el capítulo tercero se estudia la teoría de Galois de anillos graduados. El primer párrafo contiene resultados introductorios. En el segundo se obtienen propiedades del grupo de automorfismos que mas adelante son mejoradas.

Para lo que sigue se supone siempre que A es un anillo graduado con $A_o \subset Z(A)$ y B es un subanillo de A.

La teoría para anillos sin idempotentes se desarrolla en el párrafo 3. En el cuarto la teoría para anillos con un número finito de idempotentes y el quinto se dedica a los anillos que contienen infinitos idempotentes. El párrafo 6 contiene algunos complementos.

En nuestro caso, A es Galois sobre B, se entiende en el sentido debil: "A es separable sobre B, finitamente generado y proyectivo como B-módulo a derecha y existe un grupo finito F de B-automorfismos homogéneos de grado cero de A tal que $A^F = B$".

Si A no tiene idempotentes no triviales, A es Galois débil sobre B si y solo si A es Galois fuerte sobre B.

Los resultados que se obtienen muestran que la teoría de A sobre B se reduce a la de A_o sobre B_o. En efecto, se prueba que:

1°) A_o es Galois sobre B_o y $A \simeq B \otimes_{B_o} A_o$.

2°) $G(A/B) = G(A_o/B_o)$.

3°) Para cada subgrupo finito H del grupo total G, $A^H \simeq B \otimes_{B_o} A_o^H$.

4°) Valen los teoremas de Galois que caracterizan todos los anillos C tales que $B \subset C \subset A$ y C es B-separable, conocidos para el caso conmutativo(Chase, Harrison y Rosenberg-Villamayor y Zelinski).

5°) Todo subanillo de A que contiene a B y es B-separable, es homogéneo y de la forma $B \otimes_{B_o} C_o$, con $B_o \subset C_o \subset A_o$ y C_o es separable sobre B_o.

6°) Todo automorfismo de A que deja fijo B es homogéneo de grado cero.

Si B no tiene idempotentes, se tiene también el siguiente teorema: "A es débilmente Galois sobre B con grupo G si y solo si existe un subgrupo H de G tal que A es Galois fuerte sobre B con grupo H".

Como es usual, se supone aquí que todos los anillos tienen unidad, todos los módulos son unitarios y los homomorfismos de anillos transforman la unidad en la unidad.

Quiero expresar mi agradecimiento al Profesor Orlando E. Villamayor, quién ha dirigido y alentado la realización de este trabajo. Sin sus valiosas sugerencias el mismo no hubiera existido.

Mi reconocimiento también para los Profesores E. Gentile, M. Harada y A. Micali, por la orientación que me prestaran.

La parte fundamental de este trabajo fué realizada mientras el autor gozaba de una beca otorgada por el Consejo Nacional de Investigaciones Científicas y Técnicas y de una licencia acordada por la Universidad Nacional de Rosario.

Miguel A. Ferrero.

Buenos Aires, Diciembre de 1969.-

CAPITULO I - RESULTADOS PREVIOS

§1.- Anillos separables

La definición de extensión separable para anillos no conmutativos dada en [H-S] es como sigue:

Sea $R \longrightarrow S$ un homomorfismo de anillos (frecuentemente la inclusión, que es el caso considerado en [H-S]).

Entonces S es un R-módulo a ambos lados y el grupo abeliano $S \otimes_R S$ es un S-módulo a ambos lados. Por lo tanto, si S° indica el anillo opuesto de S y Z el anillo de los números enteros, $S \otimes_R S$ es un $S \otimes_Z S^\circ$-módulo a izquierda con producto definido por: $x \otimes y^\circ \in S \otimes_Z S^\circ$, $u \otimes v \in S \otimes_R S$, $(x \otimes y^\circ).(u \otimes v) = x u \otimes v y$.

La multiplicación $\phi: S \otimes_R S \longrightarrow S$ es un S-S-homomorfismo, es decir, es un $S \otimes_Z S^\circ$-homomorfismo. Decimos que S es R-separable si existe un $S \otimes_Z S^\circ$-homomorfismo $\psi: S \longrightarrow S \otimes_R S$ tal que $\phi \circ \psi = id_S$.

Esto es equivalente a la existencia de elementos x_i, y_i $(i = 1, \ldots, m)$ en S tal que $\sum_i x_i y_i = 1$ y $\sum_i x x_i \otimes y_i = \sum_i x_i \otimes y_i x, \forall\, x \in S$, en $S \otimes_R S$.

Si R es un anillo conmutativo y $R \longrightarrow S$ es un homomorfismo de anillos cuya imagen está en el centro de S, entonces S es una R-álgebra. En general diremos que S es un R-anillo si R y S son anillos y $R \longrightarrow S$ es un homomorfismo de anillos.

Un homomorfismo de R-anillos es un homomorfismo de anillos el cual es un R-homomorfismo.

Si $R \subset S$, S es un R-anillo por la inclusión $R \longrightarrow S$. En este caso la separabilidad siempre será referida a esta estructura.

Damos a continuación algunas propiedades de los R-anillos separables, que son generalizaciones simples de las conocidas para álgebras sobre anillos conmutativos.

Traduciendo a nuestro lenguaje las proposiciones 2.4., 2.5. y 2.8. de [H-S] se tienen las siguientes:

Proposición 1.1.- Si $R \longrightarrow T$ es un R-anillo y $T \longrightarrow S$ es un T-anillo:

(1) Si S es R-separable entonces S es T-separable.

(2) Si T es R-separable y S es T-separable entonces S es R-separable.

Proposición 1.2.- Sean $R \longrightarrow S$ y $R \longrightarrow T$ dos R-anillos y $f: S \longrightarrow T$ un homomorfismo suryectivo de R-anillos. Si S es R-separable entonces T es R-separable.

Proposición 1.3.- Sean R un anillo conmutativo, S y T dos R-álgebras (no necesariamente conmutativas). Entonces si S es R-separable, $S \otimes_R T$ es T-separable.

Lema 1.4.- Sean $R \longrightarrow S$ un R-anillo y T un S-S-sumando directo de S. Entonces si S es R-separable, T es R-separable a través de la composición $R \longrightarrow S \xrightarrow{\pi} T$ (donde π es la proyección).

D) En efecto, la proyección $\pi: S \longrightarrow T$ es un homomorfismo suryectivo de R-anillos por lo que basta aplicar la proposición 1.2.

Lema 1.5.- Si R es un anillo y $\phi: R \longrightarrow R \oplus R$ es la aplicación diagonal: $\phi(x) = (x,x), \forall x \in R$, entonces $R \oplus R$ es R-separable.

D) Utilizamos los isomorfismos de $R \oplus R$-módulos a ambos lados:

$(R \oplus R) \otimes_R (R \oplus R) \simeq (R \otimes_R R) \oplus (R \otimes_R R) \oplus (R \otimes_R R) \oplus (R \otimes_R R) \simeq$

$\simeq R \oplus R \oplus R \oplus R$, tal que, $(x,y) \otimes (u,v) \longmapsto (x \otimes u, x \otimes v, y \otimes u, y \otimes v) \longmapsto (x.u, x.v, y.u, y.v)$, donde $R \oplus R$ actúa a izquierda a través de: $(x_1,y_1).(x \otimes u, x \otimes v, y \otimes u, y \otimes v) =$

$= (x_1 x \otimes u, x_1 x \otimes v, y_1 y \otimes u, y_1 y \otimes v)$ y análogamente a derecha.

La multiplicación $\Phi: R \oplus R \oplus R \oplus R \longrightarrow R \oplus R$ es la proyección en los sumandos primero y último como se puede verificar. Por lo tanto el elemento $(1,0,0,1) \in R \oplus R \oplus R \oplus R$ satisface las condiciones de separabilidad.

Proposición 1.6.- Si $R_i \longrightarrow S_i$ $(i = 1, \ldots, n)$ son

R_i-anillos, entonces S_i es R_i-separable para todo i si y solo si $\bigoplus_{i=1}^{n} S_i$ es $\bigoplus_{i=1}^{n} R_i$-separable.

D) Razonando inductivamente, basta suponer n = 2.

Es facil ver que existe un isomorfismo de $S_1 \oplus S_2$-módulos a ambos lados:

$$(S_1 \oplus S_2) \otimes_{R_1 \oplus R_2} (S_1 \oplus S_2) \simeq (S_1 \otimes_{R_1} S_1) \oplus (S_2 \otimes_{R_2} S_2)$$

$(x_1,x_2) \otimes (y_1,y_2) \longmapsto (x_1 \otimes y_1, x_2 \otimes y_2)$, donde $S_1 \oplus S_2$ actúa a la izquierda, en el segundo miembro a través de los primeros factores de $S_1 \otimes_{R_1} S_1$ y $S_2 \otimes_{R_2} S_2$, y a la derecha por los segundos factores.

Consideramos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} (S_1 \oplus S_2) \otimes_{R_1 \oplus R_2} (S_1 \oplus S_2) & \xrightarrow{\Gamma} & (S_1 \otimes_{R_1} S_1) \oplus (S_2 \otimes_{R_2} S_2) \\ & \searrow^{\Phi} \quad \swarrow_{\Phi_1 \oplus \Phi_2} & \\ & S_1 \oplus S_2 & \end{array}$$

donde Γ es el isomorfismo anterior y Φ, Φ_1 y Φ_2 las multiplicaciones.

Si S_i es R_i-separable y $\phi_i : S_i \longrightarrow S_i \otimes_{R_i} S_i$ $(i = 1,2)$ en un $S_i \otimes_Z S_i^o$-homomorfismo tal que $\Phi_i \circ \phi_i = id_{S_i}$, la aplicación $\Gamma^{-1} \circ (\phi_1 \oplus \phi_2) : S_1 \oplus S_2 \longrightarrow (S_1 \oplus S_2) \otimes_{R_1 \oplus R_2} (S_1 \oplus S_2)$ es una $(S_1 \oplus S_2) \otimes_Z (S_1 \oplus S_2)^o$-inversa a derecha de Φ.

Recíprocamente, sea $S_1 \oplus S_2$ separable sobre $R_1 \oplus R_2$ y $\phi : S_1 \oplus S_2 \longrightarrow (S_1 \oplus S_2) \otimes_{R_1 \oplus R_2} (S_1 \oplus S_2)$ es un $(S_1 \oplus S_2)$-homomorfismo a ambos lados tal que $\Phi \circ \phi = id_{S_1 \oplus S_2}$

Si $\pi_i : (S_1 \otimes_{R_1} S_1) \oplus (S_2 \otimes_{R_2} S_2) \longrightarrow S_i \otimes_{R_i} S_i$ es la proyección sobre el i-ésimo sumando $(i = 1,2)$, es fácil comprobar que $\pi_i \circ \Gamma \circ \phi / S_i : S_i \longrightarrow S_i \otimes_{R_i} S_i$, es un $S_i \otimes_Z S_i^o$-homomorfismo, el cual es inversa a derecha de Φ_i.

Proposición 1.7.- Si $R \longrightarrow S$ es un R-anillo y $S = \bigoplus_{i=1}^{n} S_i$ es una suma directa de S-submódulos biláteros, S es R-separable si y solo si S_i es R-separable para $i = 1, \ldots, n$.

D) Si S es R-separable, por el lema 1.4., cada S_i es R-separable.

Recíprocamente, si S_i es R-separable para todo i, por la proposición anterior $S = \bigoplus_{i=1}^{n} S_i$ es separable sobre $\bigoplus^{n} R$. Además por el lema 1.5., $\bigoplus^{n} R$ es R-separable.

Por lo tanto, utilizando la transitividad de la proposición 1.1., resulta la tesis.

Proposición 1.8.- Sean $R \longrightarrow S$ un R-anillo separable y M un S-módulo a derecha. Entonces si M es R-proyectivo (finitamente generado), M es S-proyectivo (finitamente generado).

D) Sean $m_i \in M$, $\phi_i \in \mathrm{Hom}_R(M,R)$, $i \in I$, las coordenadas proyectivas de M y $\phi : C \longrightarrow S \otimes_R S$ el S-homomorfismo bilátero tal que $\Phi \circ \phi = id_S$ (donde Φ es la multiplicación $S \otimes_R S \longrightarrow S$).

Sea Ψ_i la aplicación de M es S, definida por la composición siguiente:

$$M \simeq M \otimes_S S \xrightarrow{1_M \otimes \phi} M \otimes_S S \otimes_R S \simeq M \otimes_R S \xrightarrow{\phi_i \otimes 1} R \otimes_R S \simeq S$$

Entonces $\Psi_i \in \mathrm{Hom}_S(M,S)$.

Si $\phi(1) = \sum_j x_j \otimes y_j \in S \otimes_R S$, para cada $x \in M$ la familia $\{\Psi_i(x)\} = \{\sum_j \phi_i(x.x_j)\, y_j\}$ es nula salvo un conjunto finito de índices $i \in I$, y se tiene:

$$\sum_i m_i\, \Psi_i(x) = \sum_{i,j} m_i\, \phi_i(x.x_j)\, y_j = \sum_i x.x_j.y_j = x, \text{ lo que}$$

completa la prueba.

§2.- Discusión sobre monoides

Los anillos graduados para los cuales vale la teoría que construiremos, son graduados sobre monoides que verifican ciertas condiciones. En este párrafo caracterizamos estos monoides.

Sea I un monoide aditivo, es decir, en I está definida una operación +, asociativa, conmutativa y con elemento neutro: 0.

Decimos que I verifica la condición (I_1) si se satisface:

$\forall\, x, y$ en I, $x + y = 0 \Longleftrightarrow x = y = 0$

Un monoide I es totalmente ordenado si está dada una relación de orden total $\geq$, compatible con la suma, es decir: $x \geq y \Longrightarrow x + z \geq y + z, \forall\, z \in I$.

Decimos que un monoide totalmente ordenado I verifica (I_2) o (I_3), respectivamente, si:

(I_2): 0 es el primer elemento de I.

(I_3): I es cancelativo: $x + y = x + z \Longrightarrow y = z$.

Un monoide totalmente ordenado que verifica (I_2) e (I_3) se denominará admisible (para nuestra teoría).

Analizamos algunas relaciones simples.

Lema 2.1.- Si I es un monoide totalmente ordenado que verifica (I_2), entonces verifica (I_1).

Las condiciones (I_2) e (I_3) son independientes.

D) Si I verifica (I_2): $x + y = 0$, $x \geq 0 \Longrightarrow 0 = x + y \geq 0 + y = y \Longrightarrow 0 = y = x$.

Sea I el submonoide aditivo de $\mathbb{R}$ (números reales) cuyos elementos son de la forma $n\sqrt{3} - m\sqrt{2}$ con n y m números naturales no negativos. Entonces I verifica (I_3) pero no (I_2).

Finalmente, sea $I' = \{0,1,2,3\}$ con la suma definida por $0 + x = x$, $\forall\, x \in I'$; $x + y = 3, \forall\, x > 0, \forall\, y > 0$. Entonces I' es un monoide totalmente ordenado que verifica (I_2) pero no (I_3).

La recíproca del precedente lema no es válida, como lo muestra el mismo monoide I anterior. En efecto, I satisface (I_1) pero no (I_2).

En particular, el lema 2.1. muestra que todo monoide admisible verifica (I_1).

Lema 2.2.- Sea I un monoide admisible. Entonces si

$x_i \in I$ $(i = 1,\ldots,m)$ y $x = \sum_{i=1}^{n} x_i$ se tiene:

1°) $x \geq x_i$ $(i = 1,\ldots,n)$.

2°) $x = x_k \Longrightarrow x_i = 0$ para todo $i \neq k$.

D) Por inducción basta suponer $n = 2$.

Si $x = x_1 + x_2$ y $x_1 \geq x$ entonces $x = x_1 + x_2 \geq x + x_2$. Pero $x_2 \geq 0$ de donde $x + x_2 \geq x$. Luego $x + x_2 = x \Longrightarrow x_2 = 0 \Longrightarrow x = x_1$.

Los únicos monoides admisibles son caracterizados inmediatamente:

Proposición 2.3.- I es un monoide admisible si y solo si existe un grupo totalmente ordenado G tal que I es un submonoide de G^+ (submonoide de los $x \in G$ tales que $x \geq 0$).

D) Es claro que si G es un grupo totalmente ordenado, todo submonoide de G^+ es un monoide admisible.

Recíprocamente, si I es un monoide admisible definimos en I x I una relación de equivalencia:
$(x,y) \sim (u,v)$ sii $x + v = y + u$, y designamos por $[x,y]$ la clase de (x,y) en $G = I \times I/_{\sim}$.

Entonces la suma $[x,y] + [u,v] = [x + u, y + v]$ y el orden $[x,y] \geq [u,v]$ sii $x + v \geq y + u$, hacen de G un grupo totalmente ordenado tal que $I \subset G^+$ por la aplicación $x \longrightarrow [x,0]$.

Observación Si la condición (I_2) se reemplaza por:

(I_2'): 0 es el último elemento de I, la teoría posterior podrá aplicarse aún. En efecto, basta definir en I el orden opuesto.

§3.- Propiedades hereditarias de módulos graduados

En todo este párrafo, salvo mención expresa en contrario, I designa un monoide que verifica (I_1) y $A = \bigoplus_{i \in I} A_i$ un anillo graduado sobre I.

