# Extensiones Galois de anillos

Marco Andrés Farinati*

Buenos Aires, 29-30 de noviembre 2001

# Índice



*Dto. de Matemática, FCEyN UBA - Argentina.

# 1. Generalidades y definición

El objetivo de este curso es el de estudiar la relación entre las propiedades de anillos de invariantes y el contexto Morita existente entre $A^G$ y $A * G$, donde $G$ es un subgrupo finito de automorfismos de anillos de $A$. Veremos que la condición Galois se corresponderá con la equivalencia de categorías de $A^G$-módulos y $A * G$-módulos. Explotaremos ese punto de vista, en particular para el cálculo de invariantes homológicos.

Comenzamos fijando las notaciones. Sea $A$ un anillo (no necesariamente conmutativo) y $G$ un subgrupo finito de automorfismos de anillos de $A$. Hay dos anillos asociados a esos datos:

$$A^G = \{a \in A \ / \ g(a) = a \forall g \in G\}$$

$$A * G = \oplus_{g \in G} A.g$$

La multiplicación de $A^G$ es la inducida por la de $A$ (es decir $A^G$ es un subanillo de $A$), la multiplicación de $A * G$ está definida por

$$(a.g)(b.h) := ag(b).gh \quad a, b \in A, \quad g, h \in G$$

El anillo $A$ es evidentemente un $A^G$-bimódulo, pero además, la multiplicación en $A * G$ está definida de manera tal que la aplicación

$$A * G \to End_{A^G}(A_{A^G})$$

que identifica cada elemento de $A$ con la multiplicación a izquierda por él, y los elementos de $G$ como elementos de $\mathrm{Aut}(A) \subset \mathrm{End}_{A^G}(A)$, sea un morfismo de anillos.

A través de este morfismo de anillos, $A$ es un $A * G$-$A^G$-bimódulo. Más concretamente, si $x \in A$, $b \in A^G$ y $ag$ es un elemento de $A.g$, la estructura de bimódulo de $A$ está dada por la fórmula

$$ag.x.b := ag(x)b = ag(xb)$$

En [C-F-M], Cohen, Fischman y Montgomery pusieron en evidencia la existencia de un contexto Morita "natural" entre $A^G$ y $A * G$. Los bimódulos del contexto son los dos iguales a $A$, pero con estructuras diferentes. La primera ya fue descrita antes, la otra dada por:

$$b.x.ag := bg^{-1}(xa) = g^{-1}(bxa)$$

donde se guardaron las notaciones anteriores, es decir, $x \in A$, $b \in A^G$, $ag \in A.g$.

Un cálculo de rutina es la demostración del lema siguiente:

**Lema 1.1.** *Sea $A$ un anillo, $G$ un subgrupo finito de automorfismos de $A$. Denotamos $\mathrm{tr} : A \to A^G$ al morfismo de traza definido por $\mathrm{tr}(a) = \sum_{g \in G} g(a)$. Entonces, los morfismos siguientes están bien definidos y proveen un contexto de Morita entre $A^G$ y $A * G$:*

$$\begin{aligned} \mathrm{Tr} : A \otimes_{A*G} A &\to A^G \\ (a \otimes b) &\mapsto \mathrm{tr}(ab) \\ \beta : A \otimes_{A^G} A &\to A * G \\ (a \otimes b) &\mapsto \sum_{g \in G} ag(b).g \end{aligned}$$

La pregunta que surge es cuándo este contexto es un equivalencia. La respuesta no es más que una aplicación particular de la teoría de Morita, que recolectamos en la proposición siguiente:

**Proposición 1.2.** *Sea $A$ un anillo, $G$ un subgrupo finito de automorfismos de $A$. Las condiciones siguientes son equivalentes:*

1. *Los funtores $A \otimes_{A^G} -$ y $A \otimes_{A*G} -$ son equivalencias entre las categorías de $A^G$-módulos y $A * G$-módulos. Cada uno de los funtores es quasi-inverso del otro.*

2. *El funtor* $A \otimes_{A*G} - : A^G\text{-}mod \to A*G\text{-}mod$ *es una equivalencia de categorías.*

3. *El funtor* $(-)^G : A*G\text{-}mod \to A^G\text{-}mod$ *es una equivalencia de categorías.*

4. $A_{A^G}$ *es* $A^G$*-proyectivo de tipo finito y* $A^G$*-generador, y el morfismo de estructura* $A*G \to End_{A^G}(A_{A^G})$ *es un isomorfismo.*

5. ${}_{A*G}A$ *es* $A*G$*-proyectivo y generador.*

6. *Los morfismos* $\mathrm{Tr} : A \otimes_{A*G} A \to A^G$ *y* $\beta : A \otimes_{A^G} A \to A*G$ *son isomorfismos.*

7. *Los morfismos* Tr *y* $\beta$ *son sobreyectivos.*

8. *Existe un elemento* $a \in A$ *tal que* $\mathrm{tr}(a) = 1$ *y un elemento* $\sum_i a_i \otimes b_i \in A \otimes_{A^G} A$ *tal que* $\beta\left(\sum_i a_i \otimes b_i\right) = 1_{A*G}$.

9. *Existe un elemento* $a \in A$ *tal que* $\mathrm{tr}(a) = 1$ *y elementos* $a_i, b_i$ *(*$i \in I$ *un conjunto finito) tales que para todo* $g \in G$, $\sum_{i\in I} a_i g(b_i) = \delta_{Id,g}$ *(la delta de Krönecker).*

La demostración de esta proposición no tiene sorpresas, vamos solamente a delinearla.

A partir de la teoría de Morita, si $C$ es un anillo y $P_C$ es un $C$-módulo a derecha (y por lo tanto $\mathrm{End}_C(P)$-$C$-bimódulo), llamamos $B := \mathrm{End}_C(P)$. El funtor $P \otimes_C -$ es una equivalencia entre las categorías $C$- mod y $B$- mod si y solamente si $P$ es $C$-proyectivo de tipo finito generador, o bien $P$ es $B$-proyectivo de tipo finito generador, o bien $\mathrm{Hom}_B(P, -)$ es una equivalencia (ver por ejemplo [A-F]).

En nuestro caso, los condiciones de proyectividad y generación son respectivamente 4 y 5. (Observamos que hemos identificado $A^G \cong \mathrm{End}_{A*G}({}_{A*G}A)$, y que el isomorfismo $A*G \cong \mathrm{End}_{A^G}(A_{A^G})$ es parte de la condición 4.)

La parte correspondiente al funtor $P \otimes_C -$ es 2, el funtor $\mathrm{Hom}_{A*G}(A, -)$ se identifica canonicamente con $(-)^G$ (por lo tanto 3).

$1 \Leftrightarrow 6$ es claro. $6 \Leftrightarrow 7$ es también bien conocido (ver por ejemplo [A-F]). Como $\beta$ y Tr son morfismos de bimódulos, sus imágenes son ideales biláteros, y ésto muestra $7 \Leftrightarrow 8$. Finalmente $8 \Leftrightarrow 9$ no es otra cosa que una reescritura de lo mismo.