Proposición 3.1.- Sea $M = \bigoplus_{i \in I} M_i$ un A-módulo a derecha

graduado. Entonces

a) M es finitamente generado sobre $A \Longrightarrow M_o$ es finitamente generado sobre A_o.

b) M es A-proyectivo $\Longrightarrow M_o$ es A_o-proyectivo.

c) M es A-playo $\Longrightarrow M_o$ es A_o-playo.

D) Sean $\pi_M: M \longrightarrow M_o$, $\pi_A: A \longrightarrow A_o$ las proyecciones y $j_M: M_o \longrightarrow M$, $j_A: A_o \longrightarrow A$ las inyecciones.

Observemos que como I verifica (I_1), π_A es un homomorfismo de anillos ya que si $a = \sum_{i \in I} a_i \in A$, $a' = \sum_{j \in I} a'_j \in A$ (donde a_i, a'_j son las componentes homogéneas de grado i y j de a y a' respectivamente), se tiene:

$$\pi_A(a.a') = \sum_{i+j=0} a_i.a'_j = a_o.a'_o = \pi_A(a).\pi_A(a')$$

Por lo tanto M_o es un A-módulo a través de π_A y un cálculo similar muestra que π_M es un A-homomorfismo.

a) Sean $x_1,\ldots,x_r$ los generadores de M sobre A. Para cada $x \in M$ existen $a_1,\ldots,a_r$ en A tal que $x = \sum_{i=1}^{r} x_i\, a_i$. Entonces

$$\pi_M(x) = \sum_{i=1}^{r} \pi_M(x_i)\, a_i = \sum_{i=1}^{r} \pi_M(x_i)\, \pi_A(a_i)$$

Como π_M es suryectiva, la última igualdad muestra que $\pi_M(x_1),\ldots,\pi_M(x_r)$ generan M_o sobre A_o

b) Sean $x_j \in M$, $\phi_j \in \mathrm{Hom}_A(M,A)$, $j \in J$, las coordenadas proyectivas de M sobre A.

Ponemos $\Psi_j = \pi_A \circ \phi_j \circ j_M: M_o \longrightarrow A_o$, para todo $j \in J$ y entonces $\Psi_j \in \mathrm{Hom}_{A_o}(M_o,A_o)$, $\pi_M(x_j) \in M_o$..

Para cada $x \in M_o$, la familia $\{\Psi_j(x)\} = \{\pi_A \circ \phi_j\ (j_M(x))\}$ es nula salvo un subconjunto finito de J y se tiene:

$$\sum_{j \in J} \pi_M(x_j)\ \Psi_j(x) = \sum_{j \in J} \pi_M(x_j)\ \pi_A\left(\phi_j(j_M(x))\right) =$$

$$= \pi_M\Big(\sum_{j \in J} x_j.\phi_j(j_M(x))\Big) = \pi_{M_o} j_M\ (x) = x,$$ lo que prueba que M_o es A_o-proyectivo.

c) Sea N un A_o-módulo a izquierda. Entonces N es un A-módulo a izquierda y existen dos aplicaciones

$M_o \otimes_{A_o} N \xrightarrow{\phi} M \otimes_A N \xrightarrow{\Psi} M_o \otimes_{A_o} N$, tal que $\Psi_o \phi = id_{M_o \otimes_{A_o} N}$. En efecto, basta verificar que $\phi(x \otimes y) = j_M(x) \otimes y, \Psi(u \otimes v) = \pi_M(u) \otimes v$, están bien definidas.

Si N' es otro A_o-módulo y $f: N \longrightarrow N'$ es un A_o-homomorfismo (es también un A-homomorfismo), el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} M \otimes_A N & \xrightarrow{1_M \otimes f} & M \otimes_A N' \\ \Psi \downarrow \uparrow \phi & & \Psi' \downarrow \uparrow \phi' \\ M_o \otimes_{A_o} N & \xrightarrow{1_{M_o} \otimes f} & M_o \otimes_{A_o} N' \end{array}$$

donde ϕ' y Ψ' son las aplicaciones definidas como ϕ y Ψ.

Supongamos que M es A-playo y f es inyectiva. Entonces $1_M \otimes f$ es inyectiva y por lo tanto si $x \in M_o \otimes_{A_o} N$, $(1_{M_o} \otimes f)(x) = 0 \Longrightarrow \phi_o (1_{M_o} \otimes f)(x) = 0 \Longrightarrow (1_M \otimes f)_o \ \phi(x) = 0 \Longrightarrow \phi(x) = 0 \Longrightarrow x = \Psi_o \phi(x) = 0$.

Luego, $1_{M_o} \otimes f$ es inyectiva lo que muestra que M_o es A_o-playo.

Sean A y B dos anillos; decimos que A es un <u>B-anillo homogéneo</u> si $A = \bigoplus_{i \in I} A_i$, $B = \bigoplus_{i \in I} B_i$ son anillos graduados sobre el mismo monoide I (el cuál no necesariamente verifica (I_1)) y el homomorfismo de anillos $\rho : B \longrightarrow A$ es homogéneo de grado cero, es decir, $\rho(B_i) \subset A_i$, para todo $i \in I$.

<u>Proposición 3.2.-</u> Si A es un B-anillo homogéneo entonces,

a) A es B-separable $\Longrightarrow$ A_o es B_o-separable.

b) A es B-fielmente playo a derecha $\Longrightarrow$ A_o es B_o-fielmente playo a derecha.

D) Con la misma notación de la proposición anterior y teniendo en cuenta que I satisface (I_1), es fácil verificar que

Ψ: $A \otimes_B A \longrightarrow A_o \otimes_{B_o} A_o$, definida por

$\Psi(a \otimes a') = \pi_M(a) \otimes \pi_M(a')$, está bien definida y es un A_o-homomorfismo a ambos lados.

Además el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} A \otimes_B A & \xrightarrow{\Psi} & A_o \otimes_{B_o} A_o \\ \downarrow \Phi & & \downarrow \Phi' \\ A & \xrightarrow{\pi_A} & A_o \end{array}$$

, donde Φ y Φ' son las multiplicaciones.

Como A es B-separable, existe $e \in A \otimes_B A$ tal que $a\,e = e\,a$, $\forall\, a \in A$, y $\Phi(e) = 1$. Entonces es fácil comprobar que $e' = \Psi(e) \in A_o \otimes_{B_o} A_o$ satisface las condiciones de separabilidad. Por lo tanto A_o es B_o-separable.

b) Sea A fielmente playo como módulo a derecha sobre B. Designamos con ρ el homomorfismo $B \longrightarrow A$.

Por [B] (cap I, §3, n°5, prop 9) esto es equivalente a: "ρ es inyectivo y el B-módulo a derecha $A/\rho(B)$ es playo".

Por lo tanto, $\rho_o = \rho/_{B_o} : B_o \longrightarrow A_o$ es inyectivo y solo falta probar que el B_o-módulo a derecha $A_o/\rho_o(B_o)$ es playo sobre B_o.

Es claro que $A/\rho(B)$ es un B-módulo a derecha, graduado sobre I, con elementos homogéneos de grado i:

$$(A/\rho(B))_i = \{\bar{a} : a \in A_i\}$$

Además, $A/\rho(B)$ es B-playo y por la proposición anterior $(A/\rho(B))_o$ es B_o-playo. Para completar la prueba basta observar que $(A/\rho(B))_o \simeq A_o/\rho_o(B_o)$

Observación. Las recíprocas de las propiedades anteriores no son ciertas en general. En efecto, basta tomar $I = N$ (monoide de los enteros no negativos), $A = A_o$ un anillo conmutativo y $A_i = 0$ para todo $i \geq 1$.

Si M es un A-módulo consideramos el álgebra tensorial de M: T(M). Entonces $T_o(M) = A_o$ es finitamente generado, proyectivo, separable y fielmente playo sobre A_o. No obstante:

1°) Si $M = A$, $T(M) = A[X]$ no es finitamente generado sobre A y como es proyectivo sobre A, por [V-Z-I] prop. 1.1., no es separable sobre A.

2°) Si M es un A-módulo no proyectivo resulta que $T(M)$ no es A-proyectivo.

3°) Si M no es A-playo, $T(M)$ no es A-playo.

§4.- Algunas propiedades sobre anillos graduados

En el capítulo siguiente desarrollamos una teoría de Galois para anillos no conmutativos que verifican cierta condición. Esta condición aparece en forma bastante natural en los anillos graduados objeto de nuestro estudio. Comenzamos este párrafo discutiendo la misma.

Sea S un anillo. Designamos en lo que sigue con $\mu: S \otimes_Z S^o \longrightarrow S$ la multiplicación. Decimos que S verifica (H) si:

$v \in S \otimes_Z S^o$, $\mu(v) = \mu(v^2) \Longrightarrow \mu(v) = 0$ ó $\mu(v) = 1$.

Equivalentemente, S verifica (H) si para cada familia finita x_i, y_i en S:

$$\sum_{i,j} x_i.x_j.y_j.y_i = \sum_i x_i.y_i \Longrightarrow \sum_i x_i.y_i = 0 \text{ ó } \sum_i x_i.y_i = 1.$$

Si S verifica (H), no tiene idempotentes salvo 0 y 1. En efecto, si $e \in S$ y $e^2 = e$, aplicando la condición para $v = e \otimes 1^o$ se obtiene $e = 0$ ó $e = 1$.

Si S es conmutativo entonces (H) vale si y solo si S no tiene idempotentes no triviales pues, en este caso, μ es un homomorfismo de anillos.

Proposición 4.1.- Sea $A = \bigoplus_{i \in I} A_i$ un anillo graduado sobre un monoide admisible I y suponemos que $A_o \subset Z(A)$ ($Z(A)$ es el centro de A). Si $v \in A \otimes_Z A^o$ satisface $\mu(v) = \mu(v^2)$ entonces $\mu(v) = p_o \in A_o$ es un idempotente.

D) Sea $v = \sum_{j=1}^{p} x_j \otimes y_j^o \in A \otimes_Z A^o$ y suponemos que $x_j = \sum_{i\in I} a_j^i$, $y_1 = \sum_{k\in I} b_1^k$, es la descomposición en componentes homogéneas.

Entonces $v^2 = \sum_{j,1=1}^{p} x_j.x_1 \otimes (y_1.y_j)^c$, de donde $\mu(v^2) = \sum_{j=1}^{p} x_j \left(\sum_{1=1}^{p} x_1.y_1\right)y_j = \sum_{j=1}^{p} x_j\, \mu(v).y_j$. Suponemos que $\mu(v) = \sum_{r\in I} p_r$, es la descomposición en componentes homogéneas. Por hipótesis:

$$\sum_{s\in I} p_s = \sum_{j=1}^{p} x_j \left(\sum_{r\in I} p_r\right)y_j = \sum_{j=1}^{p} \left(\sum_{i,r,k\in I} a_j^i\, p_r\, b_j^k\right)$$

Igualando grados ceros, teniendo en cuenta que I es admisible y $A_o \subset Z(A)$, se tiene,

$$p_o = \sum_{j=1}^{p} a_j^o\, p_o b_j^o = p_o \sum_{j=1}^{p} a_j^o\, b_j^o = p_o^2.$$

Por lo tanto p_o es un idempotente de A_o.

Sea $I' \subset I$ un subconjunto finito tal que $p_s = 0$ para todo $s \notin I'$ y sean $0 < s_1 < s_2 < \ldots < s_m$, los elementos de I'.

Por el lema 2.2., el grado s_1-esimo de $\mu(v^2)$ se obtiene sumando productos de términos de grados menores o iguales de los factores. Por lo tanto, en dicha suma solo pueden aparecer p_o y p_{s_1} (el resto de los términos es nulo) de donde, grado s_1-ésimo de $\mu(v^2) = \sum_{j=1}^{p} \sum_{i+k=s_1} a_j^i\, p_o\, b_j^k +$

$$+ \sum_{j=1}^{p} a_j^o\, p_{s_1}\, b_j^o = 2p_o.p_{s_1},$$ puesto que:

$$\sum_{j=1}^{p} \sum_{i+k=s_1} a_j^i\, b_j^k = p_{s_1}.$$

Como $\mu(v) = \mu(v^2)$ se tiene, $p_{s_1} = 2\, p_o\, p_{s_1}$ y siendo p_o idempotente, $p_o\, p_{s_1} = 2\, p_o\, p_{s_1}$. Por lo tanto $p_o\, p_{s_1} = 0$ de donde sigue que $p_{s_1} = 0$.

Razonando inductivamente supongamos que $p_{s_q} = 0$, $\forall\ q < t$ y entonces:

grado s_t-ésimo de $\mu(v^2) = \sum_{j=1}^{p} \sum_{i+k=s_t} a_j^i . p_o . b_j^s +$

$+ \sum_{j=1}^{p} a_j^o . p_{s_t} . b_j^o = p_{s_t} . p_o .$

Como antes $p_{s_t} . p_o = 0$ de donde $p_{s_t} = 0$ para todo $t = 1, \ldots, m$, lo que completa la prueba.

Corolario 4.2.- Sea $A = \bigoplus_{i \in I} A_i$ un anillo graduado sobre un monoide admisible I con $A_o \subset Z(A)$. Entonces todo idempotente de A está en A_o.

D) Si $e \in A$ es un idempotente, $v = e \otimes 1^o \in A \otimes_Z A^o$ satisface $\mu(v) = \mu(v^2)$. Por lo tanto $e = \mu(v) = p_o \in A_o$.

Corolario 4.3.- Sea $A = \bigoplus_{i \in I} A_i$ un anillo graduado sobre un monoide admisible I con $A_o \subset Z(A)$. Entonces A verifica (H) si y solo si A no tiene idempotentes no triviales si y solo si A_o no tiene idempotentes no triviales.

D) Por el corolario anterior y la observación que precede a la proposición 4.1., solo necesitamos probar que si A no tiene idempotente no triviales, verifica (H).

En efecto, si $v \in A \otimes_Z A^o$ satisface $\mu(v) = \mu(v^2)$, por la porposición 4.1., $\mu(v)$ es un idempotente de A_o y entonces debe ser 0 o 1.

El corolario 4.3. muestra que existen anillos no conmutativos que satisfacen (H). En particular, si A es un anillo conmutativo sin idempotentes, M un A-módulo cualquiera, U el funtor T (álgebra tensorial) o Λ (álgebra exterior), entonces U(M) verifica (H) (notar que U = S-álgebra simétrica- no tiene interés pues en este caso U(S) es conmutativo).

Corolario 4.4.- Sean $A = \bigoplus_{i\in I} A_i$ un anillo sin idempotentes, graduado sobre un monoide admisible I con $A_o \subset Z(A)$ y J un ideal bilátero homogéneo tal que $A_o \cap J = (0)$. Entonces A/J verifica (H).

D) Como J es homogéneo, A/J es graduado sobre I. Además, de $A_o \cap J = (0)$ se deduce que $(A/J)_o = A_o$ no tiene idempotentes. Por lo tanto A/J satisface (H).

Si $R \longrightarrow S$ es un R-anillo, un R-subanillo de S es un subanillo T de S tal que $Im(R \longrightarrow S) \subset T$. Si T es un R-subanillo de S y $f: T \longrightarrow S$, escribiremos en todo lo que sigue, $f = 1_T$ si f es la inclusión de T en S.

Lema 4.5.- Sean $R \longrightarrow S$ un R-anillo, T un R-subanillo de S separable sobre R y $\sum_i x_i \otimes y_i \in T \otimes_R T$ el elemento que satisface las condiciones de separabilidad. Si $f: T \longrightarrow S$ es un homomorfismo de R-anillos, entonces:

a) $x \sum_i x_i f(y_i) = \sum_i x_i f(y_i) f(x), \forall x \in T.$

b) $\sum_i x_i f(y_i) = 1 \Longleftrightarrow f = 1_T.$

c) Si $e_f = \sum_i x_i \otimes (f(y_i))^o \in S \otimes_Z S^o$, entonces

$$\mu(e_f) = \mu(e_f^2)$$

D) Por hipótesis, $\sum_i x.x_i \otimes y_i = \sum_i x_i \otimes y_i.x, \forall x \in T$, en $T \otimes_R T$. Aplicando a esta relación la composición:

$T \otimes_R T \xrightarrow{1\otimes f} T \otimes_R S \xrightarrow{\Phi} S$, donde Φ es la multiplicación, se obtiene:

$x \sum_i x_i f(y_i) = \sum_i x_i f(y_i.x) = \sum_i x_i f(y_i).f(x)$, para todo $x \in T$.

Si $\sum_i x_i.f(y_i) = 1$ entonces para a), $x = f(x)$ para

todo $x \in T$, de donde $f = 1_T$.

Si $f = 1_T$, como $y_i \in T$ se tiene, $\sum_i x_i f(y_i) = \sum_i x_i y_i = 1$.

Finalmente, utilizando a),

$\mu(e_f^2) = \sum_i x_i \sum_j x_j \cdot f(y_j) \cdot f(y_i) = (\sum_i x_i y_i) \cdot \sum_j x_j f(y_j) = \mu(e_f)$.