Para entender mejor este contexto de Morita, es conveniente definir el elemento $e := \sum_{g\in G} g \in A*G$. Con la ayuda de este elemento vemos que $\mathrm{Tr}(a \otimes b) = eab$ y que $\beta(a \otimes b) = aeb$. Además, el ideal a izquierda generado por $e$ es isomorfo a $A$ como $A*G$-$A^G$-bimódulo, y respectivamente a derecha, es decir,

$$ {}_{A*G}A_{A^G} \cong A*G.e \quad (a \mapsto ae), \text{ y } {}_{A^G}A_{A*G} \cong e.A*G \quad (a \mapsto ea)$$

Se ve por lo tanto que el contexto anterior es una equivalencia si y solamente si $e.A*G.e = A^G$ y $A*G.e.A*G = A*G$.

**Definición 1.3.** *Sea* $A$ *un anillo y* $G$ *un subgrupo finito de automorfismos de* $A$*. Diremos que* $(A, G)$ *es* **Galois** *o que* $A$ *es una* **extensión Galois** *de* $A^G$ *si y solamente si se satisface alguna de las condiciones equivalentes de la proposición 1.2.*

# 2. Comentarios sobre la definición

## 2.1. Extensiones de cuerpos

Sean $E$ un cuerpo, $G$ un subgrupo finito de automorfismos de cuerpos de $E$, y $F := E^G$. Como $E$ no tiene ideales biláteros no triviales, y como además es conmutativo, los automorfismos (salvo la identidad) no son interiores. Utilizando el teorema 6.1 de la sección 6 (ver también [Mo]), el anillo $E*G$ es simple. El morfismo de anillos $E*G \to End_F(E)$ es un morfismo de $F$-álgebras, y sabemos también que $\dim_F(E) = |G|$. Como $E*G$ es simple, ese morfismo es inyectivo, pero las dos álgebras tienen la misma dimensión (sobre $F$), entonces es un isomorfismo. Se observa también que como $F = E^G$ es un subcuerpo, $E$ es un $F$-módulo libre (por lo tanto proyectivo generador).

Se ha visto entonces que una extensión Galois finita 'clásica' de cuerpos es siempre una extensión Galois en el sentido de la definición 1.3.

## 2.2. Las dos mitades de la definición

Para ilustrar la relación entre la propiedad de tener un elemento de traza uno y los elementos que satisfacen las condiciones de ortogonalidad, mostramos un cálculo independiente de la equivalencia entre 5 y 9, que está "partida en dos".

**Proposición 2.1.** *Sea $A$ un anillo, $G$ un grupo finito de automorfismos de $A$.*

- *${}_{A*G}A$ es $A*G$ proyectivo si y solamente si existe un elemento $a$ tal que* $\mathrm{tr}(a) = 1$
- *${}_{A*G}A$ es $A*G$ generador si y solamente si existen elementos $a_i$, $b_i$ tales que para todo $g \in G$:* $\sum_{i\in I} a_i g(b_i) = \delta_{Id,g}$.

*Demostración:* Se tiene un epimorfismo de $A*G$-módulos $A*G \to A$ definido por $\epsilon : \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g$, entonces $A$ es proyectivo si y solamente si este epimorfismo es un retracción. Sea $s : A \to A*G$ un morfismo de $A*G$-módulos a izquierda tal que $\epsilon s = Id$, en particular $\epsilon(s(1)) = 1$. Si notamos $s(1) = \sum_G a_g g$, como $s$ es morfismo de $A*G$-módulos se tiene, para todo $h \in G$:

$$\sum_G a_g g = s(1) = s(h(1)) = hs(1) = \sum_G h(a_g)hg$$

De donde se obtiene $h(a_g) = a_{hg}$ para todo $h$ y $g$. En particular, si $a = a_{Id}$, $a_h = h(a)$ para todo $h \in G$. Se ve bien que $\epsilon(s(1)) = \epsilon\left(\sum_{g\in G} g(a)g\right) = \epsilon(ea) = \mathrm{tr}(a)$, y hemos encontrado un elemento de traza uno.

Recíprocamente, si $a \in A$ es tal que $\mathrm{tr}(a) = 1$, la fórmula $s(x) := \sum_{g\in G} xg(a)g = xea$ nos da una sección de $\epsilon$.

Para la segunda parte de la proposición, se supone $A$ generador como $A*G$-módulo. Entonces existe un epimorfismo de $A*G$-módulos $A^{(I)} \to A*G$, y como $A*G$ es finitamente generado sobre sí mismo se puede suponer que $I$ es un conjunto finito. Llamamos $e_i$ la base canónica de $A^{(I)}$ como $A$-módulo y $x_i$ sus imágenes en $A*G$. Cada $x_i$ se escribe como $x_i = \sum_{g\in G} x_{i,g} g$, llamamos $b_i := x_{i,Id}$.

Notamos primero que como $h.e_i = e_i$ para todo $i$ y todo $h \in G$, tenemos que $hx_i = \sum_{g\in G} h(x_{i,g})hg$ debe ser igual a $x_i = \sum_{g\in G} x_{i,g} g$, por lo tanto (tomando $h = g^{-1}$) vale la fórmula $g^{-1}(x_{i,g}) = x_{i,Id} = b_i$ para todo $g$, es decir $x_i = \sum_{g\in G} g(b_i)g$.

Como tenemos un epimorfismo, en particular debe existir un elemento de $A^{(I)}$ que se escribe como $\sum_{i\in I} a_i e_i$ cuya imagen es igual a $1_{A*G}$. Con las notaciones introducidas, tenemos:

$$1_{A*G} = \sum_{i\in I} a_i x_i = \sum_{i\in I, g\in G} a_i g(b_i) g$$

Si se mira componente a componente eso quiere decir $\delta_{Id,g} = \sum_{i\in I} a_i g(b_i)$.

La recíproca es casi evidente. Se define un morfismo a través de la fórmula anterior (usando los $x_i$) y se ve que es un epimorfismo de $A*G$-módulos.

Se puede también "partir en dos" (aunque no lo haremos) la equivalencia entre 4 y 9. Se puede demostrar por ejemplo que $A^G$ es un sumando directo de $A$ como $A^G$-módulo a derecha (resp. a izquierda) si y solamente si existe un elemento de traza uno. Además, $A^G$ es sumando directo de $A$ *como $A^G$-bimódulo* si y solamente si se puede encontrar un elemento de traza uno *en el centro* de $A$. La existencia de los $a_i$, $b_i$ es equivalente a la biyectividad del morfismo $A*G \to End_{A^G}(A)$.

## 2.3. Otras definiciones

En la literatura se encuentran diferentes definiciones de extensión Galois de anillos. En [A-R-S], los autores dan una definición que es más restrictiva, ellos piden no solamente que $A^G$ y $A*G$ sean equivalentes Morita (lo que ellos llaman pre-Galois), sino también una condición mas sobre los anillos $A^G/\mathrm{an}_{A^G}(S)$, donde $S$ es cualquier $A$-módulo simple. Ellos muestran, de cualquier manera, que esta condición suplementaria se verifica automáticamente cuando el anillo $A$ es 'básico' (i.e. $A/\mathrm{an}_A(S)$ es un

anillo de división para todo $A$-módulo simple $S$), en particular si $A$ es commutativo (o de división), $A$ es básico.