Corolario 4.6.- Sean $B \longrightarrow A$ un B-anillo homogéneo, graduado sobre un monoide admisible con $A_o \subset Z(A)$ y C un B-subanillo de A el cuál es B-separable. Si $\sum_i x_i \otimes y_i \in C \otimes_B C$ es el elemento que determina la separabilidad y $f: C \longrightarrow A$ es un homomorfismo de B-anillos entonces $\sum_i x_i f(y_i) = p_o \in A_o$ es un idempotente.

D) Por el lema anterior si $e_f = \sum_i x_i \otimes (f(y_i))^o \in A \otimes_Z A^o$, $\mu(e_f) = \mu(e_f^2)$ y de la proposición 4.1. se obtiene: $\sum_i x_i f(y_i) = \mu(e_f) = p_o \in A_o$ es un idempotente.

Proposición 4.7.- Sean $B \longrightarrow A$ un B-anillo homogéneo, graduado sobre un monoide admisible con $A_o \subset Z(A)$ y C un B-subanillo homogéneo de A el cuál es separable sobre B. Si $f: C \longrightarrow A$ es un homomorfismo homogéneo de grado cero de B-anillos, entonces $f/C_o = 1_{C_o}$ si y solo si $f = 1_C$.

D) Sea $\sum_i x_i \otimes y_i \in C \otimes_B C$ el elemento que satisface las condiciones de separabilidad.

Por el corolario anterior, $\sum_i x_i f(y_i) = p_o \in A_o$. Suponiendo que los grados cero de x_i e y_i son x_i^o e y_i^o, respectivamente, como f es homogéneo de grado cero e I es admisible, igualando grados cero en la última igualdad se tiene: $p_o = \sum_i x_i^o f(y_i^o)$.

Si $f/C = 1_C$, como $y_i^o \in C_o$ resulta,

$p_o = \sum_i x_i^o f(y_i^o) = \sum_i x_i^o y_i^o =$ grado cero de $\sum_i x_i \cdot y_i = 1$.

Por lo tanto $\sum_i x_i f(y_i) = 1$ y del lema 4.5. sigue que $f = 1_C$.

Obtenemos ahora uno de los resultados fundamentales. Si $B \longrightarrow A$ es un B-anillo homogéneo, con $G(A/B)$ indicamos el grupo de todos los B-automorfismos homogéneos de grado cero de A, (es decir, de los automorfismos homogéneos de grado cero de A que dejan fijo la imagen de B)y con $G(A_o/B_o)$ el grupo de todos los B_o-automorfismos de A_o. Se tiene entonces el siguiente

Teorema 4.8.- Sea $B \longrightarrow A$ un B-anillo homogéneo separable, graduado sobre un monoide admisible con $A_o \subset Z(A)$. Si σ es un automorfismo homogéneo de grado cero de A que deja fijo la imagen de B entonces,

$$\sigma/_{A_o} = 1_{A_o} \Longleftrightarrow \sigma = id_A$$

Por lo tanto, $G(A/B) \subset G(A_o/B_o)$ por la aplicación $\sigma \longmapsto \sigma/_{A_o}$.

D) La primera parte se obtiene como caso particular de la proposición anterior. Es claro que la aplicación $\sigma \longmapsto \sigma/_{A_o}$ de $G(A/B)$ em $G(A_o/B_o)$ está bien definida y es un homomorfismo de grupos. Por la primera parte también es inyectiva.

Mas adelante obtendremos algunas consecuencias de este teorema.

§5.- El espectro booleano.-

Dado un anillo R, en $\left(P\right)$ se define un anillo de Boole asociado a R cuyos elementos son los idempotentes centrales de R. Las operaciones en este anillo de Boole están definidas por:

$$e \oplus f = e + f - 2.e.f \quad y \quad e \times f = e.f.$$

Si R es conmutativo, se puede utilizar este anillo de Boole para estudiar la teoría de Galois. Este método es usado en [V-Z-II] para el caso en que R tiene infinitos idempotentes.

En el capítulo III, el mismo método nos sirve para estudiar la teoría de Galois de anillos graduados. Para esto, generalizamos ahora los resultados de [V-Z-II].

Teniendo en cuenta que muchos resultados, y aún muchas pruebas, son iguales a los del caso conmutativo, nos referiremos unicamente a los resultados que nos interesan y omitimos o abreviamos las demostraciones. Para mas detalles ver [V-Z-II].

Sea R un anillo y $B(R)$ el anillo de idempotentes centrales de R, definido en [P].

El espectro booleano de R es el espacio X = Spect $B(R)$, cuyos elementos son los ideales primos (equivalentemente maximales) de $B(R)$.

Un elemento $x \in X$ está caracterizado por:

a) Para todo idempotente central e de R, $e \in x$ ó $1-e \in x$ pero no ambas.

b) Si e y f son idempotentes centrales de R entonces $e.f \in x$ si y solo si $e \in x$ ó $f \in x$.

Para cada $x \in X$, $0 \in x$ y $1 \notin x$, el R-ideal R.x es un ideal bilátero propio y todo conjunto finito de elementos del mismo está contenido en R.e, para algún $e \in x$. En particular, $r \in R.x$ si y solo si $r = r.e$ para algún $e \in x$ si y solo si existe $e \in x$ tal que $r.(1-e) = 0$.

Definimos la localización de R en x como el anillo $R_x = R/R.x$. La imagen de $r \in R$ en R_x por la aplicación natural se indica con r_x.

El término 'localización' se justifica por el hecho que R_x puede considerarse como el anillo de fracciones $R \otimes_{Z(R)} S^{-1}Z(R)$, donde S es el sistema multiplicativo de Z(R) cuyos elementos son los 1-e, $e \in x$.

Para un elemento $r \in R$ se tiene $r_x = 0$ si y solo si existe $e \in x$ tal que $r.(1-e) = 0$.

Si M es un R-módulo a derecha y x ε X, cualquier familia finita del submódulo M.x está contenida en M.e para algún e ε x. Por lo tanto, m ε M.x si y solo si existe e ε x tal que m = m.e si y solo si m.(1-e) = 0 para algún e ε x.

Definimos la localización de M en x como el R_x-módulo a derecha $M_x = M/M.x$. La imagen de m ε M por la aplicación natural $M \longrightarrow M_x$, se indica por m_x. El módulo M_x es el módulo de fracciones $M \otimes_{Z(R)} S^{-1} Z(R)$, con S como antes. Además existe un R_x-isomorfismo $M_x \simeq M \otimes_R R_x$. Un elemento m ε M verifica $m_x = 0$ si y solo si existe e ε x tal que m = m.e si y solo si m.(1-e) = 0, para algún e ε x.

Diremos que un R-anillo $R \longrightarrow T$ es <u>bueno</u> si todo idempotente central de R se aplica en el centro de T.

Si ϕ: $R \longrightarrow T$ es un R-anillo bueno y x ε Spect $B(R)$, entonces T_x es un anillo y ϕ induce (por pasaje al cociente) un homorfismo de anillos ϕ_x: $R_x \longrightarrow T_x$ tal que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} R & \xrightarrow{\phi} & T \\ \downarrow & & \downarrow \\ R_x & \xrightarrow{\phi_x} & T_x \end{array}$$

, donde las aplicaciones verticales son canónicas.

Es necesario aclarar que aquí preferimos la definición de la locaclización como un cociente porque si queremos considerar $T_x = T \otimes_R R_x$, debemos tomar como producto en el segundo miembro otro distinto del producto natural, cuando R no es conmutativo.

Si M y N son dos R-módulos a derecha y f: $M \longrightarrow N$ es un R-homomorfismo, existe un R_x-homomorfismo f_x: $M_x \longrightarrow N_x$ tal que el siguiente diagrama es conmutativo

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow & & \downarrow \\ M_x & \xrightarrow{f_x} & N_x \end{array}$$

, donde las aplicaciones verticales son canónicas. La aplicación f_x se obtiene de f por pasaje al cociente y si se consideran los isomorfismos

$M_x \simeq M \otimes_R R_x$ y $N_x \simeq N \otimes_R R_x$, entonces $f_x = f \otimes 1$. Si M y N son dos R-anillos buenos, f_x es un homomorfismo de anillos. (si f lo es).

Notemos que R_x es playo como R-módulo a izquierda y derecha.

Proposición 5.1.- Si M es un R-módulo a derecha y $x \in X$ entonces:

a) M es R-finitamente generado $\Rightarrow$ M_x es R_x-finitamente generado.

b) M es R-proyectivo $\Rightarrow$ M_x es R_x-proyectivo.

c) M es R-playo $\Rightarrow$ M_x es R_x-playo.

d) M es R-fielmente playo $\Rightarrow$ M_x es R_x-fielmente playo.

e) M es R-finitamente presentado $\Rightarrow$ M_x es R_x-finitamente presentado.

Proposición 5.2.- Si $\phi: R \longrightarrow T$ es un R-anillo bueno separable entonces $\phi_x: R_x \longrightarrow T_x$ es separable.

D) Como $T \longrightarrow T_x$ es un homomorfismo suryectivo de R-anillos, por la proposición 1.2., T_x es R-separable. Aplicando la porposición 1.1. a: $R \longrightarrow R_x \longrightarrow T_x$, resulta la tesis.

Proposición 5.3.- Si M y N son dos módulos sobre un anillo conmutativo R, entonces existe un R_x-isomorfismo de módulos: $M_x \otimes_{R_x} N_x \simeq (M \otimes_R N)_x$, tal que para todo $m \in M$, $n \in N$, $m_x \otimes n_x \longleftrightarrow (m \otimes n)_x$.

Si M y N son dos R-álgebras, el isomorfismo es de R-álgebras.

D) En efecto,

$$M_x \otimes_{R_x} N_x \simeq M \otimes_R R_x \otimes_{R_x} N \otimes_R R_x \simeq M \otimes_R N \otimes_R R_x \simeq (M \otimes_R N)_x$$

Lema 5.4.- Sea M un R-módulo a derecha y $x \in X$.

a) Si $P \subset M$ es un subconjunto finito entonces $m_x = 0$, $\forall$ $m \in M$ si y solo si existe $e \in x$ tal que $m.(1-e) = 0$ $\forall$ $m \in P$.

b) Si m y m' están en M entonces $m_x = m'_x$ si y solo si existe $e \in x$ tal que $m.(1-e) = m'.(1-e)$.

Proposición 5.5.- Si M es un R-módulo entonces

a) Si m y m' están en M, $m_x = m'_x$ para cada $x \in X$ si y solo si $m = m'$.

b) Si N es un submódulo de M y $N_x = M_x$, para cada $x \in X$, entonces $N = M$.

Como la prueba de [V-Z-II] utiliza propiedades topológicas de X, no mencionadas aquí, observamos que la misma puede realizarse independientemente.

D) a) Por hipótesis, para todo $x \in X$ existe $e_x \in X$ tal que $m.(1-e_x) = m'.(1-e_x)$. Sea $\underline{p}$ el ideal de $B(R)$ generado por $\{1-e_x : x \in X\}$. Entonces es fácil ver que $\underline{p} = B(R)$, de donde sigue que $1 \in \sum_{i=1}^{n} R.(1-e_{x_i})$, para algunos x_i de X.

Por lo tanto, existen $r_i \in R$ tal que

$1 = \sum_{i=1}^{n} r_i.(1-e_{x_i})$ y entonces,

$$m = \sum_{i=1}^{n} \left[m.(1-e_{x_i})\right].r_i = \sum_{i=1}^{n} \left[m'.(1-e_{x_i})\right].r_i = m'.$$

b) Puesto que $M_x/N_x = (M/N)_x$, si para cada $x \in X$, $N_x = M_x$, entonces $(M/N)_x = 0$ y por a), $M/N = 0$.

Proposición 5.6.- Si $f: M \longrightarrow N$ es un R-homomorfismo de módulos tal que $f_x: M_x \longrightarrow N_x$ sea inyectivo (suryectivo, biyectivo) para todo x de X, entonces f es inyectivo (respectivamente suryectivo, biyectivo).

D) Basta aplicar b) del teorema anterior a Ker(f) e Im(f) respectivamente.

Proposición 5.7.- Sea $R \longrightarrow T$ un R-anillo bueno y $x \in X$. Si $u \in T_x$ es un idempotente, existe un idempotente $v \in T$ tal que $v_x = u$.

Si u es un idempotente central y vale alguna de las siguientes condiciones:

a) x es finito,

b) T es Z(T)-finitamente generado,

c) Todo idempotente de T es central, entonces existe un idempotente central v' ε T tal que $v'_x = u$.

D) Sea w cualquier representante de u. Entonces $(w^2 - w)_x = 0$ y por lo tanto existe un e ε x tal que $(w^2 - w).(1-e) = 0$. Para la primera parte basta tomar $v = w.(1-e)$.

Si todo idempotente de T es central, v lo es.

En general, si u es central, $(t.v-v.t)_x = 0$ para todo t ε T y entonces para cada t ε T existe un e_t ε x tal que $(t\ v-vt).(1-e_t) = 0$.

Si x es finito basta elegir $v' = v.\prod_{e\in x}(1-e)$.

Si T es Z(T)-finitamente generado y $t_1, \ldots, t_p$ son los generadores, basta poner $v' = v.\prod_{i=1}^{p} (1-e_{t_i})$

Corolario 5.8.- Sea R un anillo y x ε X. Si vale alguna de las siguientes condiciones,

a) x es finito,

b) R es finitamente generado sobre Z(R),

c) Todo idempotente de R es central, entonces R_x no tiene idempotentes centrales salvo 0 y 1.

Más aún, en el caso c), R_x no tiene idempotentes no triviales (ver (2.13) de [V-Z-II]).

Corolario 5.9.- Si $A = \bigoplus_{i\in I} A_i$ es un anillo graduado sobre un monoide admisible I con $A_o \subset Z(A)$, entonces para cada x ε Spect $\mathcal{B}(A)$, A_x no tiene idempotentes no triviales.

Proposición 5.10.- Sea $A = \bigoplus_{i\in I} A_i$ un anillo graduado tal que todo idempotente central de A es homogéneo. Entonces si x ε Spect $\mathcal{B}(A)$, A_x es un anillo graduado donde los elementos homogéneos de grado i estan dados por:
$(A_x)_i = A_i/A_i x, \forall\ i \in I$.

Si M es un A-módulo graduado, M_x es un A_x-módulo graduado y $(M_x)_i = M_i/M_i x, \forall\ i \in I$.

Finalmente, si ϕ: $A \longrightarrow B$ es un A-anillo homogéneo bueno, ϕ_x: $A_x \longrightarrow B_x$ es un A_x-anillo homogéneo, donde la graduación de B_x se tiene considerando a B como un A-módulo graduado.

D) Sea e un idempotente central de A. Entonces e es homogéneo y grado (e) = 2.grado (e), de donde $e \in A_o$.

Por lo tanto, si $x \in$ Spect $B(A)$, $x \subset A_o$. Entonces el ideal A.x es homogéneo porque está generado por elementos homogéneos. Resulta que A_x es graduado y $(A_x)_i = A_i/A_i \cap A.x$.

Pero es fácil comprobar que $A_i \cap A.x = A_i.x$ de donde sigue la primera afirmación.

Ahora no hay dificultad para completar la prueba.

Corolario 5.11.- Sean $A = \bigoplus_{i \in I} A_i$ un anillo graduado sobre un monoide admisible I con $A_o \subset Z(A)$, M un A-módulo graduado y $A \longrightarrow B$ un A-anillo homogéneo bueno. Si $x \in$ Spect $B(A)$ entonces $(A_x)_i = A_{i_x}$, $(M_x)_i = M_{i_x}$, $(B_x)_i = B_{i_x}$, $\forall\ i \in I$, donde los segundos miembros indican las localizaciones como A_o- módulos.

D) La hipótesis hace válida la siguiente afirmación: $x \in$ Spect $B(A)$ si y solo si $x \in$ Spect $B(A_o)$, de la cuál, y el corolario anterior, sigue la tesis.

Proposición 5.12.- Sean A un anillo graduado donde todo idempotente central de A es homogéneo, M y N dos A-módulos graduados y f: $M \longrightarrow N$ un A-homomorfismo. Si para cada $x \in$ Spect $B(A)$, f_x: $M_x \longrightarrow N_x$ es homogéneo de grado cero, entonces f es homogéneo de grado cero.

D) Sea $m \in M_i$ y $f(m) = \sum_{j \in I} n_j$ con $n_j \in N_j$, para todo $j \in I$.

Por hipótesis, $f_x(m_x) \in N_{i_x}$. Entonces sigue que $n_{j_x} = 0$ para todo $x \in$ Spect $B(A)$ y para todo $j \neq i$, de donde $n_j = 0$ para $j \neq i$.

§6.- Apéndice - Sobre separabilidad de álgebras universales.-

Sean A un anillo conmutativo, N el monoide de los números naturales, $\underline{mod}_A$ la categoría de los A-módulos y $\underline{Alg}_A$

la categoría de las A-álgebras graduadas sobre N, con morfismos homogéneos de grado cero.

Supongamos que $F: \underline{mod}_A \longrightarrow \underline{Alg}_A$ es un funtor covariante tal que para cada A-módulo M existe una aplicación A-lineal inyectiva $\alpha_M: M \longrightarrow F(M)$ tal que $Im(\alpha_M) \subset F(M)_1$ y si $\phi: M \longrightarrow M'$ es un homomorfismo de módulos, el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} M & \xrightarrow{\phi} & M' \\ {\scriptstyle \alpha_M}\downarrow & & \downarrow{\scriptstyle \alpha_{M'}} \\ F(M) & \xrightarrow{F(\phi)} & F(M') \end{array}$$

Suponemos además que F(M) es generada como álgebra graduada por $Im(\alpha_M) \cup \{1_A\}$. Entonces es claro que $F(M)_o = A$.

Lema 6.1.- Si G es un grupo de automorfismos de M entonces G es un grupo de automorfismos (homogéneos de grado cero) de F(M), por la aplicación $\sigma \longmapsto F(\sigma)$, para cada $\sigma \in G$.

D) Por ser F un funtor, la aplicación $\sigma \longmapsto F(\sigma)$ está bien definida y es un homomorfismo de grupos. Además, si $F(\sigma) = 1_{F(M)}$, por la conmutatividad del diagrama anterior, $\alpha_M \circ \sigma = \alpha_M$. Como α_M es inyectiva resulta $\sigma = 1_M$. Entonces $\sigma \longmapsto F(\sigma)$ es inyectiva.

Si G es un grupo de automorfismos de un anillo A, con A^G denotamos el subanillo de los elementos de A que son invariantes por cada elemento de G.

Teorema 6.2.- Sea $G \neq \{id\}$ un grupo de automorfismos de M. Entonces F(M) no es separable sobre $F(M)^G$.

D) Si F(M) es $F(M)^G$-separable, por el teorema 4.8. cada $\sigma \in G$ induce un automorfismo diferente sobre $F(M)_o = A$. Pero como para cada $\sigma \in G$, $F(\sigma)$ es un A-homomorfismo, se deduce

que $F(\sigma)/_A = id_A$ lo que es un absurdo.

Corolario 6.3.- Si M es un A-módulo tal que $2 \notin Ann(M)$ (Ann(M) es el anulador de M), entonces F(M) no es A-separable.

D) Sea σ el automorfismo de M tal que $\sigma(x) = -x$, para cada $x \in M$. Entonces $G = \{id, \sigma\}$ es un grupo no trivial de automorfismos de M.

Como $A \subset F(M)^G$, si F(M) es A-separable entonces F(M) es $F(M)^G$-separable (prop. 1.1.), lo que contradice el teorema anterior.

Corolario 6.4.- Si M es un A-módulo libre y una base de M sobre A tiene al menos dos elementos, entonces F(M) no es A-separable.

D) La hipótesis permite afirmar que M tiene automorfismos no triviales. La prueba sigue como en el corolario anterior.

Corolario 6.5.- Sea M un A-módulo, P un sumando directo tal que si $M = P \oplus Q$ entonces existe un automorfismo no trivial de Q. (por ejemplo $2 \notin Ann(Q)$). Entonces F(M) no es separable sobre F(P).

D) Observemos primero que como P es sumando directo de M, F(P) se identifica a una subalgebra graduada de F(M).

Sea $\phi : Q \longrightarrow Q$ un automorfismo no trivial y G el grupo de automorfismos de M que dejan fijo P.

Entonces G es no trivial porque $1_D \oplus \phi \in G$.

Además es claro que si $\sigma \in G$, $F(\sigma)$ deja fijo F(P). Por lo tanto $F(P) \subset F(M)^G$ de donde sigue que F(M) no es F(P)-separable.

El siguiente teorema se aplica en particular al álgebra exterior y al algebra Δ.

Teorema 6.6.- Sea M un A-módulo y suponemos que en F(M) se verifica la siguiente condición: para cada par x, y en M, x.y = -y.x. Entonces las siguientes condiciones son equivalentes:

(1) F(M) es central separable sobre A.

(2) M = 0.

D) Si M = 0, F(M) = A es central separable.

Recíprocamente, supongamos que F(M) es central separable.

Por el teorema 2, pag 6, de [C-M],

$Z(T(M)) = F(M)^{\circ} \oplus \left[(0:\ 2M) \cap F(M)^1\right]$, donde

$F(M)^{\circ} = \bigoplus_{q\ \text{par}} F(M)_q$, $F(M)^1 = \bigoplus_{q\ \text{impar}} F(M)_q$, y

$(0:\ 2\ M) = \{u \mid u \in F(M),\ 2.\alpha_M(x).u = 0,\ \ x \in M\}$

Entonces por hipótesis, debe ser $F(M)^{\circ} = A$ y

$(0:\ 2\ M) \cap F(M)^1 = 0$.

Si existe $x \in M$, $x \neq 0$, se tiene $\alpha_M(x) \in F(M)^1$, de donde $\alpha_M(x) \notin (0:\ 2M)$. Por lo tanto existe $m \in M$ tal que $2.\alpha_M(m).\alpha_M(x) \neq 0$ de donde sigue que $2 \notin Ann(M)$. Por el corolario 6.3., F(M) no es A-separable lo que contradice la hipótesis. Entonces M = 0.

CAPITULO II - SOBRE TEORIA DE GALOIS DE ANILLOS NO CONMUTATIVOS

§1.- Introducción

En este capítulo utilizamos con frecuencia la técnica y la notación de [C-H-R].

Sean S un anillo, G un grupo finito de automorfismos de S y $R = S^G$ el subanillo fijo. Decimos que S es una extensión de Galois de R con grupo G (o que S es Galois sobre R con grupo G) si existen x_i, y_i ($i = 1,\dots, n$) en S tal que:

$$\sum_i x_i.\sigma(y_i) = \delta_{1,\sigma} \quad \text{para todo } \sigma \in G.$$

En este caso también se dice que S es Galois fuerte o fuertemente Galois sobre R con grupo G.

Indicamos con $D = D(S,G)$ al producto cruzado de S con G, es decir, al S-módulo libre con base $(u_\sigma)_{\sigma\in G}$, el cuál es un anillo con el producto usual, y con tr la aplicación traza, es decir, la aplicación de S en R definida por $tr(x) = \sum_{\sigma\in G} \sigma(x)$.

$S^\cdot$ denota la estructura de S como módulo a derecha, sobre el anillo mencionado en cada caso.

La aplicación $d: D \longrightarrow Hom_R(S^\cdot, S^\cdot)$, definida por $d(s.u_\sigma)(x) = s.\sigma(x)$, para cada s, x en S y cada σ en G, es un homomorfismo de anillos y S-módulo a ambos lados.

Como en [C-H-R], E designa el conjunto de todas las funciones de G en S. Entonces E es un anillo y un S-módulo a ambos lados de manera obvia. Además, E es suma directa de los S-submódulos $S.v_\sigma(\sigma\in G)$, donde $v_\sigma: G \longrightarrow S$ está definida por $v_\sigma(\tau) = \delta_{\sigma,\tau}$.

Si M es un D-módulo a izquierda y M^G es el R-submódulo cuyos elementos son los $m \in M$ tales que $\mu_\sigma.m = m$, $\forall \sigma\in G$, la aplicación $\omega: S \otimes_R M^G \longrightarrow M$, definida por $\omega(s \otimes m) = s.m$, es un S-homomorfismo.

Si $h: S \otimes_R S \longrightarrow E$, está definida por $h(s \otimes t)(\sigma) = s.\sigma(t)$, entonces h es un S-homomorfismo bilátero, es decir, es un $S \otimes_Z S^{\circ}$-homomorfismo.

§2.- Extensiones de Galois

Las condiciones de la siguiente proposición son las dadas en [C-H-R] para anillos conmutativos. La prueba es una extensión trivial de aquella por lo que la omitimos. La equivalencia entre (a) y (b) está demostrada, para anillos no conmutativos en [K].

Proposición 2.1.- Si S es un anillo, G un grupo finito de automorfismos de S y $R = S^G$, las siguientes condiciones son equivalentes:

(a) S es Galois sobre R con grupo G.

(b) S es finitamente generado y proyectivo como R-módulo a derecha y $d: D \longrightarrow \mathrm{Hom}_R(S^{\cdot}, S^{\cdot})$ es un isomorfismo.

(c) Si M es un D-módulo a izquierda, $\omega: S \otimes_R M^G \longrightarrow M$ es un isomorfismo.

(d) $h: S \otimes_R S \longrightarrow E$ es un isomorfismo.

Por otra parte, es [H-S] se demuestra que si S es Galois sobre R con grupo G, entonces S es R-separable.

Consideramos aquí un caso donde vale la recíproca. La condición (H) mencionada en seguida, es la del párrafo 4 del capítulo I.

Proposición 2.2.- Sean S un anillo que verifica (H), G un grupo finito de automorfismos de S y $R = S^G$. Entonces S es una extensión de Galois de R con grupo G si y solo si S es R-separable.

D) Si S es R-separable y $\sum_i x_i \otimes y_i \in S \otimes_R S$ satisface las condiciones de separabilidad, por el lema 4.5. del capítulo I, para cada $\sigma \in G$ se tiene que,

$e_\sigma = \sum_i x_i \otimes (\sigma(y_i))^\circ \in S \otimes_Z S^\circ$, verifica $\mu(e_\sigma) = \mu(e_\sigma^2)$.

Entonces por hipótesis, $\mu(e_\sigma) = \sum_i x_i.\sigma(y_i)$ es 0 ó 1. Pero por b) del mismo lema, $\sum_i x_i.\sigma(y_i) = 1$ si y solo si $\sigma = id$.

Por lo tanto $\sum_i x_i.\sigma(y_i) = \delta_{1,\sigma}$.

§3.- Un teorema de Galois

Una parte de la siguiente proposición es la proposición 3.4. de [H-S]. El resto es una generalización inmediata del teorema 2 de [C-H-R].

Proposición 3.1.- Sea S una extensión de Galois de R con grupo G, H un subgrupo de G y $T = S^H$. Entonces S es Galois sobre T con grupo H y H es el conjunto de todos los elementos de G que dejan puntualmente fijo T.

Si tr(S) = R, entonces T es R-separable y si además H es normal en G, T es Galois sobre R con grupo G/H.

La hipótesis anterior sobre S, permite probar el teorema recíproco con la misma técnica utilizada en [C-H-R].

Proposición 3.2.- Sea S una extensión de Galois de R con grupo G. Suponemos que S verifica (H) y que tr(S) = R. Si T es un subanillo de S que contiene a R y es R-separable entonces existe un subgrupo H de G tal que $T = S^H$.

D) Sea H el conjunto de los elementos de G tales que su restricción a T es la identidad y $\sum_i x_i \otimes y_i \in T \otimes_R T$ el elemento que satisface las condiciones de separabilidad.

Como en la proposición 2.2., utilizando el lema 4.5. del capítulo I, se tiene:

$$(1)\quad \sum_i x_i.\sigma(y_i) = \begin{cases} 1 & \text{si } \sigma \in H \\ 0 & \text{si } \sigma \notin H \end{cases}$$

Como en [C-H-R] definimos una acción de G en E por $\sigma \in G$, $\tau \in G$, $v \in E$, $\sigma(v)(\tau) = v(\tau\circ\sigma)$. Entonces E^H es el

conjunto de los elementos de E, los cuales son constantes sobre cada clase derecha de H en G.

Siendo S proyectivo como R-módulo a derecha y $h: S \otimes_R S \longrightarrow E$ un isomorfismo, se tienen las invecciones $S \otimes_R T \longrightarrow S \otimes_R S^H \longrightarrow S \otimes_R S \simeq E$, donde la imagen de $S \otimes_R S^H$ está contenida en E^H.

Vamos a mostrar que $S \otimes_R T \longrightarrow E^H$ es suryectiva.

Sea $v \in E^H$ y J una familia de índices tal que $(\sigma_j)_{j\in J}$ contiene un elemento y solo uno, de cada clase derecha de H en G.

Escribimos $z = \sum_{j\in J} \sum_i v(\sigma_j).\sigma_j(x_i) \otimes y_i \in S \otimes_R T$.

Utilizando (1) es fácil ver que $h(z)(\sigma_k) = v(\sigma_k)$, $\forall\, k \in J$. Como h(z) y v son constantes sobre cada clase derecha, sigue que $h(z) = v$.

Entonces $S \otimes_R T \simeq S \otimes_R S^H$ y aplicando $tr \otimes 1$ obtenemos $T = S^H$, lo que completa la prueba.

Las dos proposiciones anteriores dan la siguiente versión del teorema de Galois:

Teorema 3.3.- Sea S Galois osbre R con grupo G. Si S verifica (H) y tr(S) = R, existe una correspondencia biunívoca entre subgrupos de G y subanillos de S que contienen a R y son R-separables, tal que el subgrupo H corresponde al subanillo T si y solo si $T = S^H$.

§4.- Una conexión con [M]

En [C-H-R] se define la noción de automorfismos fuertemente distintos. Miyashita en [M], generaliza al caso no conmutativo. Cuando los anillos en cuestión no tienen idempotentes centrales no triviales, todo par de automorfismos distintos son fuertemente distintos. Por lo tanto, si S verifica (H), G es un grupo finito de automorfismos de S y T es un subanillo de S, $G/_T$ es fuertemente distinto.

La tesis del teorema 3.3. es, en nuestro caso, la misma que la del teorema 2.9. de [M]. La hipótesis allí supone que S es Galois exterior sobre R, es decir, que el centralizador de R en $S(V_S(R))$ es igual al centro de S y que R es un sumando directo de S como R-módulo bilátero. En nuestro caso se pide que S verifique (H) y que R sea un sumando directo de S como R-módulo a derecha (esto es equivalente a tr(S) = R).

Por otra parte, la noción de Galois exterior puede expresarse como sigue.

Un automorfismo σ de S se denomina exterior si

$$a.\sigma(x) = x.a, \forall\ x \in S \Longrightarrow a = 0$$

Tenemos entonces el siguiente,

Lema 4.1.- Si S es un anillo, G un grupo finito de automorfismos de S y $R = S^G$, entonces S es Galois exterior sobre R con grupo G si y solo si S es Galois sobre R con grupo G y G es un grupo de automorfismos exteriores.

D) Sea S una extensión de Galois de R con grupo G.

Si cada $\sigma \in G$, $\sigma \neq 1$, es exterior, entonces $J_\sigma = \{a \in S: a.\sigma(x) = x.a, \forall\ x \in S\} = (0)$ y recíprocamente.

Pero en [M] se observa que esto sucede si y solo si S es Galois exterior sobre R con grupo G.

Es interesante observar como la relación del lema 4.5., capítulo I, parte a), muestra que si G es un grupo de automorfismos exteriores entonces la separabilidad de S sobre R implica que S es Galois sobre R y se tiene así el teorema 1.5. de [M]:

Proposición 4.2.- Si S es un anillo, G un grupo finito de automorfismos exteriores de S y $R = S^G$ entonces las siguientes condiciones son equivalentes:

a) S es Galois sobre R con grupo G.

b) S es R-separable.

Lo que sucede aquí es que G es automáticamente fuertemente distinto. En efecto, si $\sigma, \tau \in G$ y $e \in S$ es un idempotente central de S tal que $\sigma(x).e = \tau(x).e$, para cada $x \in S$ entonces, $\tau^{-1} \circ \sigma(x).\tau^{-1}(e) = \tau^{-1}(e).x$, para cada $x \in S$, de donde sigue que $e = 0$ ó $\sigma = \tau$.

También queremos observar que en el caso de Galois exterior, Z(R) es el anillo fijo de Z(S) por el grupo G/Z(S):

Proposición 4.3.- Sea S Galois exterior sobre R con grupo G. Entonces $Z(R) = Z(S) \cap R$ o lo que es equivalente $Z(S)^G = Z(R)$.

D) En general $Z(S)^G \subseteq Z(R)$. Recíprocamente, $Z(R) \subseteq R \cap V_S(R) = R \cap Z(S) = Z(S)^G$.

Finalmente, utilizando el lema 4.1. se tiene,

Proposición 4.4.- Sean S un anillo, G un grupo finito de automorfismos de S y $R = S^G$. Si Z(S) es Galois sobre Z(R) con grupo G, entonces S es Galois exterior sobre R con grupo G y existe un elemento central c en S tal que tr(c) = 1.

D) De la hipótesis se deduce que S es Galois sobre R con grupo G (ver proposición 5.5) y que existe un elemento central de traza uno.

Sea $\sigma \in G$, $\sigma \neq 1$ tal que $a.\sigma(x) = x.a$, $\forall\ x \in S$.

En particular si x_i, y_i, son los elementos de Z(S) tales que $\sum_i x_i.\sigma(y_i) = \delta_{1,\sigma}$ se tiene:

$$a = \sum_i x_i.y_i.a = \sum_i x_i.a.\sigma(y_i) = a.\sum_i x_i.\sigma(y_i) = 0.$$

§5.- Endomorfismos, automorfismos y homomorfismos

Proposición 5.1.- Sea S una extensión de Galois de R con grupo G. Suponemos que cada R-automorfismo no exterior de S

está en G. Entonces G es el grupo de todos los R-automorfismos de S.

D) Sean x_i, y_i, los elementos de S tales que $\sum_i x_i.\sigma(y_i) = \delta_{1,\sigma}$. La prueba de la proposición 3.3. de [H-S] muestra que el elemento $\sum_i x_i \otimes y_i \in S \otimes_R S$ satisface las condiciones de separabilidad. Entonces por a) del lema 4.5., capítulo I, si τ es un R-automorfismo exterior de S, $\sum_i x_i.\tau(y_i) = 0$.