Un de los teoremas principales en [A-R-S] dice que si $A$ es un álgebra de dimensión finita sobre un cuerpo algebraicamente cerrado, $G$ un subgroupo de automorfismos del álgebra $A$, y $A/\mathrm{rad}(A)$ básica, entonces $(A, G)$ es Galois si y solamente si la acción de $G$ sobre los $A$-módulos simples es libre. En la teoría de representaciones de álgebras de dimension finita, está definida una noción de revestimiento de Galois, y lo que muestran en [A-R-S] es que al nivel de álgebras, ésto corresponde (cuando el grupo de Galois asociado es finito) a las extensiones Galois en el sentido de nuestra definición.

En [K-T] se encuentra un definición de extensión Galois entre $A$ y $A^{co\,H}$ donde $A$ es una $R$-álgebra ($R$ un anillo conmutativo), $H$ una $R$-álgebra de Hopf $R$-proyectiva de tipo finito, y se pide que $A$ sea un $H$-comódulo álgebra. En el caso $R = \mathbb{Z}$ y $H = \mathbb{Z}^{(G)}$ se ve que estos objetos son exactemente los anillos con una acción de $G$ por automorfismos de anillo. Ellos miran el morfismo de Galois

$$\begin{aligned} \kappa : A \otimes_{A^{co\,H}} A &\to A \otimes_R H \\ a \otimes b &\mapsto \sum ab_0 \otimes b_1 \end{aligned}$$

donde $b \mapsto \sum b_0 \otimes b_1 \in A \otimes H$ es el morfismo de estructura de $A$ como $H$-comódulo, y piden que ese morfismo sea biyectivo. En el caso $H = \mathbb{Z}^{(G)}$ se reencuentra $a \otimes b \mapsto \sum_{g\in G} ag(b)g$ (identificando, con el morfismo no canónico pero evidente, $A \otimes_{\mathbb{Z}} \mathbb{Z}^{(G)} \cong \oplus_{g\in G} A.g = A * G$).

Para los álgebras de Hopf en general, la definición de Kreimer–Takeuchi se toma como definición de extensión Galois, pero no hay acuerdo general, la mayoría de los autores agregan (a la definición de Kreimer–Takeuchi) que $A$ sea fielmente playa sobre $A^{co\,H}$. Esta hipótesis de playitud (en el caso de anillos conmutativos) es muy parecida a pedir que $A$ sea $A^G$-proyectivo generador, puesto que un morfismo de anillos conmutativos $f : A \to B$ hace de $B$ una $A$-álgebra fielmente playa si y solamente si $f$ es un monomorfismo y $A$ (via $f$) es un sumando directo de $B$ como $A$-módulo.

## 2.4. Generadores de $A$ y $A^*$

Como se pudo ver en la proposición 2.1, hay propiedades del anillo $A$ que dependen 'separadamente' de la condición o bien de traza, o bien de los $a_i, b_i$. He aquí un segundo ejemplo, que de hecho será utilizado para demostrar que la parte de existencia de un elemento de traza uno es superflua cuando $A$ es conmutativo e íntegro.

**Proposición 2.2.** *Sea $A$ un anillo, $G$ un subgrupo finito de automorfismos de $A$ tal que existen $a_i$, $b_i$ elementos en $A$ que verifican $\sum_i a_i g(b_i) = \delta_{Id,g}$. Entonces*

1. *$A_{A^G}$ es $A^G$-proyectivo de tipo finito.*
2. *la aplicación $a \mapsto \mathrm{tr}(a.-)$ da un isomorfismo ${}_{A^G}A \cong \mathrm{Hom}_{A^G}(A_{A^G}, A^G)$, en particular se tiene la propiedad simétrica a la anterior, es decir, $A$ es $A^G$-proyectivo de tipo finito también a izquierda.*

*Demostración:* 1. Si $x \in A$,

$$x = \sum_{g\in G} \delta_{Id,g} g(x) = \sum_i \sum_{g\in G} a_i g(b_i) g(x) = \sum_i a_i \mathrm{tr}(b_i.x)$$

Se tiene entonces que $A$ está generado a derecha por los $a_i$, y que $\mathrm{tr}(b_i.-)$ es una 'base proyectiva' dual a los $a_i$, *ergo* $A_{A^G}$ es proyectivo de tipo finito y $\mathrm{Hom}_{A^G}(A_{A^G}, A^G)$ es $A^G$-proyectivo de tipo finito a izquierda, además, los elementos $\mathrm{tr}(b_i.-)$ son un sistema de generadores de $\mathrm{Hom}_{A^G}(A_{A^G}, A^G)$.

2. Sea $a \in A$ tal que $\mathrm{tr}(a.x) = 0$ para todo $x \in A$, en particular

$$0 = \sum_i \mathrm{tr}(a.a_i)b_i = \sum_{g\in G} \sum_i g(a)g(a_i)b_i = \sum_{g\in G} g(a)\delta_{Id,g^{-1}} = a$$

Lo que muestra que la aplicación $a \mapsto \mathrm{tr}(a.-)$ es inyectiva. Consideremos ahora $f \in \mathrm{Hom}_{A^G}(A_{A^G}, A^G)$ y $x \in A$,

$$f(x) = \sum_i f(a_i \mathrm{tr}(b_i x)) = \sum_i f(a_i)\mathrm{tr}(b_i x) = \sum_i \mathrm{tr}(f(a_i)b_i x) = \mathrm{tr}\left((\sum_i f(a_i)b_i).x\right)$$

Esto muestra que $f$ es de la forma $\mathrm{tr}(b.-)$, con $b = \sum_i f(a_i)b_i$.

### 2.5. Sobre la traza

Se verá más tarde que si $A$ es conmutativo e íntegro, la existencia de los $a_i$ $b_i$ implica automáticamente la existencia de un elemento de traza uno. Bajo la hipótesis de integridad, esta media-parte de la definición de extensión Galois es por lo tanto superflua.

Hace falta observar también que si $|G|$ es inversible en $A$, entonces $\mathrm{tr}(1/|G|)$ es igual a uno. Por lo tanto, en característica cero, no hace falta preocuparse por la traza (independientemente de los $a_i$ $b_i$!).

## 3. Consecuencias inmediatas

### 3.1. $A^{op}$

Sea $A$ un anillo y $G$ un subgrupo finito de automorfismos de $A$. Esto quiere decir que, para todo par de elementos $a$, $b$ en $A$, y para todo par de elementos $g$, $g'$ en $G$ las igualdades $g(a+b) = g(a) + g(b)$, $g(ab) = g(a)g(b)$ y $g(1) = 1$ son satisfechas. También $g(g'(a)) = (gg')(a)$. Es evidente entonces que se puede considerar $G$ como subgrupo de automorfismos de $A^{op}$.

**Proposición 3.1.** *Con las notaciones anteriores, si $A$ es una extensión Galois de $A^G$ entonces $A^{op}$ es una extensión Galois de $(A^{op})^G$.*

*Demostración:* Si $a \in A$ es tal que $\mathrm{tr}(a) = 1$, se considera el mismo elemento $a$ en $A^{op}$ y evidentemente se tiene $\mathrm{tr}(a) = 1$.

Si $a_i$, $b_i$ son los elementos tales que para todo $g \in G$,

$$\sum_i a_i g(b_i) = \delta_{Id,g}$$

entonces se define $a'_i := b_i$ y $b'_i := a_i$. Se hace el calculo:

$$\begin{aligned}\sum_i a'_{i\cdot_{op}} g(b'_i) = \sum_i b_{i\cdot_{op}} g(a_i) = \sum_i g(a_i).b_i = g\left(\sum_i a_i.g^{-1}(b_i)\right)\\ = g(\delta_{Id,g^{-1}}) = \delta_{Id,g^{-1}} = \delta_{Id,g}\end{aligned}$$

### 3.2. Sobre las singularidades

Sea ahora $A$ un anillo, y $G$ un subgrupo finito de automorfismos de $A$. Bajo ciertas condiciones se tiene un teorema de tipo Maschke:

**Proposición 3.2.** *Supongamos que existe $a \in \mathcal{Z}(A)$ tal que $\mathrm{tr}(a) = 1$. Si $p : M \to N$ es un epimorfismo de $A * G$ módulos que admite una sección $A$-lineal, entonces $p$ admite una sección $A * G$-lineal.*

*Demostración:* Como en la prueba del teorema de Maschke clásico, se "promedian" los morfismos para convertirlos en $G$-lineales. Más precisamente, si $s : N \to M$ es una sección $A$-lineal, y $a \in \mathcal{Z}(A)$ es tal que $\mathrm{tr}(a) = 1$, se define $\widetilde{s} : N \to M$ a través de la fórmula

$$\widetilde{s}(n) := \sum_{g\in G} g^{-1}(s(ag(n))$$

Si $x \in A$, $g(xn) = g(x)g(n)$, por linealidad de $s$ y como $g^{-1}(g(x)) = x$ se tiene que $\widetilde{s}$ es $A$-lineal. (Se ha utilizado la igualdad $ag(x) = g(x)a$ pues $a \in \mathcal{Z}(A)$.) Si $h \in G$,

$$\widetilde{s}(hm) = \sum_{g\in G} g^{-1}(s(ag(hn)) = \sum_{g\in G} g^{-1}(s(a(gh)(n)) =$$

$$= h.\sum_{g\in G}(gh)^{-1}(s(agh(n)) = h\widetilde{s}(n)$$

Esto muestra la $A*G$-linealidad de $\widetilde{s}$. Podemos también verificar que sigue siendo sección:

$$p(\widetilde{s}(n)) = p\left(\sum_{g\in G} g^{-1}(s(ag(n)))\right) = \sum_{g\in G} g^{-1}(ps(ag(n)))$$

$$= \sum_{g\in G} g^{-1}(ag(n)) = \sum_{g\in G} g^{-1}(a)n = \mathrm{tr}(a)n = n$$

Aquí hemos usado primero que $p$ es $G$-lineal, luego que $ps = Id_N$, y finalmente que $\mathrm{tr}(a) = 1$.

**Corolario 3.3.** *Sea $A$ un anillo conmutativo y $G$ un subgrupo finito de automorfismos de $A$ tal que la extensión $A|A^G$ sea Galois. Entonces* $\mathrm{lgldim}(A^G) = \mathrm{lgldim}(A)$

*Demostración:* Como $A^G$ es equivalente Morita a $A*G$ y la dimensión global proyectiva (a izquierda) es un invariante Morita, se tiene $\mathrm{lgldim}(A^G) = \mathrm{lgldim}(A*G)$.

Por la proposición anterior, si $M$ es un $A*G$-módulo que es proyectivo como $A$-módulo, entonces es $A*G$-proyectivo, y eso implica $\mathrm{lgldim}(A*G) = \mathrm{lgldim}(A)$.

**Corolario 3.4.** *Bajo las mismas hipótesis que antes, el anillo $A$ es regular si y solamente si $A^G$ es regular.*

*Demostración:* Después del corolario, hace falta solamente recordar que un anillo conmutativo $B$ es regular si y solamente si $\mathrm{lgldim}(B) < \infty$.

**Ejemplo:** Sea $k$ un cuerpo de característica 2, $A = k[x]$ y $G = \mathbb{Z}/2\mathbb{Z}$, con generador $\sigma$ actuando en $A$ por $\sigma(x) = x + 1$.

En este ejemplo no se puede dividir por $|G|$ y $\mathrm{tr}(1) = 0$, pero $\mathrm{tr}(x) = x + \sigma(x) = 2x + 1 = 1$.

Además, se ve bien que

$$x,1 + 1.(x + 1) = 1$$

y

$$x,1 + 1.x = 0$$

Entonces los elementos $a_1 = x$, $a_2 = 1$, $b_1 = 1$, $b_2 = (x+1)$ verifican $a_1b_1+a_2b_2 = 1$ y $a_1\sigma(b_1)+a_2\sigma(b_2) = 0$. En consecuencia, $A$ es una extensión Galois de $A^G$. Como $A$ es regular, $A^G$ es regular también. Se ve bien que no hubo necesidad de encontrar un sistema de generadores y relaciones para concluir la regularidad de $A^G$. De todas maneras, se puede calcular explícitamente $A^G$. Si se llama $t := x.(x - 1)$, se tiene $\sigma(t) = t$ pero además, se puede verificar que $A^G = k[t]$, que es claramente regular.

**Observación:** La condición $A$ regular y $A^G$ regular no es suficiente para asegurar que la extensión es Galois. Veamos un ejemplo:

Sea $k$ un cuerpo de característica diferente de 2, $A = k[x]$ y $G = \mathbb{Z}/2\mathbb{Z}$. Sea $g$ generador de $G$, se define la acción por $g(x) = -x$.

En este caso, es claro que $A^G = k[x^2]$, que es un anillo de polinomios, por lo tanto regular. Como se supone $\mathrm{ch}(k) \neq 2$, la traza es un epimorfismo, miramos ahora el morfismo $\beta : A \otimes_{A^G} A \to A * G$.

Es claro que 1 y $x$ generan a $A$ como $A^G$-módulo, por lo tanto todo elemento de $A \otimes_{A^G} A$ se puede escribir (de manera única) en la forma $p\otimes 1+q\otimes x$, con $p, q \in A$. Para ver si $1 \in Im(\beta)$ hay que resolver el sistema de ecuaciones

$$p + qx = 1$$

$$p - qx = 0$$

Es un sistema lineal, se buscan las soluciones de manera elemental. Por ejemplo, se puede ver como dos ecuaciones con coeficientes en el cuerpo $k(x)$. El determinante del sistema es $-2x$, y por lo tanto hay una solución única en $k[x, x^{-1}]$. Si esta solución se encuentra en $k[x]$, la extensión será Galois, si no, no. Pero la solución es $p = 1/2$, $q = 1/2x$, que no está en $k[x]$, y por lo tanto $A$ no es una extensión Galois de $A^G$. Por otro lado, $G$ actúa sobre $k[x, x^{-1}]$ y $k[x, x^{-1}]$ es una extensión Galois de $k[x, x^{-1}]^G = k[x^2, x^{-2}]$, donde $b_1 = 1$, $b_2 = x$, $a_1 = p$ y $a_2 = q$.