Sea ahora ρ un R-automorfismo de S que no pertenece a G. Tenemos, $h(\sum_i x_i \otimes \rho(y_i)) = \sum_{\sigma\in G} s_\sigma.v_\sigma$, con $s_\sigma = \sum_i x_i.\sigma\rho(y_i) \in S$.

Como $\sigma\rho$ no está en G, debe ser exterior. Por lo tanto $s_\sigma = 0$ para cada σ y entonces $\sum_i x_i \otimes \rho(y_i) = 0$.

Aplicando $1 \otimes \rho^{-1}$ obtenemos $\sum_i x_i \otimes y_i = 0$, lo que se contradice con $\sum_i x_i.y_i = 1$.

Si notamos con s la aplicación de S en S definida por $x \longmapsto s.x$, para cada s de S, tenemos $s \in \mathrm{Hom}_R(S^\cdot, S^\cdot)$.

Sea S Galois sobre R con grupo G. El isomorfismo $d: D \longrightarrow \mathrm{Hom}_R(S^\cdot, S^\cdot)$ permite escribir $\alpha = \sum_{\sigma\in G} s_\sigma.\sigma$, para cada $\alpha \in \mathrm{Hom}_R(S^\cdot, S^\cdot)$ donde $s_\sigma\sigma$ es la composición en $\mathrm{Hom}_R(S^\cdot, S^\cdot)$.

Análogamente, si $s \in S$ indicamos con s° la aplicación $x \longmapsto x.s$. Entonces $s^\circ \in \mathrm{Hom}_R({}^\cdot S, {}^\cdot S)$ y $s^\circ \in \mathrm{Hom}_R(S^\cdot, S^\cdot)$ si y solo si s está en el centralizador de R en S. Si $s \in S$ y $\alpha \in \mathrm{Hom}_R(S^\cdot, S^\cdot)$ con $s^\circ.\alpha$ denotamos la composición en $\mathrm{Hom}_Z(S, S)$.

Lema 5.2.- Sea S Galois sobre R con grupo G y $\alpha = \sum_{\sigma\in G} s_\sigma.\sigma \in \mathrm{Hom}_R(S^\cdot, S^\cdot)$. Entonces α es un homomorfismo de anillos si y solo si $s^\circ_\sigma.\alpha = s_\sigma.\sigma$, para cada σ en G y $\sum_{\sigma\in G} s_\sigma = 1$.

D) Sigue trivialmente de las equivalencias siguientes:
$\alpha(x.y) = \alpha(x).\alpha(y), \forall\ x \in S, \forall\ y \in S$, si y solo si,
$\sum_{\sigma\in G} s_\sigma.\sigma(x).\sigma(y) = \sum_{\tau\in G}\left[\sum_{\sigma\in G} s_\sigma.\sigma(x)\right].s_\tau.\tau(y), \forall\ x \in S, \forall\ y \in S,$
si y solo si, $\sum_{\sigma\in G} s_\sigma.\sigma(x).u_\sigma = \sum_{\tau\in G}\left[\sum_{\sigma\in G} s_\sigma.\sigma(x)\right].s_\tau.u_\tau,$
para cada $x \in S$.

El siguiente teorema es una generalización del corolario 3.3. de [C-H-R].

Teorema 5.3. Sea S Galois sobre R con grupo G y $\alpha = \sum_{\sigma\in G} s_\sigma.\sigma \in \mathrm{Hom}_R(S^*, S^*)$. Si x_i, y_i $(i = 1, \ldots, n)$, son los elementos de S tales que $\sum_i x_i.\sigma(y_i) = \delta_{1,\sigma}$ y si $e_o = \sum_i \alpha(x_i) \otimes (\sigma(y_i))^\circ \in S \otimes_Z S^\circ$, entonces $s_\sigma = \mu(e_\sigma)$.

Además, si α es un homomorfismo de anillos, cada s_σ está en el centralizador de R en S, $\mu(e_\sigma) = \mu(e_\sigma^2)$, $\mu(e_\sigma.e_\tau)=0$ si $\sigma \neq \tau$ y $\sum_{\sigma\in G} \mu(e_\sigma) = 1$.

Si S verifica (H), G es el conjunto de todos los endomorfismos del anillo S los cuales son R-homomorfismos.

Finalmente, si cada s_σ está en el centro de S y α es un homomorfismo de anillos, $(s_\sigma)_{\sigma\in G}$ es una familia de idempotentes mutuamente ortogonales cuya suma es uno.

D) Siendo que de la relación $\sum_i x_i.\sigma(y_i) = \delta_{1,\sigma}$, se deduce la relación $\sum_i \tau(x_i).\sigma(y_i) = \delta_{\tau,\sigma}$, tenemos:

$$\mu(e_\sigma) = \sum_i \alpha(x_i).\sigma(y_i) = \sum_i \sum_{\tau\in G} s_\tau.\tau(x_i).\sigma(y_i) =$$

$$= \sum_{\tau\in G} s_\tau.\delta_{\tau,\sigma} = s_\sigma.$$

Si α es un homomorfismo de anillos, del lema 5.2. obtenemos que cada s_σ conmuta con R y $\sum_\sigma \mu(e_\sigma) = 1$ (1).

Además,

$$\mu(e_\sigma.e_\tau) = \sum_{i,j} \alpha(x_i).\alpha(x_j).\tau(y_j).\sigma(y_i) = \sum_i \alpha(x_i).s_\tau.\sigma(y_i) =$$

$$= s_\tau.\sum_i \tau(x_i).\sigma(y_i) = \mu(e_\tau).\delta_{\tau,\sigma}$$

Si S verifica (H) y α es un endomorfismo del anillo S, el cual es un R-homomorfismo, $\mu(e_\sigma)$ es 0 ó 1. De (1), al menos uno de los s_σ debe ser igual a 1. Si para $\sigma \neq \tau$, $s_\sigma = s_\tau = 1$ tenemos:

$0 = \mu(e_\sigma.e_\tau) = \sum_i \alpha(x_i).s_\tau.\sigma(v_i) = 1$. Por lo tanto $\alpha = \rho$ para algún $\rho \in G$.

Finalmente, si cada s_σ está en el centro de S, del último lema obtenemos,

$s_\sigma.\sigma(x) = s_\sigma.\alpha(x) = \sum_{\tau \in G} s_\sigma.s_\tau.\tau(x), \forall\ x \in S$, por lo que $s_\sigma.s_\tau = s_\sigma.\delta_{\sigma,\tau}$, lo que completa la prueba.

El siguiente corolario puede ser obtenido como caso particular del teorema 4.1. de [M]. Como consecuencia del teorema anterior y del lema 4.1. tenemos,

Corolario 5.4.- Sea S Galois sobre R con grupo G y $\alpha = \sum_{\sigma \in G} s_\sigma.\sigma \in \mathrm{Hom}_R(S^*, S^*)$ un homomorfismo de anillos. Si G es un grupo de automorfismos exteriores, $(s_\sigma)_{\sigma \in G}$ es una familia de idempotentes centrales mutuamente ortogonales cuya suma es uno.

Proposición 5.5.- Sean S y S' anillos, G un grupo finito de automorfismos de S y S', $f: S \longrightarrow S'$ un homomorfismo de anillos el cual es un G-homomorfismo. Si S es Galois sobre R con grupo G, S' es Galois sobre S'^G con grupo G. Si además, $S'^G = R$ y f es un R-homomorfismo a derecha entonces f es un isomorfismo.

D) Si x_i, y_i están en S y satisfacen $\sum_i x_i.\sigma(y_i) = \delta_{1,\sigma}$, entonces $f(x_i)$, $f(y_i)$, satisfacen la misma relación en S'

Para probar la segunda parte basta definir f': $S' \longrightarrow S$, por $f'(x') = \sum_i x_i.tr\left[f(y_i)x'\right]$, para cada $x' \in S'$. Entonces es fácil comprobar que f' es inversa de f.

Corolario 5.6.- Sean S y S' anillos tales que $S \subset S'$. Suponemos que G es un grupo finito de automorfismos de S', cuya restricción es un grupo de automorfismos de S isomorfo a G y $R = S'^G$. Entonces si S es Galois sobre R con grupo G, $S = S'$.

D) Basta considerar la inclusión $S \longrightarrow S'$ y aplicar el teorema anterior.

Corolario 5.7.- Sean S un anillo, C su centro, G un grupo finito de automorfismos de S tal que G restringido a C es isomorfo a G y suponemos que C es Galois sobre C^G con grupo G. Entonces $S^G \subset C$ si y solo si S es conmutativo.

D) Si $S^G \subset C$ entonces $S^G = C^G$ y del corolario anterior, $S = C$.

CAPITULO III - TEORIA DE GALOIS PARA ANILLOS GRADUADOS

§1.- Introducción y primeros resultados

Decimos que S es fuertemente Galois (ó Galois fuerte) sobre R con grupo G si S es una extensión de Galois de R con grupo G en el sentido del capítulo anterior. Es decir, si S es un anillo (respectivamente anillo graduado), G un grupo finito de automorfismos (respectivamente automorfismos homogéneos de grado cero) de S y $R = S^G$, S es fuertemente Galois sobre R con grupo G si existen x_i, y_i $(i = 1, \ldots, n)$, en S tales que, para cada $\sigma \in G$, $\sum_{i=1}^{n} x_i.\sigma(y_i) = \delta_{1,\sigma}$.

Sea S un anillo (respectivamente anillo graduado) y R un subanillo de S. Entonces S es debilmente Galois (ó Galois débil) sobre R con grupo G si:

a) S es R-separable,

b) S es finitamente generado y proyectivo como módulo a derecha sobre R,

c) G es el grupo de todos los R-automorfismos (respectivamente R-automorfismos homogéneos de grado cero) de S y existe un subgrupo finito F de G tal que $S^F = R$.

En el caso graduado, según el lema siguiente, R debe ser necesariamente un subanillo homogéneo de S. Si S es fuertemente Galois sobre R con grupo G entonces S es debilmente Galois sobre R con grupo $G' \supset G$ (proposición 2.1., capítulo II). Si S es Galois débil sobre R con grupo G, $S^G = R$.

Trabajamos en general con un anillo graduado $A = \bigoplus_{i \in I} A_i$, el cual es un B-anillo sobre un subanillo homogéneo $B = \bigoplus_{i \in I} B_i$. En este caso, salvo mención expresa en contrario, automorfismo significa automorfismo homogéneo de grado cero y grupo de automorfismos, grupo de automorfismos homogéneos de grado cero. Más aún, el grupo G de todos los automorfismos es el grupo de todos los automorfismos homogéneos de grado cero. A veces diremos que G es un grupo homogéneo.

Lema 1.1.- Sean $A = \bigoplus_{i\in I} A_i$ un anillo graduado, G un grupo de automorfismos de A y $B = A^G$. Entonces B es un subanillo homogéneo de A: $B = \bigoplus_{i\in I} B_i$, con $B_i = A_i^G = A^G \cap A_i$, para todo $i \in I$.

D) Como cada $\sigma \in G$ es homogéneo de grado cero se tiene, $\sum_{i\in I} x_i \in B$, $(x_i \in A_i) \iff \forall\ \sigma \in G$, $\sum_{i\in I} \sigma(x_i) = \sum_{i\in I} x_i \iff$

$\iff \forall\ \sigma \in G, \forall\ i \in I$, $\sigma(x_i) = x_i$.

Proposición 1.2.- Sean $A = \bigoplus_{i\in I} A_i$ un anillo graduado, G un grupo finito de automorfismos de A y $B = A^G$. Entonces,

a) Si A_o es fuertemente Galois sobre B_o con grupo G, A es fuertemente Galois sobre B con grupo G.

b) Si el monoide I verifica (I_1) (§2, capítulo I), A es fuertemente Galois sobre B con grupo G si y solo si A_o es fuertemente Galois sobre B_o con grupo G.

D) Si A_o es fuertemente Galois sobre B_o con grupo G, existen elementos x_i^o, y_i^o $(i = 1, \ldots, n)$ en $A_o \subset A$ que satisfacen $\sum_i x_i^o.\sigma(y_i^o) = \delta_{1,\sigma}$, $\forall\ \sigma \in G$, lo que prueba a).

Recíprocamente, sea A fuertemente Galois sobre B con grupo G y $x_i = \sum_{j\in I} x_i^j$, $y_i = \sum_{k\in I} y_i^k$, los elementos de A tales que $\sum_i x_i.\sigma(y_i) = \delta_{1,\sigma}$ (donde x_i^j, v_i^k son las componentes homogéneas de grado j y k de x e y, respectivamente).

Teniendo en cuenta que I verifica (I_1) y que cada σ es homogéneo de grado cero, el grado cero de cada producto $x_i.\sigma(y_i)$ es, $\sum_{j+k=0} x_i^j.\sigma(y_i^k) = x_i^o.\sigma(v_i^o)$. Entonces, por restricción de la última ecuación al grado cero tenemos: $\sum_i x_i^o.\sigma(y_i^o) = \delta_{1,\sigma}$, para todo σ de G.

Probamos ahora que G es un grupo de automorfismos de A_o. Es claro que para cada $\sigma \in G$ se tiene un B_o-automorfismo de A_o: σ/A_o.

Si $\sigma/A_o = 1_{A_o}$, entonces $\sigma(y_i^o) = y_i^o$ para todo $i \in I$.

Por lo tanto, $\delta_{1,\sigma} = \sum_i x_i^o.\sigma(y_i^o) = \sum_i x_i^o.v_i^o = 1$, de donde sigue que $\sigma = 1$.

Finalmente, por el lema 1.1., $B_o = A_o^G$, lo que completa la prueba.

Observación. En la teoría general que construiremos, supondremos que I es un monoide admisible y $A_o \subset Z(A)$. Bajo estas hipótesis, G es un grupo de automorfismos de A_o (es decir, G actúa fielmente sobre A_o) por el teorema 4.8. del capítulo I. Sin embargo, aquí probamos esto sin necesidad de tales hipótesis.

Proposición 1.3.- Sean $A = \bigoplus_{i\in I} A_i$ un anillo graduado sobre un monoide I que verifica (I_1) y $B = \bigoplus_{i\in I} B_i$ un subanillo de A. Si A es debilmente Galois sobre B con grupo G entonces A_o es debilmente Galois sobre B_o con grupo $G(A_o/B_o)$. Si además, I es admisible y $A_o \subset Z(A)$, entonces $G \subset G(A_o/B_o)$.

D) Si A es Galois débil sobre B, por las proposiciones 3.1. y 3.2. del capítulo I, A_o es separable sobre B_o y finitamente generado y proyectivo como B_o-módulo a derecha.

Si H es un grupo finito de B-automorfismos de A tal que $A^H = B$, entonces H induce un grupo finito H' de automorfismos de A_o sobre B_o y por el lema 1.1., $A_o^{H'} = B_o$.

Finalmente, si I es admisible y $A_o \subset Z(A)$, el teorema 4.8., capítulo I, completa la prueba.

Mas adelante veremos que, como en [V-Z-I], la suposición de que A es finitamente generado sobre B en la definición de Galois débil, puede ser suprimida. Además veremos que esta definición es la dada en [V-Z-II], ya que la condición de ser fielmente proyectivo se deduce de las otras.

Por otra parte, probaremos que para anillos graduados sin idempotentes, Galois fuerte es equivalente a Galois débil. Por lo tanto, oportunamente diremos brevemente Galois por Galois débil.

Lema 1.4.- Sean $A = \bigoplus_{i\in I} A_i$ un anillo graduado y G un grupo finito de automorfismos de A que induce un grupo de automorfismos de A_o isomorfo a G. Entonces existe $c \in A$ tal que $tr(c) = 1$ (es decir, $tr(A) = A^G$) si y solo si existe $c_o \in A_o$ tal que $tr(c_o) = 1$. Si además, $A_o \subset Z(A)$, existe un elemento central en A de traza 1 si y solo si existe un elemento en A de traza 1.

D) Basta considerar la restricción de la ecuación $tr(c) = 1$ al grado cero.

La siguiente proposición es bien conocida.

Proposición 1.5.- Sea S fuertemente Galois sobre R con grupo G. Las siguientes condiciones son equivalentes:

a) Existe un elemento c en S tal que $tr(c) = 1$.

b) S es D(S,G)-proyectivo.

c) R es un sumando directo de S como R-módulo a derecha.

Por otra parte, también son equivalentes:

(A) Existe c en el centro de S tal que $tr(c) = 1$.

(B) D(S,G) es separable sobre S.

Observación.- Necesitamos recordar que si $c \in S$ y $tr(c) = 1$, entonces la proyección $\pi: S \longrightarrow R$ está definida por $\pi(x) = tr(c.x)$, para cada $x \in S$.

Corolario 1.6.- Sea $A = \bigoplus_{i\in I} A_i$ un anillo graduado sobre un monoide I que verifica (I_1) con A_o conmutativo y tal que A es fuertemente Galois sobre B con grupo G. Entonces A es D(A,G)-proyectivo, B es un sumando directo de A como B-módulo a derecha y la proyección de A sobre B es homogénea de grado cero. Si además $A_o \subset Z(A)$, entonces D(A,G) es A-separable.