## 3.3. Morfismos

A partir de la condición con los elementos $a$, $a_i$ y $b_i$ de la definición de Galois (es decir de la condición 9 de la proposición 1.2), se deduce de manera elemental el hecho siguiente:

**Proposición 3.5.** *Sean $A$ y $B$ dos anillos, $G$ un grupo que actúa por automorfismos de anillo en $A$ y $B$. Supongamos que existe un morfismo de anillos $f : A \to B$ que conmuta con la acción de $G$. Entonces, si la extensión $A|A^G$ es Galois, también es Galois la extensión $B|B^G$.*

*Demostración:* Si $a, a_i, b_i \in A$ son elementos que verifican $\mathrm{tr}(a) = 1$, $\sum_i a_i g(b_i) = \delta_{Id,g}$, se toman los elementos $f(a)$, $f(a_i)$ y $f(b_i)$.

Ilustraremos esta proposición con algunos casos particulares:

### Anillos graduados

Sea $A = \oplus_{n\geq 0} A_n$ un anillo $\mathbb{Z}$-graduado y $G$ un grupo finito de automorfismos de $A$ que respetan la graduación. Entonces, $A$ es una extensión Galois de $A^G$ si y solamente si $A_0$ es una extensión Galois de $A_0^G$.
*Demostración:* La inclusión $A_0 \to A$ y la proyección $A \to A_0$ son dos morfismos de anillos, $G$-equivariantes.

### Localización

Sea $A$ un anillo conmutativo, y $G$ un subgrupo finito de automorfismos de $A$. Si $S$ es un subconjunto multiplicativo de $A$, para calcular $S^{-1}A$ se puede suponer sin pérdida de generalidad que $S$ es $G$-estable. (O bien se agrega $G(S)$, o bien, para cada $s \in S$ se considera $N(s) := \prod_{g\in G} g(s)$ y se toman fracciones sobre ese tipo de denominadores.)

Entonces, si $A$ es una extensión Galois de $A^G$, $S^{-1}A$ es una extensión Galois de $(S^{-1}A)^G$.

Si $A$ no es conmutativo, pero $S$ es un subconjunto de Ore, $G$-estable, se tiene exactemente el mismo enunciado.

### Extensiones de escalares

Sea $A$ un anillo cualquiera y $G$ un subgrupo finito de automorfismos de $A$. Sea $k$ un subanillo de $\mathcal{Z}(A) \cap A^G$, y $B$ una $k$-álgebra.

Se puede considerar el álgebra $A \otimes_k B$, y se puede ver a cada $g \in G$ como un automorfismo de $A \otimes_k B$ a través de la fórmula

$$g(a \otimes b) := g(a) \otimes b$$

La flecha $k \to B$ induce un morfismo de anillos $A \cong A \otimes_k k \to A \otimes_k B$ que es $G$-equivariante. Entonces si $A$ es una extensión Galois de $A^G$, $A \otimes_k B$ es una extensión Galois de $(A \otimes_k B)^G$.

En ciertos casos se puede decir un poco más. Supongamos que $B$ es $k$-fielmente playa. Se puede identificar entonces $(A \otimes_k B)^G$ con $A^G \otimes_k B$. Además, $(A \otimes_k B) * G = (A * G) \otimes_k B$, y los morfismos

$$\mathrm{Tr} : (A \otimes_k B) \otimes_{(A*G)\otimes_k B} (A \otimes_k B) = (A \otimes_{A*G} A) \otimes_k B \to (A^G) \otimes_k B$$

$$\beta : (A \otimes_k B) \otimes_{A^G \otimes_k B} (A \otimes_k B) = (A \otimes_{A^G} A) \otimes_k B \to (A * G) \otimes_k B$$

se identifican naturalemente con $\mathrm{Tr} \otimes Id$ y $\beta \otimes Id$. Como se supuso $B$ fielmente playa sobre $k$, los morfismos $\mathrm{Tr} \otimes Id$ y $\beta \otimes Id$ son epimorfismos si y solamente si Tr y $\beta$ lo son. Se ha demostrado entonces la proposición siguiente:

**Proposición 3.6.** *Sea $A$ un anillo cualquiera y $G$ un subgrupo finito de automorfismos de $A$. Sea $k$ un subanillo de $\mathcal{Z}(A) \cap A^G$, y $B$ una $k$-álgebra fielmente playa sobre $k$. Entonces $A$ es una extensión Galois de $A^G$ si y solamente si $A \otimes_k B$ es una extensión Galois de $(A \otimes_k B)^G$.*

Para una aplicación de esta proposición, ver el ejemplo de $\mathrm{SL}(2, k)$ con $k$ un cuerpo (no necesariamente algebraicamente cerrado).

## Ideales estables

Sea $I \subset A$ un ideal bilátero, $G$ un subgrupo finito de automorfismos de $A$. Supongamos que para todo $g \in G$: $g(I) \subseteq I$. Cconsiderando la acción de $G$ sobre el anillo cociente $A/I$, si $A$ es una extensión Galois de $A^G$, entonces $A/I$ es una extensión Galois de $(A/I)^G$.
*Demostración:* la proyección canónica $\pi : A \to A/I$ es un morfismo de anillos $G$-equivariante.

## 3.4. El radical

Sea $A$ un anillo, denotamos $\mathrm{rad}(A) = J(A)$ el ideal de Jacobson de $A$, es decir la intersección de todos los ideales maximales a izquierda de $A$, que es, de hecho, un ideal bilátero (y que coincide con la intersección de todos los ideales maximales a derecha de $A$). Si $G$ es un subgrupo finito de los automorfismos de $A$, entonces $G$ opera sobre el conjunto de los ideales maximales (por ejemplo a izquierda), luego $\mathrm{rad}(A)$ es siempre un ideal $G$-estable.

La proposición siguiente aparece en [A-R-S]

**Proposición 3.7.** *Sea $A$ un anillo y $G$ un subgrupo finito de los automorfismos de $A$. Entonces $(A, G)$ es Galois si y solamente si $(A/\mathrm{rad}(A), G)$ es Galois.*

*Demostración:* Como $\mathrm{rad}(A)$ es un ideal bilátero $G$-estable, sabemos que $(A, G)$ galois implica $(A/\mathrm{rad}(A), G)$ Galois. Vamos a demostrar la recíproca, primero la sobreyectividad de Tr y luego la sobreyectividad de $\beta$.

Se supone $(A/\mathrm{rad}(A), G)$ Galois, entonces existe un elemento $\overline{a} \in A/\mathrm{rad}(A)$ tal que $\mathrm{tr}(\overline{a}) = 1_{A/\mathrm{rad}(A)}$. Esto quiere decir que $\mathrm{tr}(a) = 1 + r$ donde $r \in \mathrm{rad}(A)$. Pero además, como $1 + r \in \mathrm{Im}(\mathrm{tr}) \subseteq A^G$, el elemento $r$ pertenece a $A^G$.

Como todo elemento de la forma $1 + r$ con $r \in \mathrm{rad}(A)$ es una unidad de $A$, se tiene $1 + r \in \mathcal{U}(A) \cap A^G = \mathcal{U}(A^G)$. Entonces la imagen de la traza contiene una unidad y por lo tanto es sobreyectiva.

Sean ahora $\{\overline{a}_i, \overline{b}_i\}_{i \in I}$ elementos de $A/\mathrm{rad}(A)$ tales que, para todo $g \in G$, vale la identidad (en $A/\mathrm{rad}(A)$)

$$\sum_{i \in I} \overline{a}_i g(\overline{b}_i) = \delta_{Id,g}$$

Entonces en $A$ se puede escribir

$$\sum_{i \in I} a_i g(b_i) = \delta_{Id,g} + r_g$$

con $r_g \in \mathrm{rad}(A)$. Si se toma el elemento $\sum_{i \in I} a_i \otimes b_i \in A \otimes_{A^G} A$, la identidad precedente significa que

$$\beta\left(\sum_{i \in I} a_i \otimes b_i\right) = 1 + \sum_{g \in G} r_g g$$

Observamos ahora que $\mathrm{rad}(A) * G = \oplus_{g \in G} \mathrm{rad}(A).g \subseteq \mathrm{rad}(A * G)$, y como cada $r_g \in \mathrm{rad}(A)$, se puede concluir que la imagen de $\beta$ contiene una unidad, y por lo tanto es sobreyectiva.

## 3.5. Localización II

Para los anillos conmutativos íntegros, se tiene otra propiedad con respecto a la localización, que es de interés justamente cuando la extensión $A|A^G$ no es Galois.

Sea $A$ un anillo conmutativo íntegro y $G$ un subgrupo finito de automorfismos de $A$. En general la extensión $A|A^G$ puede no ser Galois, pero se puede mirar $E := frac(A)$, el cuerpo de fracciones de $A$.

Un elemento de $E$ es un fracción $a/b$ con $a,\ b \in A,\ b \neq 0$. Si se multiplica el numerador y el denominador por $\prod_{g \in G - \{Id\}} g(b)$ se ve que se puede suponer que la fracción tiene denominador en $A^G$. Vemos de esta manera que $E = (A^G - \{0\})^{-1} A$, y que si $F := E^G$, $F = frac(A^G)$.

Sin hipótesis sobre el subgrupo $G$, se sabe que la extensión $E|E^G$ es Galois, entonces existen $x_i, y_i \in E$ tales que

$$\sum_{i \in I} x_i g(y_i) = \delta_{Idg}$$

Como se puede escribir cada $x_i = a_i/\lambda_i$, $y_i = b_i/\mu_i$, con $\lambda_i$ y $\mu_i$ en $A^G - \{0\}$, se ve que esas ecuaciones son válidas en una localización intermedia entre $A$ y $E$.

Más precisamente, si se define $f := (\prod_i \lambda_i).(\prod_i \mu_i)$, se tiene entonces que la ecuación tiene sentido en $A[f^{-1}]$. Como $A$ (y $A[f^{-1}]$) es íntegra, se sabe (veremos luego) que la condición de los "$a_i$, $b_i$" implica la condición de la traza. Se tiene entonces la demostración de:

**Proposición 3.8.** *Sea $A$ un anillo conmutativo íntegro y $G$ un subgrupo finito de automorfismos de $A$. Entonces existe $f \in A^G$ tal que $A[f^{-1}]$ es una extensión Galois de $A[f^{-1}]^G$.*

Ahora volvemos sobre los propiedades que se deducen de manera elemental a partir del punto 9 de la proposición 1.2 justo antes de la definición de Galois.

## 3.6. Subgrupos intermedios

Sea $A$ un anillo cualquiera, $G$ un subgrupo finito de automorfismos de $A$, y $H \subseteq G$ un subgrupo de $G$.

**Proposición 3.9.** *Si $A$ es una extensión Galois de $A^G$, entonces $A$ es una extensión Galois de $A^H$*

Antes de la demostración, observamos que si por ejemplo se mira la condición 1 de la proposición 1.2, lo que acabamos de afirmar es que si el $A*G$-$A^G$-bimódulo $A$ da una equivalencia Morita entre $A^G$ y $A*G$, entonces ese mismo $A$ visto como $A*H$-$A^H$-bimódulo da una equivalencia Morita entre $A^H$ y $A*H$ para todo subgrupo $H$, lo que no parece para nada evidente, al menos desde ese punto de vista.

*Demostración:* A partir de la condición 9 de la proposición 1.2, se sabe que existen $a$, $a_i$, $b_i$ en $A$ tales que $\sum_i a_i g(b_i) = \delta_{Id,g}$ para todo $g \in G$, y $\mathrm{tr}(a) = 1$.

Es claro que si $\sum_i a_i g(b_i) = \delta_{Id,g}$ para todo $g \in G$, entonces $\sum_i a_i g(b_i) = \delta_{Id,g}$ para todo $g \in H$, y hemos verificado una mitad de la definición.

Sobre la traza:

$$1 = \sum_{g \in G} g(a) = \sum_{h \in H} h \left( \sum_{g \in (G:H)} g(a) \right)$$

donde $(G : H)$ denota un conjunto de representantes de clases de $G$ módulo $H$. Si se elige $\widetilde{a} := \sum_{g \in (G:H)} g(a)$, entonces $\mathrm{tr}_H(\widetilde{a}) = \mathrm{tr}_G(a) = 1$.

Se tiene un resultado un poco más fino que el del corolario 3.3:

**Corolario 3.10.** *Sea $A$ un anillo conmutativo regular, $G$ un subgrupo finito de automorfismos de $A$ tal que $A$ es una extensión Galois de $A^G$. Entonces, para todo subgrupo $H$ de $G$, el anillo $A^H$ es regular.*

Como aplicación se tiene un ejemplo donde se ve que la condición de ser una extensión Galois es más fuerte que la de tener acciones donde el anillo cociente sea regular:

Sea $A = k[x, y, z]$, $G = S_3$ el grupo de permutación de tres letras, actuando sobre $A$ por permutación de $x$, $y$, y $z$. Es bien conocido que $A^G = k[s_1, s_2, s_3]$ donde las $s_i$ son los polinomios simétricios elementales, es decir $s_1 = x + y + z$, $s_2 = xy + xz + yz$, $s_3 = xyz$. Se tiene entonces un ejemplo de anillo regular $A$ tal que $A^G$ es regular, pues es isomorfo a un anillo de polinomios.

Consideremos la permutación cíclica $\sigma$ definida por $x \mapsto y \mapsto z \mapsto x$, y $H =< \sigma >= \{1, \sigma, \sigma^{-1}\}$.

El elemento $\sigma$ no es una pseudo-reflexión, tampoco $\sigma^{-1}$, luego $A^H$ es *singular*. Esto implica que $A$ no es una extensión Galois de $A^H$ y en consecuencia $A$ no es una extensión Galois de $A^G$.

De todas formas se sabe que existe un polinomio invariante $f$ tal que luego de la localización por $f$, la extensión queda Galois. $A$ es $A^G$-libre de rango $|S_3| = 6$. Se puede encontrar una base de $A$ como $A^G$-módulo y proceder como en el ejemplo de $k[x]$, para llegar a un sistema de ecuaciones en $k(x, y, z)$. Si se hace todo ese camino, el determinante del sistema es (a menos de signo) una potencia del polinomio determinante $\delta = (x - y)(x - z)(y - z)$. En consecuencia, $k[x, y, z][\delta^{-1}]$ es una extensión Galois de sus invariantes.