D) Por la proposición 1.2., A_o es fuertemente Galois

sobre B_o con grupo G por lo que existe $c_o \in A_o$ tal que $tr(c_o) = 1$. Aplicando el lema 1.4. y la proposición 1.5., A es D(A,G)-proyectivo y B es un sumando directo de A como módulo a derecha sobre B.

Siendo que la proyección $\pi: A \longrightarrow B$ está definida por $\pi(a) = tr(c_o.a)$, entonces π es homogénea de grado cero.

Si $A_o \subset Z(A)$ existe en A un elemento central de traza 1 y la última parte de la proposición anterior completa la prueba.

Sean $R \longrightarrow S$ un R-anillo bueno, G un grupo de R-automorfismos de S y $x \in$ Spect $B(R)$. Entonces cada $\sigma \in G$ induce un R_x-automorfismo σ_x de S_x. Es claro que $G_x = \{\sigma_x\}_{\sigma \in G}$ es un grupo de R_x-automorfismos de S_x. Si S es graduado y G es homogéneo entonces G_x es homogéneo.

En general vale también el resultado (2.17) de [V-Z-II]. Observamos que la hipótesis que sigue asegura que $R \longrightarrow S$ es un R-anillo bueno y entonces vale la misma prueba de [V-Z-II]:

Lema 1.7.- Sean $R \subset S$ dos anillos tal que todo idempotente central en R es central en S, H un grupo finito de R-automorfismos de S y $x \in$ Spect $B(R)$. Entonces $(S^H)_x = S_x^{H_x}$.

Proposición 1.8.- Sean $R \subset S$ dos anillos tales que todo idempotente central en R es central en S y $x \in$ Spect $B(R)$. Si S es debilmente Galois sobre R, S_x es debilmente Galois sobre R_x.

D) Por las proposiciones 5.1. y 5.2. del capítulo I, S_x es R_x-separable y finitamente generado y proyectivo como R_x-módulo a derecha. Además, si F es un grupo finito de automorfismos de S tal que $S^F = R$, por el lema 1.7., $S_x^{F_x} = (S^F)_x = R_x$, lo que completa la prueba.

Corolario 1.9.- Sean $A = \bigoplus_{i\in I} A_i$ un anillo graduado sobre un monoide admisible I con $A_o \subset Z(A)$, B un subanillo de A tal que A es Galois débil sobre B y $x \in \text{Spect } B(B)$. Entonces A_x es Galois débil sobre B_x en el sentido graduado.

D) Por el corolario 4.2., capítulo I, todo idempotente de A está en A_o. En particular, todo idempotente central de B es central en A. Entonces, por la proposición anterior, A_x es Galois débil sobre B_x.

Por el corolario 5.11. del capítulo I, $B_x \longrightarrow A_x$ es una inclusión de módulos graduados. Además, si F es el grupo finito de B-automorfismos de A tal que $A^F = B$, entonces F_x es un grupo homogéneo tal que $A_x^{F_x} = B_x$, lo que completa la prueba.

§2.- Extensiones de Galois y el grupo de automorfismos.

En este párrafo damos algunos resultados cuyas demostraciones son bien simples y que utilizaremos con frecuencia.

La siguiente proposición extiende a nuestro caso el resultado del teorema 3.5. de [C-H-R].

Proposición 2.1.- Sean $A = \bigoplus_{i\in I} A_i$ un anillo sin idempotentes no triviales, graduado sobre un monoide admisible I con $A_o \subset Z(A)$, G un grupo de automorfismos de A y $B = A^G$. Suponemos que A es B-separable y finitamente generado como módulo a derecha sobre B. Entonces G es finito, A es fuertemente Galois sobre B con grupo G, $G = G(A_o/B_o)$ y además es igual al grupo de todos los B-automorfismos (homogéneos y no homogéneos) de A.

D) Como antes, indicamos con G(A/B) el grupo de todos los B-automorfismos homogéneos de grado cero de A. Entonces por el teorema 4.8., capítulo I,
$G \subset G(A/B) \subset G(A_o/B_o)$.

Pero A_o no tiene idempotentes no triviales, es separable sobre B_o y es finitamente generado como B_o-módulo a

derecha. Además $A_o^G = B_o$ y entonces, por 3.5. de [C-H-R], G es finito, A_o es fuertemente Galois sobre B_o con grupo G y $G = G(A_o/B_o)$.

Por la proposición 1.2., A es fuertemente Galois sobre B con grupo G. Además, como A verifica (H), G es el grupo de todos los B-automorfismos (homogéneos y no homogéneos) de A, (teorema 5.3., capítulo II), lo que completa la prueba.

Corolario 2.2.- Sea $A = \bigoplus_{i\in I} A_i$ un anillo sin idempotentes no triviales, graduado sobre un monoide admisible I con $A_o \subset Z(A)$. Suponemos que A es fuertemente Galois sobre B con grupo G. Entonces todo B-automorfismo de A es homogéneo de grado cero y está en G.

Observación.- Es claro que aquí la expresión todo B-automorfismo de A" se refiere a los automorfismos homogéneos y no homogéneos.

El resultado del corolario anterior será completado más adelante, donde se establece que el mismo vale aún cuando A tiene idempotentes y es debilmente Galois sobre B.

Corolario 2.3.- Sean $A = \bigoplus_{i\in I} A_i$ un anillo sin idempotentes no triviales, graduado sobre un monoide admisible I con $A_o \subset Z(A)$ y B un subanillo de A. Entonces A es fuertemente Galois sobre B con grupo G si y solo si A es debilmente Galois sobre B con grupo G.

D) Es una consecuencia inmediata de las conclusiones del §2 del capítulo II y de la última proposición.

Observación.- Cuando A tiene idempotentes, la hipótesis frecuente es "A es debilmente Galois sobre B". Si A no tiene idempotentes se supone que A es fuertemente Galois sobre B. No obstante, por el corolario anterior podemos suponer en todos los casos que A es debilmente Galois sobre B. Por esta razón diremos que A es Galois sobre B si A es debilmente Galois sobre B y utilizaremos generalmente esta hipótesis.

Corolario 2.4.- Sea $A = \bigoplus_{i\in I} A_i$ un anillo sin idempotentes no triviales, graduado sobre un monoide admisible I con $A_o \subset Z(A)$. Si A es Galois sobre B con grupo G entonces $o(G) = [A_o : B_o]$ ($o(G)$ es el orden de G y $[A_o : B_o]$ el rango de A_o sobre B_o).

D) Por hipótesis, A_o es fuertemente Galois sobre B_o con grupo G y entonces basta aplicar el segundo corolario que sigue al lema 5 de [V].

También se puede extender a nuestro caso el teorema 2. de [V].

Proposición 2.5.- Sean $A = \bigoplus_{i\in I} A_i$ un anillo graduado sobre un monoide admisible I con $A_o \subset Z(A)$, B un subanillo de A tal que A es B-separable y proyectivo como B-módulo a derecha y G un grupo finito de B-automorfismos de A tal que $A^G = B$. Suponemos que A_o tiene rango sobre B_o y que $o(G) = [A_o : B_o]$. Entonces A es fuertemente Galois sobre B con grupo G.

D) Por hipótesis, A_o es Galois sobre B_o en el sentido de [V] y $o(G) = [A_o : B_o]$. Entonces, por el teorema 2 de [V], A_o es fuertemente Galois sobre B_o con grupo G de donde sigue la tesis.

Proposición 2.6.- Sean $A = \bigoplus_{i\in I} A_i$ un anillo graduado sobre un monoide admisible I con $A_o \subset Z(A)$, B un subanillo de A tal que A es B-separable y proyectivo como B-módulo a derecha y $A^G = B$, donde G es el grupo de todos los B-automorfismos de A. Suponemos además que A tiene solo un número finito de idempotentes. Entonces G es finito.

D) Por hipótesis, A_o es B_o-separable, proyectivo y finitamente generado como B_o-módulo (proposición 1.1. de [V-Z-I]) y $A_o^G = B_o$. Entonces $A_o^{G(A_o/B_o)} = B_o$ y por la proposición 1.3. de [V-Z-I], $G(A_o/B_o)$ es finito.

Pero el teorema 4.8., capítulo I, establece que $G \subset G(A_o/B_o)$, lo que completa la prueba.

Observación.- Este resultado será mejorado más adelante donde se prueba que, bajo las mismas hipótesis, $G = G(A_o/B_o)$.

§3.- Anillos sin idempotentes no triviales.

Por el resto del capítulo, salvo mención expresa en contrario, hacemos la siguiente:

Hipótesis.- $A = \bigoplus_{i\in I} A_i$ es un anillo graduado sobre un monoide admisible I, $A_o \subset Z(A)$ y B es un subanillo de A.

Teorema 3.1.- Si A no tiene idempotentes salvo 0 y 1 y es Galois sobre B con grupo G, la correspondencia usual de la teoría de Galois es una correspondencia biunívoca entre subgrupos de G y subanillos C de A tales que $B \subset C$ y C es B-separable. Si H es un subgrupo de G y C un B-subanillo separable de A, las siguientes condiciones son equivalentes:

1°) $C = A^H$

2°) $C_o = A_o^H$ (es decir, C_o corresponde a H por la teoría de $\left[C\text{-}H\text{-}R\right]$).

Todo B-subanillo separable de A es un subanillo homogéneo.

D) Por hipótesis, A_o es fuertemente Galois sobre B_o con grupo G. Entonces por el lema 1.4., $tr(A) = B$. Por otra parte, A verifica (H) y aplicando el teorema 3.3. del capítulo II, se tiene la correspondencia entre subgrupos y subanillos.

Como cada subanillo separable C es igual a A^H para algún subgrupo H de G, C es homogéneo.

Es claro que la condición 1°) implica 2°).

Recíprocamente, si H es el subgrupo tal que $C_o = A_o^H$ (dado por la teoría de $\left[C\text{-}H\text{-}R\right]$) y H' el subgrupo tal que; $C = A^{H'}$ (dado por el teorema 3.3., capítulo II) entonces $H' \subset H$. Si $\sigma \in H$ entonces $\sigma/C_o = 1_{C_o}$. Por la proposición 4.7. del capítulo I, $\sigma/C = 1_C$ de donde sigue que $\sigma \in H'$.

Luego H' = H, lo que prueba la equivalencia entre 1°) y 2°).

Observación.- La correspondencia biunívoca del teorema anterior puede ser obtenida del teorema 2.9. de [M]. En efecto, con el mismo razonamiento de la proposición 4.4. del capítulo II, se deduce que A es Galois exterior sobre B y que existe un elemento central en A de traza 1 (esto es, B es un sumando directo de A como $B \otimes_Z B^o$-módulo).

También utilizando [M], teorema 5.1., podemos obtener:

Teorema 3.2.- Sea A fuertemente Galois sobre B con grupo G. Entonces

a) Para todo subgrupo H de G, $A^H \simeq B \otimes_{B_o} A_o^H$. En particular, $A \simeq B \otimes_{B_o} A_o$.
   Si suponemos además que A no tiene idempotentes no triviales.

b) Las condiciones 1°) y 2°) del teorema 3.1. son equivalentes a $C = B \otimes_{B_o} A_o^H$.

c) Un B-subanillo $C = \bigoplus_{i \in I} C_i$ de A es separable sobre B si y solo si $C = B \otimes_{B_o} C_o$, donde C_o es B_o-separable.

D) la parte a) sigue inmediatamente del teorema 5.1. de [M] y b) es consecuencia directa de a)

Si C_o es B_o-separable y $C = B \otimes_{B_o} C_o$, por la proposición 1.3., capítulo I, C es B-separable.

Recíprocamente, si C es B-separable entonces $C = B \otimes_{B_o} A_o^H$, para algún subgrupo H de G, con $A_o^H = C_o$ lo que completa la prueba.

Observación.- El teorema 3.2., parte a), vale también con la hipótesis "A es debilmente Galois sobre B" como veremos. Con esta misma hipótesis mostraremos también que la parte c) no necesita de la suposición "A no tiene idempotentes no triviales".

Un resultado recíproco del teorema anterior es el siguiente.

Teorema 3.3.- Sean A_o y B_o anillos conmutativos tales que A_o es fuertemente Galois sobre B_o con grupo G y

$B = B_o \oplus (\bigoplus_{i\neq 0} B_i)$ cualquier anillo graduado sobre un monoide admisible con $B_o \subset Z(B)$. Entonces $A = B \otimes_{B_o} A_o$ es un anillo graduado el cual es fuertemente Galois sobre B con grupo homogéneo G y $A_o \subset Z(A)$.

D) Como B y A_o son B_o-álgebras y B_o es sumando directo de B como B_o-módulo, A es graduado y $A_o \subset Z(A)$. Para completar la prueba basta aplicar el teorema 5.2. de [M].

Observación.- El resultado correspondiente para extensiones debilmente Galois, también será establecido más adelante.

§4.- Anillos con un número finito de idempotentes.

Sea G el grupo de todos los B-automorfismos de A. Suponemos que A tiene un número finito de idempotentes y que es Galois sobre B con grupo G.

Si B tiene idempotentes, estos están en B_o por lo que son centrales. Entonces B y A se descomponen en suma directa de anillos, G es producto directo de los grupos de cada sumando de A y, por la proposición 1.6. del capítulo I, cada sumando de A es Galois sobre un sumando de B con grupo total un factor de G. Por otra parte, cada B-subanillo separable de A es suma directa de subanillos separables sobre los sumandos de B (proposición 1.6., capítulo I).

Por lo tanto, como en [V-Z-I] (y puesto que vale la misma observación que allí), para estudiar la teoría de Galois de A sobre B, basta considerar el caso en que B no tiene idempotentes no triviales. Desde ya, suponemos que esto se verifica.

Sea G' el grupo de todos los B_o-automorfismos de A_o. Por la proposición 1.3., A_o es Galois sobre B_o con grupo G' y como B_o no tiene idempotentes salvo 0 y 1, podemos aplicar la proposición 1.3. de [V-Z-I]. Entonces $A \simeq \bigoplus_{i=1}^{n} A_o.e_i$, donde $\{e_i\}$ es el conjunto (finito) de los idempotentes minimales de A_o (y también de A); cada $A_o.e_i$ es Galois sobre B_o; G' es finito y es igual al producto semi-directo del grupo

simétrico de orden n y el producto de los grupos de automorfismos de cada sumando.

Recalcamos que para el resto del párrafo, salvo mención expresa en contrario, suponemos la siguiente:

Hipótesis.- A es Galois sobre B con grupo G y B no tiene idempotentes salvo 0 y 1.

Además, con G' indicamos el grupo de todos los B_o-automorfismos de A_o y $\{e_i\}$ es el conjunto de idempotentes minimales de A_o.

Proposición 4.1.- A es suma directa de los B-subanillos homogéneos $A.e_i$ ($i = 1, \ldots, n$). Cada $A.e_i$ no tiene idempotentes no triviales y es fuertemente Galois sobre B. Finalmente, $G = G'$ es producto semi-directo del grupo simétrico de orden n y el producto de los grupos de automorfismos de cada $A.e_i$ sobre B.

D) Como los idempotentes de A son centrales, podemos comenzar la prueba repitiendo la demostración de la proposición 1.3. de [V-Z-I]. Establecemos así la primera parte y la descomposición de G en producto semi-directo. Resulta además que para cada par i, j, $A.e_i \simeq A.e_j$ y $G_i \simeq G_j$, donde G_i es el grupo de todos los B-automorfismos de $A.e_i$.

Siendo que cada $A.e_i$ verifica (H) y es B-separable, para probar la segunda parte basta mostrar que $(A.e_i)^{G_i} = B$.

Indicamos con B_i la imagen de B por la aplicación canónica $h_i : B \longrightarrow A.e_i$. Entonces $B_i \subset (A.e_i)^{G_i}$.

Si $a \in (A.e_i)^{G_i}$, eligiendo isomorfismos $\alpha_j : A.e_i \longrightarrow A.e_j$, ($j = 1, \ldots, n$), con $\alpha_i = id_{A.e_i}$, se tiene que $c = \sum_{j=1}^{n} \alpha_j(a) \in A^G = B$, y $h_i(c) = a$. Por lo tanto, $a \in B_i$ lo que muestra que $(A.e_i)^{G_i} = B_i$.

Entonces $A.e_i$ es fuertemente Galois sobre B_i con grupo G_i. Por el corolario 1.6., B_i es un sumando directo de $A.e_i$ como B_i-módulo a derecha (es decir, como B-módulo a derecha), de donde sigue que B_i es B-proyectivo a derecha.

Por lo tanto, la sucesión exacta:

$$0 \longrightarrow \text{Ker } h_i \longrightarrow B \xrightarrow{h_i} B_i \longrightarrow 0,$$

se escinde. Luego Ker $h_i = e.B$, donde e es un idempotente de B. Necesariamente $e = 0$ y entonces h_i es inyectivo por lo que $B_i = B$, lo que completa la prueba de la segunda parte.

Finalmente, si G'_i es el grupo de todos los B_o-automorfismos de $A_o.e_i$, por la proposición 2.1., $G_i = G'_i$ para cada i. Entonces $G = G'$.

Proposición 4.2.- La aplicación $B \otimes_{B_o} A_o \longrightarrow A$, definida por $b \otimes a_o \longmapsto b.a_o$, es un B-isomorfismo de anillos graduados.

D) Por la proposición anterior y el teorema 3.2., $A.e_i \simeq B \otimes_{B_o} A_o.e_i$. Entonces,

$A \simeq \bigoplus_{i=1}^{n} A.e_i \simeq B \otimes_{B_o} (\bigoplus_{i=1}^{n} A_o.e_i) \simeq B \otimes_{B_o} A_o$, y el isomorfismo es el de la tesis.

El siguiente teorema se prueba utilizando la técnica de [V-Z-I] (ver 4, §3). No obstante, como allí se usa el concepto de grupoide, damos brevemente una prueba directa que se obtiene como traducción de aquella.

Teorema 4.3.- Para cualquier subgrupo H de G, A^H es B-separable.

D) Definimos una relación de equivalencia en $\{1,2,..,n\}$ por: $i \sim j$ si existe $\sigma \in H$ tal que $\sigma(e_i) = e_j$. Sea J una clase de equivalencia y $e_J = \sum_{i \in J} e_i$. Entonces e_J es un idempotente minimal de A^H y todos los idempotentes minimales de A^H son de esa forma.

Por lo tanto, $A^H = \bigoplus_J A^H.e_J$ y bastará probar que cada $A^H.e_J$ es B-separable.

Sea $i_o \in J$ y para cada $i \in J$ elegimos $\sigma_i \in H$, tal que $\alpha_i = \sigma_i/A.e_{i_o}$ es un isomorfismo de $A.e_{i_o}$ sobre $A.e_i$.

Definimos θ: $A.e_{i_o} \longrightarrow A$, por $\theta(x) = \sum_{i \in J} \alpha_i(x)$. Entonces θ es un B-isomorfismo sobre un subanillo de A (excepto que la unidad de $A.e_{i_o}$ se aplica en una unidad del subanillo que no es unidad de A), tal que $A^H.e_J \subset \mathrm{Im}\theta$.

Sea H_{i_o} el subgrupo de G_{i_o} obtenido por restricción a $A.e_{i_o}$ de los elementos $\sigma \in H$ tales que $\sigma(e_{i_o}) = e_{i_o}$. Por el teorema 3.1., $(A.e_{i_o})^{H_{i_o}}$ es B-separable. Pero la imágen de $(A.e_{i_o})^{H_{i_o}}$ por θ es exactamente $A^H.e_J$. Por lo tanto, $A^H.e_J$ es B-separable.

Proposición 4.4.- B es un sumando directo de A como B-módulo a derecha y la proyección π: $A \longrightarrow B$ es homogénea de grado cero. Para cada subgrupo H de G, $A^H \simeq B \otimes_{B_o} A_o^H$.

D) Como $A_o \supset B_o$ son anillos conmutativos y A_o es proyectivo sobre B_o, el argumento de [V-Z-I] (pág. 729, antes del primer punto) muestra que B_o es un B_o-sumando directo de A_o. Sea π': $A_o \longrightarrow B_o$ la proyección. Entonces $\pi = 1 \otimes \pi'$: $B \otimes_{B_o} A_o \longrightarrow B \otimes_{B_o} B_o = B$, es una proyección homogénea de grado cero de A sobre B.

Sea H un subgrupo de G y ϕ: $B \otimes_{B_o} A_o^H \longrightarrow A^H$, definida por $\phi(b \otimes a_o) = b.a_o$.

Siendo que A^H es B-separable y A es finitamente generado y proyectivo como B-módulo a derecha, por la proposición 1.8. del capítulo I, A es finitamente generado y proyectivo como A^H-módulo a derecha. Además, como A es B-separable, A es A^H-separable. Entonces A es Galois (débil) sobre A^H. Por lo tanto, A^H es un sumando directo de A como A^H-módulo a derecha, con proyección homogénea de grado cero π_1: $A \longrightarrow A^H$ (ver observación posterior), y A_o^H es un sumando directo de A_o como A_o^H-módulo.

La última conclusión muestra que $B \otimes_{B_o} A_o^H$ es un B-sumando directo de $B \otimes_{B_o} A_o \simeq A$, de donde sigue que ϕ es inyectivo, porque se obtiene restringiendo el último isomorfismo al sumando directo.

Si $a \in A^H \subset A \simeq B \otimes_{B_o} A_o$, entonces $a = \sum_i b_i.a_o^i$, con $b_i \in B$ y $a_o^i \in A_o$. Por lo tanto,

$$a = \pi_1(a) = \sum_i \pi_1(a_o^i.b_i) = \sum_i \pi_1(a_o^i).b_i =$$

$$= \phi(\sum_i b_i \otimes \pi_1(a_o^i)) \in \text{Im } \phi,$$ de donde sigue que ϕ es suryectiva, lo que completa la prueba.

Observación: La afirmación de arriba (A^H es sumando directo de A) vale porque la primera parte de la tesis se verifica aún cuando B tiene un número finito de idempotentes. En efecto, si $\{f_i\}$, $(i = 1, \ldots, m)$, es el conjunto de idempotentes minimales de B, entonces $A = \bigoplus_{i=1}^m A.f_i$, $B = \bigoplus_{i=1}^m B.f_i$, cada $A.f_i$ es Galois sobre $B.f_i$ y $B.f_i$ no tiene idempotentes no triviales. Entonces si $\pi_i: A.f_i \longrightarrow B.f_i$ es la proyección homogénea de grado cero, cuya existencia muestra la primera parte del teorema, $\pi = \bigoplus_{i=1}^m \pi_i: A \longrightarrow B$, es una proyección homogénea de grado cero.

Por lo tanto, el resultado puede aplicarse para A^H en lugar de B.

En [V-Z-I] se dice que un subgrupo H de G es gordo si contiene cada automorfismo σ, tal que la restricción de σ a cada $A.e_i$ coincide con la restricción de un elemento de H.

La noción referida a subgrupos de G como grupo de automorfismos de A o de A_o coinciden, por el teorema 4.8. del capítulo I y la conclusión demostrada que establece que $G(A/B) = G(A_o/B_o)$.

Obtenemos ahora para nuestro caso el teorema de Galois de [V-Z-I]. En el enunciado del mismo, subanillo separable significa subanillo separable homogéneo. No obstante, en el párrafo 6 probamos que todo B-subanillo separable de A es homogéneo. Por esta razón preferimos omitir la palabra homogéneo en el enunciado.

Teorema 4.5.- La correspondencia usual de la teoría de Galois es una correspondencia biunívoca entre subgrupos gordos de G y subanillos de A que contienen a B y son B-separables. Si H es un subgrupo gordo de G y C un B-subanillo separable de A, las siguientes condiciones son equivalentes,

1°) $C = A^H$

2°) $C_o = A_o^H$ (es decir, C_o corresponde a H por la teoría de [V-Z-I]).

3°) $C = B \otimes_{B_o} A_o^H$.

En particular, un B-subanillo $C = \bigoplus_{i \in I} C_i$ de A es B-separable si y solo si $C = B \otimes_{B_o} C_o$, donde C_o es B_o-separable.

D) Sea C un B-subanillo separable de A. Entonces C_o es B_o-separable y por el teorema de [V-Z-I], existe un subgrupo gordo H' de G tal que $C_o = A_o^{H'}$.

Por otra parte, sea $H = \{\sigma: \sigma \in G, \sigma/_C = 1_C\}$. Por la proposición 4.7. del capítulo I, para cada $\sigma \in G$, $\sigma \in H$ si y solo si $\sigma \in H'$. Entonces $H = H'$ y se tiene:

$$C \subseteq A^H = B \otimes_{B_o} A_o^H = B \otimes_{B_o} C_o \subseteq C.$$

Por lo tanto, $C = A^H = B \otimes_{B_o} A_o^H = B \otimes_{B_o} C_o$.

Además, si H es un subgrupo gordo de G, por el teorema 4.3. y la proposición 4.4., $A^H = B \otimes_{B_o} A_o^H$ es B-separable, lo que completa la prueba.

§5.- Anillos con infinitos idempotentes

Si A es Galois sobre B, A_o es B_o-separable, finitamente generado y proyectivo como B_o-módulo y existe un grupo finito H de B-automorfismos de A tal que $A_o^H = B_o$. Por otra parte $A_o = B_o \oplus D_o$ como B_o-módulos, de donde sigue que $A_o/B_o = D_o$ es B_o-plavo (mas aún, es B_o-proyectivo). Entonces por [B] (capítulo I, §3, n° 5, proposición 9), A_o es B_o-fiel.

Por lo tanto, A_o es Galois sobre B_o en el sentido dado en [V-Z-II]. En el párrafo siguiente mostramos que también A es Galois sobre B en este mismo sentido, es decir, que A es B-fiel (proposición 6.4.).

Proposición 5.1.- Si A es Galois sobre B con grupo G,

para cada subgrupo finito F de G, $A^F = B \otimes_{B_o} A_o^F$. En particular, $A = B \otimes_{B_o} A_o$.

D) Sea ϕ: $B \otimes_{B_o} A_o^F \longrightarrow A^F$, la aplicación definida por $\phi(b \otimes a_o) = b.a_o$.

Para cada $x \in \text{Spect } B(B_o) = \text{Spect } B(B)$, la teoría del párrafo 4 se aplica a A_x sobre B_x. Entonces $B_x \otimes_{B_{o_x}} A_{o_x}^{F_x} = A_x^{F_x}$.

Como F es finito, del último isomorfismo y el lema 1.7., resulta el isomorfismo $B_x \otimes_{B_{o_x}} (A_o^F)_x = (A^F)_x$, de donde sigue que $(B \otimes_{B_o} A_o^F)_x = (A^F)_x$.

Siendo que el último isomorfismo es ϕ_x, se tiene que para cada $x \in \text{Spect } B(B)$, ϕ_x es un isomorfismo. Luego ϕ es un isomorfismo.

Proposición 5.2.- Si A es Galois sobre B con grupo G, entonces $G = G(A_o/B_o)$.

D) Por el teorema 4.8. del capítulo I, la aplicación $G \longrightarrow G(A_o/B_o)$, tal que $\sigma \longmapsto \sigma/A_o$ es un monomorfismo.

Sea ahora $\tau \in G(A_o/B_o)$. Entonces $1 \otimes \tau$ es un B-automorfismo de A tal que $(1 \otimes \tau)/A_o = \tau$.

Es fácil ver entonces que la aplicación $G(A_o/B_o) \longrightarrow G$, tal que $\tau \longmapsto 1 \otimes \tau$, es inversa de la anterior.

En [V-Z-II] se define la clausura de un subgrupo H de G como el conjunto de todos los B-automorfismos τ de A tales que, para algún conjunto $\{e_i\}$ de idempotentes de A, con $\bigoplus_1 e_i = 1$ (donde $\bigoplus_1 e_i$ es la suma booleana de los e_i), y para cada i, existe un $\sigma_i \in H$ tal que $e_i.\tau = e_i.\sigma_i$ (la notación $e_i.\tau$ y $e_i.\sigma_i$ se interpreta con el significado dado en el párrafo 5, capítulo II).

Si A es Galois sobre B con grupo G, por la proposición anterior y el isomorfismo $A = B \otimes_{B_o} A_o$ (de donde se deduce que si $e_i.\tau/A_o = e_i.\sigma_i/A_o$ entonces $e_i.\tau = e_i.\sigma_i$), resulta

que la clausura de un subgrupo H de G es la misma, considerando a H como un grupo de automorfismos de A o de A_o.

Un subgrupo H es cerrado si coincide con su clausura. Por la observación anterior, la noción de subgrupo cerrado es la misma si se considera al subgrupo como grupo de automorfismos de A o de A_o.

El siguiente teorema de Galois es extensión de (3.8) de [V-Z-II]. Aquí vale la misma observación que precede al teorema 4.5., es decir, subanillo separable significa subanillo separable homogéneo.

Teorema 5.3.- Si A es Galois sobre B con grupo G, la usual correspondencia de la teoría de Galois es una correspondencia biunívoca entre subanillos de A que contienen a B y son B-separables y subgrupos H de G que satisfacen las siguientes condiciones:

a) H es cerrado

b) Para algún subgrupo finito F de H, $A^F = A^H$.

Si H es un subgrupo de G que verifica a) y b) y C es un B-subanillo separable de A, las siguientes condiciones son equivalente,

1°) $C = A^H$

2°) $C_o = A_o^H$ (es decir, C_o corresponde a H por la teoría de [V-Z-II]).

3°) $C = B \otimes_{B_o} A_o^H$

En particular, un B-subanillo $C = \bigoplus_{i \in I} C_i$ de A es B-separable si y solo si $C = B \otimes_{B_o} C_o$, donde C_o es B_o-separable.

D) Sea C un B-subanillo de A que es B-separable y H el grupo de todos los B-automorfismos σ de A tales que $\sigma/C = 1_C$. Por la proposición 4.7., capítulo I,
$H = \{ \sigma : \sigma \in G \text{ y } \sigma/_{C_o} = 1_{C_o} \}$.

Entonces por (3.9 a) y (3.9 c) de [V-Z-II], H es cerrado y existe un subgrupo finito F de H tal que $A_o^F = A_o^H = C_o$. Por lo tanto,
$C \subset A^H \subset A^F = B \otimes_{B_o} A_o^F = B \otimes_{B_o} A_o^H = B \otimes_{B_o} C_o \subset C$, de donde sigue

que $C = A^H = A^F = B \otimes_{B_o} A_o^H$.

Recíprocamente, si H es un subgrupo cerrado de A y F un subgrupo finito de H tal que $A^F = A^H$, por (3.9 b) de [V-Z-II], $A_o^F = A_o^H$ es B_o-separable de donde sigue que $A^H = A^F = B \otimes_{B_o} A_o^F = B \otimes_{B_o} A_o^H$ es B-separable.

Finalmente, aplicando (3.9 d) de [V-Z-II] se tiene: $\{\sigma: \sigma \in G \text{ y } \sigma/_{A^H} = 1_{A^H}\} = \{\sigma : \sigma \in G \text{ y } \sigma/_{A_o^H} = 1_{A_o^H}\} = H$, lo que completa la prueba.

§6.- Algunos complementos

El resultado (3.15) de [V-Z-II] muestra que S es debilmente Galois sobre R si y solo si existe una familia finita $\{e_i\}$ de idempotentes ortogonales de R cuya suma es 1, tal que para cada i, $S.e_i$ es fuertemente Galois sobre $R.e_i$. En particular, si R no tiene idempotentes no triviales, S es debilmente Galois sobre R con grupo G si y solo si existe un subgrupo H de G tal que S es fuertemente Galois sobre R con grupo H.

Probamos ahora este resultado para el caso graduado.

Teorema 6.1.- Si B no tiene idempotentes no triviales, A es separable sobre B y proyectivo como B-módulo a derecha y $A^G = B$, donde G es el grupo de todos los B-automorfismos de A si y solo si existe un subgrupo H de G tal que A es fuertemente Galois sobre B con grupo H.

D) Si A es fuertemente Galois sobre B con grupo H, A es debilmente Galois sobre B con grupo G.

Recíprocamente, sea A separable sobre B y proyectivo como B-módulo a derecha, tal que $A^G = B$. Entonces A_o es debilmente Galois sobre B_o con grupo $G(A_o/B_o)$ y $A_o = \bigoplus_{i=1}^{n} A_o.e_i$, donde $\{e_i\}$ es el conjunto de idempotentes minimales de A_o, y $A_o.e_i$ es Galois fuerte sobre B_o con grupo G_i (el grupo de todos los B_o-automorfismos de $A_o.e_i$).

Repitiendo la prueba de la proposición 4.1. (la hipótesis A finitamente generado sobre B no se utiliza porque

lo anterior asegura que $1 = \sum_{i=1}^{n} e_i$), se deduce que $A.e_i$ es Galois sobre B para cada i. Entonces $A.e_i$ es finitamente generado sobre B de donde sigue que A es finitamente generado sobre B.

Entonces A es debilmente Galois sobre B con grupo G y volviendo a la proposición 4.1. resulta que $G = G(A_o/B_o)$ y G_i es el grupo de todos los B-automorfismos de $A.e_i$.

Para cada $i = 1, \ldots, n$, elegimos un B-isomorfismo $\sigma_i : A\,e_1 \longrightarrow A.e_i$. Definimos un homomorfismo de grupos $\Psi : G_1 \longrightarrow G$, por: $\Psi(\tau)(\sum_{i=1}^{n} a.e_i) = \sum_{i=1}^{n} \sigma_i \circ \tau_o \circ \sigma_i^{-1}(a.e_i)$, para cada $\tau \in G_1$ y cada $a \in A$.

Se puede verificar fácilmente que Ψ es un monomorfismo. Entonces $H' = \psi(G_1)$ es un grupo de B-automorfismos de A, cuyo orden es el orden de G_1.

Definimos ahora $\rho \in G$ por $\rho(\sum_{i=1}^{n} a.e_i) = \sum_{i} \sigma_{i+1} \circ \sigma_i^{-1}(a.e_i)$, para cada $a \in A$ (donde $i + 1$ indica $i + 1 \pmod n$).