Se verá más tarde una manera de reencontrar este resultado sin necesidad de hacer las cuentas.

Si $H$ es un subgrupo invariante de $G$, se puede considerar el grupo $G/H$, y si $G$ actúa sobre un anillo $A$, el subanillo más grande de $A$ donde $H$ actúa trivialmente es, por definición, $A^H$. La acción de $G$ sobre $A$ induce una acción de $G/H$ en $A^H$, y se tiene el resultado esperado:

**Proposición 3.11.** *Sea $(A, G)$ una extensión Galois y $H$ un subgrupo invariante de $G$, entonces $(A^H, G/H)$ es una extensión Galois.*

*Demostración:* Sea $a \in A$ tal que $\mathrm{tr}_G(a) = 1$ y $\{a_i, b_i\}_{i\in I} \subseteq A$ tales que $\sum_{i\in I} a_i g(b_i) = \delta_{Id,g}$.

Se define

$$a' := \mathrm{tr}_H(a),\ a'_i = \mathrm{tr}_H(a'a_i),\ b'_i = \mathrm{tr}_H(b_i)$$

De manera elemental se tiene:

$$\sum_{\overline{g}\in G/H, h\in H} \overline{g}(h(a)) = \sum_{g\in G} g(a) = 1$$

Si $\overline{g} \in G/H$,

$$\sum_{i\in I} a'_i \overline{g}(b'_i) = \sum_{i\in I} a'_i g(b'_i) = \sum_{i\in I,\ h,h'\in H} h(a'a_i)g(h'(b_i)) =$$

$$= \sum_{h\in H} h\left(\sum_{i\in I, h'\in H} a'a_i h^{-1} g(h'(b_i))\right) = \sum_{h\in H} h\left(\sum_{h'\in H} a'\delta_{Id,h^{-1}gh'}\right)$$

Pero todos esos términos son cero, salvo cuando $h^{-1}gh' = Id$, o bien $g = h(h')^{-1}$, que sucede sólo cuando $g \in H$ (i.e $\overline{g} = Id$), y en ese caso, esa suma es igual a $\sum_{h\in H} h(a') = 1$. O sea, esta suma es igual a $\delta_{Id,\overline{g}}$

# 4. Sobre la traza en los anillos íntegros

El objetivo de esta sección es mostrar que si $A$ es un anillo íntegro, y $G$ un subgrupo finito de automorfismos de $A$ tal que existen $a_i$, $b_i$ en $A$ verificando $\sum_i a_i g(b_i) = \delta_{Id,g}$ $(\forall g \in G)$, entonces $A$ es una extensión Galois de $A^G$; es decir, la existencia de los $a_i$, $b_i$ implican, cuando $A$ es íntegra, la existencia de un elemento de traza uno.

Este resultado ha sido probado con un poco más de generalidad en [C-H-R] utilizando una hipótesis sobre los idempotentes (siempre en el caso conmutativo), pero no dan ejemplos. Se encuentra también en [Fe] una condición (expresada en términos de los idempotentes) para tener un enunciado análogo en el caso no conmutativo. De todas maneras, esta propiedad parece ser bastante particular de las álgebras conmutativas íntegras, pues se verá más tarde un contraejemplo con $G = \mathbb{Z}/2\mathbb{Z}$ y $A = M_3(k)$ con $k$ un cuerpo de característica 2, en donde existen los $a_i$, $b_i$, pero ningun elemento tiene traza uno (ver Ejemplo con matrices II).

Comenzamos con algunos lemas de álgebra conmutativa.

**Lema 4.1.** *Sea $R$ un anillo conmutativo, $M$ un $R$-módulo de tipo finito, $J$ un ideal de $R$. Entonces $J.M = M$ si y solamente si $R = J + \mathrm{an}(M)$.*

Una implicación es evidente y no se necesita que $M$ sea finitamente generado, pues si $R = J+\mathrm{an}(M)$, se puede escribir $1 = j + r$ con $j \in J$ y $r \in \mathrm{an}(M)$, entonces para $m \in M$, $1.m = j.m + r.m = j.m$, es decir, $J.M = M$.

Para la recíproca, se hace inducción en la cantidad de generadores de $M$

*Caso $n = 1$:*

Se supone $M$ cíclico, sea $m_0 \in M$ un generador. Por hipótesis, $M = J.M$, en particular, existen $m_1 \in M$ y $j_1 \in J$ tales que

$$m_0 = j_1.m_1$$

pero como $m_0$ genera $M$, existe $a \in A$ tal que $m_1 = am_0$, y se llega a la igualdad:

$$m_0 = j_1.m_1 = j_1.a.m_0$$

Si se escribe $j := j_1.a \in J$, se tiene $m_0 = j.m_0$ lo que implica $r := (1 - j) \in \mathrm{an}(< m_0 >) = An(M)$, y $1 = j + r$.

*Caso general:*

Sea $M$ un $R$-módulo con generadores $m_1, \ldots, m_n$ que verifican $J.M = M$, y sea $N := M/\langle m_1 \rangle$. Se ve bien que $J.N = N$ y $N$ está generado por un cantidad menor de elementos. Por hipótesis inductiva se puede escribir $1 = j_1 + r_1$, donde $j_1 \in J$ y $r_1$ verifica $r_1.m_i \in \langle m_1 \rangle \ \forall i = 2, \ldots, n$. Se mostrará ahora que $< m_1 >$ también verifica $J.\langle m_1 \rangle = \langle m_1 \rangle$.

Por hipótesis, $M = J.M$, en particular $m_1 \in M$ se puede escribir en la forma

$$m_1 = \sum_{i=1}^{n} x_i.m_i$$

donde $x_i \in J$. Utilisando la escritura $1 = j_1 + r_1$, se tiene:

$$m_1 = j_1.m_1 + r_1.m_1 = j_1.m_1 + \sum_{i=1}^{n} x_i.r_1.m_i$$

Como $r_1.m_i \in \langle m_1 \rangle$, $j_1 \in J$, $x_i \in J$ se concluye $m_1 \in J.m_1$. Estamos por lo tanto en el caso cíclico, luego sabemos que existen $j_0 \in J$, $r_0 \in An(m_1)$ tales que $1 = j_0 + r_0$. Juntando las dos descomposiciones de 1 obtenemos:

$$1 = (j_1 + r_1)(j_0 + r_0) = (j_1.j_0 + j_1.r_0 + r_1.j_0) + r_1.r_0$$

Lo que está entre paréntesis pertenece a $J$, y $r_1.r_0 \in An(M)$ pues la imágen de la multiplicación por $r_1$ está contenida en el submódulo generado por $m_1$, y $r_0.m_0 = 0$.