Entonces las potencias de ρ forman un subgrupo H'' de G, cuyo orden es n.

Siendo que $H' \cap H'' = \{1\}$, si H es el subgrupo de G generado por $H' \cup H''$, se tiene que $o(H) = n.o(G_1)$.

Por otra parte, se puede ver que $A^H = B$.

Además, como A_o es debilmente Galois sobre B_o y B_o no tiene idempotentes, $[A_o : B_o] = n.o(G_1) = o(H)$. Entonces, por la proposición 2.5., A es fuertemente Galois sobre B con grupo H.

Corolario 6.2.- Si B no tiene idempotentes no triviales, A es debilmente Galois sobre B con grupo G si y solo si existe un subgrupo H de G tal que A es fuertemente Galois sobre B con grupo H.

Contraejemplo.- El corolario anterior no es válido si B tiene idempotentes no triviales. Para ver esto basta restringirnos al grado cero y considerar el caso de anillos conmutativos.

Sean S y R anillos conmutativos donde R tiene un número finito de idempotentes. Entonces es claro que: "S es fuertemente Galois sobre R con grupo G si y solo si para cada idempotente e de R, S.e es fuertemente Galois sobre R.e con grupo G" (ver [Kr.]).

Si S_i es debilmente Galois sobre R_i con grupo G_i, S_i no tiene idempotentes no triviales (i = 1,2) y $[S_1 : R_1] \neq [S_2 : R_2]$ (por corolario del lema 5 de [V], esto implica que $o(G_1) \neq o(G_2)$. En rigor, bastaría pedir que $G_1 \not\simeq G_2$) ; entonces $S_1 \oplus S_2$ es debilmente Galois sobre $R_1 \oplus R_2$ con grupo $G_1 \times G_2$.

Si existe algún subgrupo H de $G_1 \times G_2$ tal que $S_1 \oplus S_2$ es fuertemente Galois sobre $R_1 \oplus R_2$ con grupo H, por la afirmación anterior, S_i es fuertemente Galois sobre R_i con grupo H (i = 1,2), de donde sigue que $G_1 \simeq H \simeq G_2$, lo que es una contradicción.

En el siguiente corolario recalcamos el hecho que la condición "A es finitamente generado como B-módulo" puede ser suprimida como en [V-Z-I].

Corolario 6.3.- Si A es B-separable proyectivo como B-módulo a derecha y para algún grupo finito F de B-automorfismo de A, $A^F = B$, entonces A es debilmente Galois sobre B.

D) Si B no tiene idempotente no triviales basta aplicar el teorema 6.1.

En general, para cada $x \in \mathrm{Spect}\, B(B)$, A_x es B_x-separable, proyectivo como B_x-módulo a derecha y $A_x^{F_x} = B_x$. Como B_x no tiene idempotentes no triviales, A_x es Galois sobre B_x de donde sigue que $A_x \simeq B_x \otimes_{B_{ox}} A_{ox} \simeq (B \otimes_{B_o} A_o)_x$..

Entonces $A \simeq B \otimes_{B_o} A_o$ lo que muestra que A es finitamente generado sobre B.

Por el teorema 6.1. y el teorema 2.9. de [M], todos los B-subanillos separables C de A, tales que G/C es fuertemente distinto son de la forma $C = A^{H'}$ con H' subgrupo de H. No obstante, si H' es un subgrupo de H solo podemos asegurar que $C = A^{H'}$ es B-separable y H/C es fuertemente distinto, pero no que G/C sea fuertemente distinto.

Por otra parte, el teorema 6.1. nos muestra que si B no tiene idempotentes no triviales y A es Galois sobre B con grupo G, existe un subgrupo H de G con $A^H = B$, tal que:

a) $tr_H: A \longrightarrow B$, definida por $tr_H(a) = \sum_{\sigma \in H} \sigma(a)$, es suryectivo,

b) A es D(A,H)-proyectivo y

c) D(A,H) es A-separable

De la condición a) se deduce que A es fielmente proyectivo como B-módulo a derecha. La siguiente proposición muestra que esto sucede aún cuando B tiene idempotentes. Por lo tanto que las definiciones de extensiones de Galois utilizadas en [V-Z-I] y [V-Z-II] son las mismas para nuestro caso y coinciden con la definición de Galois débil usada aquí.

Proposición 6.4.- Si A es Galois sobre B con grupo G, entonces A es fielmente proyectivo como B-módulo a derecha.

D) Si $f: M \longrightarrow N$ es un B-homomorfismo a izquierda tal que $1_A \otimes f: A \otimes_B M \longrightarrow A \otimes_B N$ es inyectivo, siendo que $A \simeq B \otimes_{B_o} A_o$ se tiene que $1_{A_o} \otimes f: A_o \otimes_{B_o} M \longrightarrow A_o \otimes_{B_o} N$ es inyectivo.

Pero por la observación del comienzo del párrafo 5, A_o es B_o-fielmente proyectivo de donde sigue que f es inyectivo.

Teorema 6.5.- Si A es Galois sobre B con grupo G, todo B- subanillo separable de A es un subanillo homogéneo.

D) Sabemos que existe un isomorfismo $\phi: A \longrightarrow B \otimes_{B_o} A_o$. Entonces $A \otimes_B A \simeq (B \otimes_{B_o} A_o) \otimes_B (B \otimes_{B_o} A_o) \simeq B \otimes_B B \otimes_{B_o} A_o \otimes_{B_o} A_o \simeq$ $\simeq (B \otimes_{B_o} A_o) \otimes_{B_o} A_o \simeq A \otimes_{B_o} A_o$, donde $A \otimes_{B_o} A_o$ es un anillo

graduado cuyos elementos homogéneos de grado i están dados por el submódulo $A_i \otimes_{B_o} A_o$.

Si designamos con Ψ: $A \otimes_L A \longrightarrow A \otimes_{B_o} A_o$ el isomorfismo anterior, es fácil ver que si $a \otimes a' \in A \otimes_B A$, $\Psi(a \otimes a') = a \otimes 1.\ \phi(a')$ y si $a \otimes a_o \in A \otimes_{B_o} A_o$ entonces $\Psi^{-1}(a \otimes a_o) = a \otimes a_o \in A \otimes_B A$.

Sea C un B-subanillo separable de A y x_i, y_i elementos en C tales que $e = \sum_i x_i \otimes y_i \in C \otimes_B C$ satisface las condiciones de separabilidad. Indicamos con $i: C \longrightarrow A$ la inclusión. Entonces para cada $x \in C$, $x.(i \otimes i)(e) = (i \otimes i)(e).x$, en $A \otimes_B A$. Por lo tanto,

$$\sum_{i,j} x_i x_j \otimes y_j.y_i = \sum_j x_j \otimes y_j.(\sum_i x_i.y_i) = \sum_j x_j \otimes y_j, \text{ en } A \otimes_B A.$$

Si aplicamos a esta relación el isomorfismo Ψ tenemos,

$$\sum_{i,j} (x_i \otimes 1).(x_j \otimes 1).\phi(y_j).\phi(y_i) = \sum_j (x_j \otimes 1).\phi(y_j).$$

Entonces considerando $v = \sum_i (x_i \otimes 1) \otimes (\phi(y_i))^\circ \in (A \otimes_{B_o} A_o) \otimes_Z (A \otimes_{B_o} A_o)^\circ$, de la última relación sigue que $\mu(v) = \mu(v^2)$ y por la proposición 4.1. del capítulo I, $\mu(v)$ está en $(A \otimes_{b_o} A_o)_o = A_o \otimes_{B_o} A_o$. Por lo tanto $\mu(v) = \sum_j (x_j \otimes 1).\phi(y_j) = \sum_i u_i^\circ \otimes v_i^\circ \in A_o \otimes_{B_o} A_o$.

Aplicando Ψ^{-1} se tiene:

(1) $\sum_j x_j \otimes y_j = \sum_i u_i^\circ \otimes v_i^\circ$, en $A \otimes_B A$, donde u_i°, v_i° están en A_o

Por otra parte, A es finitamente generado y proyectivo como B-módulo a derecha y puesto que $A \simeq B \otimes_{B_o} A_o$, podemos elegir $a_r^\circ \in A_o$, $\phi_r \in \mathrm{Hom}_B(A\cdot, B\cdot)$ $(r = 1, \ldots, n)$, tal que para cada $a \in A$, $a = \sum_r a_r^\circ.\phi_r(a)$, donde ϕ_r es homogéneo de grado cero para $r = 1, \ldots, n$.

Como C es B-separable por la proposición 1.8. del capítulo I, A es finitamente generado y proyectivo como C-módulo a derecha y las coordenadas proyectivas de A sobre C están

dadas por a_r^o, Ψ_r: A $\longrightarrow$ C definida por $\Psi_r(a) = \sum_j \phi_r(a\ x_j).y_j$, donde x_j, y_j son los elementos determinados mas arriba.

Multiplicando la relación (1) a izquierda por a y aplicando $\Phi_o(\phi_r \otimes 1)$, donde Φ: B $\otimes_B$ A $\longrightarrow$ A es la multiplicación se obtiene, $\sum_j \phi_r(a\ x_j).y_j = \sum_i \phi_r(a\ u_i^o).v_i^o$. Entonces para todo a ε A, $\Psi_r(a) = \sum_i \phi_r(a\ u_i^o).v_i^o$, de donde sigue que para todo r, Ψ_r es una aplicación que conserva el grado.

Por lo tanto, si designamos con $C_o = C \cap A_o$, para cada $a_o \varepsilon A_o$ se tiene $a_o = \sum_r a_r^o.\Psi_r(a^o)$, donde Ψ_r/A_o: $A_o \longrightarrow C_o$ es un C_o-homomorfismo. Esto muestra que A_o es C_o-proyectivo y finitamente generado de donde sigue que $A_o = C_o \oplus D_o$ como C_o-módulo.

Sea $c = \sum_{i\varepsilon I} c_i \varepsilon C$. Entonces para cada r, $\Psi_r(c) = \Psi_r(1).c$. Puesto que Ψ_r conserva el grado, $\Psi_r(c_o) = \Psi_r(1).c_o$. Por otra parte, $c_o \varepsilon A_o$ de donde sigue que existen $c_o' \varepsilon C_o$ y $d_o \varepsilon D_o$ tal que $c_o = c_o' + d_o$. Por lo tanto, $\Psi_r(c_o) = \Psi_r(1)c_o = \Psi_r(1)c_o' + \Psi_r(1).d_o$.

Puesto que $\Psi_r(c_o) \varepsilon C_o$ y $\Psi_r(1).c_o' \varepsilon C_o$, $\Psi_r(1).d_o = 0$ para cada r y $0 = \sum_r a_r^o.\Psi_r(1).d_o = 1.d_o$. Entonces $c_o = c_o' \varepsilon C_o$.

Si π: C $\longrightarrow$ A_o es la aplicación definida por $\pi(\sum_{i\varepsilon I} c_i) = c_o$, para cada $\sum_{i\varepsilon I} c_i \varepsilon C$, lo anterior muestra que Im $(\pi) \subset C_o$. En consecuencia, π es un homomorfismo suryectivo de anillos sobre C_o y por la proposición 2.4. de [H-S], C_o es separable sobre $\pi(B) = B_o$.

Sea H el subgrupo de G tal que $C_o = A_o^H$.

Si $\sigma \varepsilon$ H, por el corolario 4.6. del capítulo I, $\sum_i x_i.\sigma(y_i) = p_o \varepsilon A_o$. Teniendo en cuenta que $y_i \varepsilon C$, $y_i^o \varepsilon C_o$ e igualando grados cero, $p_o = \sum_i x_i^o.\sigma(y_i^o) = \sum_i x_i^o.y_i^o = 1$. Entonces $\sum_i x_i\ \sigma(y_i) = 1$ y por el lema 4.5. del capítulo I, $\sigma/C = 1_C$.

Por lo tanto, $C \subset A^H = B \otimes_{B_o} A_o^H = B \otimes_{B_o} C_o \subset C$, de

donde sigue que $C = A^H$ es un subanillo homogéneo.

La teoría de Galois construída solo considera los automorfismos homogéneos de grado cero. No obstante, el corolario 2.2. muestra que no existen automorfismos no homogéneos de A que dejan fijo B, cuando A no tiene idempotentes. Generalizando,

Teorema 6.6.- Si A es Galois sobre B con grupo homogéneo G, todo B-automorfismo de A es homogéneo de grado cero.

D) Suponemos que B no tiene idempotentes no triviales. Sea G' el grupo de todos los B-automorfismos (homogéneos y no homogéneos) de A. Como en la proposición 4.1. y utilizando la misma notación, se demuestra que G' es producto semi-directo del grupo simétrico de orden n y el producto de los grupos de automorfismos (homogéneos y no homogéneos) de cada $A.e_i$ sobre B.

Por el corolario 2.2., el grupo de automorfismos de cada $A.e_i$ sobre B es igual al grupo de automorfismos homogéneos de grado cero de $A.e_i$ sobre B. Entonces G' = G.

En general, si σ es un B-automorfismo cualquiera de A, σ_x es un B_x-automorfismo de A_x, para cada $x \in \text{Spect } B(B)$. Por la primera parte σ_x es homogéneo de grado cero. Entonces, por la proposición 5.12. del capítulo I, σ es homogéneo de grado cero.

Hemos visto que si A es debilmente Galois sobre B con grupo G, $A \simeq B \otimes_{B_o} A_o$ y G actúa a través del segundo factor. Por otra parte, el teorema 3.3. muestra que, para extensiones fuertemente Galois vale el resultado recíproco.

Finalmente, vamos a demostrar este resultado para extensiones debilmente Galois.

Teorema 6.7.- Sean A_o y B_o anillos conmutativos tales que A_o es Galois sobre B_o con grupo G y $B = B_o \oplus (\bigoplus_{i \neq 0} B_i)$ cualquier anillo graduado sobre un monoide admisible con $B_o \subset Z(B)$. Entonces $A = B \otimes_{B_o} A_o$ es un anillo graduado el cual es Galois sobre B

con grupo homogéneo G y $A_o \subset Z(A)$.

D) Supongamos primero que B_o no tiene idempotentes no triviales. Por el teorema 6.1., existe un subgrupo H de G tal que A_o es fuertemente Galois sobre B_o con grupo H. Entonces por el teorema 3.3., $A = B \otimes_{B_o} A_o$ es un anillo graduado el cual es fuertemente Galois sobre B con grupo homogéneo H y $A_o \subset Z(A)$.

Aplicando el corolario 6.2., A es Galois sobre B con grupo homogéneo G'. Pero por la proposición 5.2., G' = G.

En general, $A = B \otimes_{B_o} A_o$ es B-separable y finitamente generado y proyectivo como B-módulo a derecha. Además A es graduado y $A_o \subset Z(A)$.

Sea H el subgrupo finito de G tal que $A_o^H = B_o$. Entonces para cada $x \in \text{Spect } B(B_o)$, $A_{o_x}^{H_x} = B_{o_x}$. Como B_{o_x} no tiene idempotentes no triviales, por la primera parte demostrada, $B_x \otimes_{B_{o_x}} A_{o_x}$ es debilmente Galois sobre B_x de donde sigue que:

$$\left(A^H\right)_x = A_x^{H_x} = \left(B_x \otimes_{B_{o_x}} A_{o_x}\right)^{H_x} = B_x \otimes_{B_{o_x}} A_{o_x}^{H_x} = B_x.$$

Por lo tanto $A^H = B$. Entonces A es Galois sobre B y por la proposición 5.2., el grupo de A sobre B es G.

REFERENCIAS

[B].- N. Bourbaki. Algèbre commutative, capítulo 1 y 2. Hermann, París 1961.

[C-H-R].- S. U. Chase, D. K. Harrison y A. Rosenberg. Galois theory and Galois cohomology of commutative rings. Mem. Amer. Math. Soc. nº 52, 1965.

[C-M] - P. Corsini y A. Micali. Etude de certaines algèbres associatives graduées. Faculté des Sciences, Montpellier, Secrétariat des Mathématiques, public. nº 52, 1968-1969.

[H-S].- K. Hirata y K. Sugano. On semisimple extensions and separable extensions over non commutative rings. J. Math. Soc. Japan, Vol. 18, nº 4, 1966.

[K].- T. Kanzaki. On Galois extension rings. Nagoya Math. J. Vol. 27, nº 1, 1966.

[Kr.].- H. F. Kreimer. A note on the Galois theory of commutative rings. A aparecer.

[M].- Y. Miyashita. Finite outer Galois theory of non commutative rings. J. Fac. Sci. Hokkaido Univ. Ser. I, Vol. XIX, nº 3,4, 1966.

[P].- R. S. Pierce. Modules over commutative regular rings. Mem. Amer. Math. Soc. nº 70, 1967.

[V].- O. Villamayor. Separable algebras and Galois extensions. Osaka J. Math. Vol. 4, nº 1, 1967.

[V-Z-I].- O. Villamayor y D. Zelinsky. Galois theory for rings with finitely many idempotents. Nagoya Math. J. Vol. 27, 1966.

[V-Z-II].- O. Villamayor y D. Zelinsky. Galois theory with infinitely many idempotents. Nagoya Math. J., Vol. 35, 1969.