**Corolario 4.2.** *Sea $R$ un anillo conmutativo íntegro, $M$ un $R$-módulo proyectivo de tipo finito, entonces $M$ es un generador. Es decir, la imagen del morfismo canónico $ev : M^* \otimes_R M \to R$ es todo $R$.*

*Demostración:* Como $M$ es proyectivo de tipo finito, existe un sistema de generadores $m_1, \ldots, m_n$ y elementos $p_1, \ldots, p_n \in M^*$ tales que, para todo $x \in M$,

$$x = \sum_{i=1}^{n} p_i(x).m_i$$

Sea $I := \mathrm{Im}(ev : M^* \otimes M \to R)$, $I$ es un ideal de $R$, y la fórmula anterior nos dice en particular que $I.M = M$. Como $M$ es finitamente generado, se está en los condiciones del lema y $R = I + \mathrm{an}(M)$. Pero además, $M$ es proyectivo sobre un anillo íntegro, por lo tanto no tiene torsión, y $\mathrm{an}(M) = 0$, por lo tanto $I = R$.

Ahora el teorema enunciado:

**Teorema 4.3.** *Sea $A$ un anillo íntegro y $G$ un subgrupo finito de automorfismos de $A$. Se supone que existen $a_1, \ldots, a_n, b_1, \ldots, b_n$ en $A$ verificando, para todo $g \in G$, $\sum_{i=1}^{n} a_i g(b_i) = \delta_{Id,g}$. Entonces, existe un elemento $a \in A$ tal que $\sum_{g \in G} g(a) = 1$.*

*Demostración:* se está en condiciones de utilizar la proposición 2.2 (punto 1), que nos asegura que $A$ es $A^G$-proyectivo de tipo finito.

Por el corolario anterior, la imagen de la evaluación $A^* \otimes_{A^G} A \to A$ contiene al 1, existen por lo tanto $p_i \in A^*$, $x_i \in A$ tales que $\sum_{i=1}^{n} p_i(x_i) = 1$.

Utilizando otra vez la proposición 2.2, (el punto 2), sabemos que la aplicación $A \to A^*$ dada por $a \mapsto \mathrm{tr}(a.-)$ es una biyección, entonces cada $p_i$ es de la forma $\mathrm{tr}(y_i.-)$, por lo podemos escribir

$$1 = \sum_{i=1}^{n} p_i(x_i) = \sum_{i=1}^{n} tr(y_i.x_i) = \mathrm{tr}\left(\sum_{i=1}^{n} y_i x_i\right)$$

Se toma $a := \sum_{i=1}^{n} y_i x_i$ y la demostración queda terminada.

# 5. Extensiones de Galois de anillos conmutativos

## 5.1. Caracterización en términos de ideales maximales

Cuando el anillo $A$ es conmutativo, se puede mirar la condición de Galois en términos de ideales maximales. La proposición siguiente proviene de [D-I]:

**Teorema 5.1.** *Sea $A$ un anillo conmutativo, $G$ un subgrupo finito de automorfismos de $A$. Las dos condiciones siguientes son equivalentes:*

1. *Existen $a_i$, $b_i$ tales que para todo $g \in G$ $\sum_{i\in I} a_i g(b_i) = \delta_{Id,g}$.*
2. *Para todo ideal maximal $\mathcal{M}$ y para todo $g \in G$, existe $x \in A$ tal que $x - g(x) \notin \mathcal{M}$.*

**Observación:** Si $F$ es un cuerpo, $G$ un grupo finito de automorfismos de $F$, y $g \in G$ diferente de la identidad, es claro que existe $x \in F$ tal que $x - g(x) \neq 0$. Suponiendo demostrada la proposición, se ve por la segunda vez que todo cuerpo es una extensión Galois de sus invariantes.

La demostración que se propone es esencialmente idéntica a la de [D-I], salvo que elegí escribir en forma de lema el argumento principal, porque de esta manera se obtendrá un corolario interesante que no se menciona en la literatura.

**Lema 5.2.** *Sea $A$ un anillo conmutativo y $g$ un automorfismo de $A$. Si el ideal generado por los elementos de la forma $x - g(x)$ coincide con $A$, entonces existen elementos de $A$, $a_i$, $b_i$, ($i \in I$ un conjunto finito) tales que $\sum_{i\in I} a_i b_i = 1$ y $\sum_{i\in I} a_i g(b_i) = 0$.*

*Demostración:* Por hipótesis, el ideal generado por los elementos de la forma $(x - g(x))$ es igual a $A$, entonces existen $x_i$, $y_i$, $i = 1, ..., n$ tales que $1 = \sum_{i=1}^{n} x_i(y_i - g(y_i))$. Se puede rescribir esta fórmula de la manera siguiente:

$$1 = \sum_{i=1}^{n} x_i y_i + \left(\sum_{i=1}^{n} x_i g(y_i)\right).(-1)$$

Se toma $a_i = x_i$, $b_i = y_i$, $i = 1, ..., n$, $a_{n+1} := \sum_{i=1}^{n} x_i g(y_i)$, $b_{n+1} = -1$. Con esos cambios de notacions se tiene $\sum_{i=1}^{n+1} a_i b_i = 1$, pero también

$$\sum_{i=1}^{n+1} a_i g(b_i) = \sum_{i=1}^{n} a_i g(b_i) + a_{n+1} g(b_{n+1}) = \sum_{i=1}^{n} x_i g(y_i) + \left(\sum_{i=1}^{n} x_i g(y_i)\right).g(-1) = 0$$

**Lema 5.3.** *Sea $A$ un anillo conmutativo, $g$ y $h$ dos automorfismos de $A$. Supongamos que existen elementos $a_i$, $b_i$, $a'_j$, $b'_j$ tales que*

$$\sum_{i\in I} a_i b_i = 1 \ ; \ \sum_{j\in J} a'_j b'_j = 1$$

$$\sum_{i\in I} a_i g(b_i) = 0 \ ; \ \sum_{j\in J} a'_j h(b'_j) = 0$$

*Entonces, se pueden encontrar elementos $a''_k$, $b''_k$ que tienen las mismas propiedades para $h$ y $g$ simultaneamente, más precisamente, que verifiquen $\sum_{k\in K} a''_k b''_k = 1$, $\sum_{k\in K} a''_k g(b''_k) = 0$ y $\sum_{k\in K} a''_k h(b''_k) = 0$.*

*Demostración:* Se define el conjunto de índices $K := I \times J$, y para cada $k \in K$,

$$a''_{ij} := a_i a'_j$$

$$b''_{ij} := b_i b'_j$$

De manera elemental, se obtiene

$$\sum_{k\in K} a''_k b''_k = \sum_{i\in I}\left(\sum_{j\in J} a_i a'_j b_i b'_j\right) = \sum_{i\in I} a_i \left(\sum_{j\in J} a'_j b'_j\right) b_i = \sum_{i\in I} a_i b_i = 1$$

Las otras igualdades son análogas, por ejemplo con $g$,

$$\sum_{k\in K} a''_k g(b''_k) = \sum_{i\in I}\left(\sum_{j\in J} a_i a'_j g(b_i)g(b'_j)\right) = \sum_{j\in J} a'_j\left(\sum_{i\in I} a_i g(b_i)\right) g(b'_j) = \sum_{j\in J} a'_j,0.g(b'_j) = 0$$

Se observa que la commutatividad de $A$ ha sido utilizada.

La demostración del teorema 5.1 está casi terminada:

$1 \Rightarrow 2$.

Sea $\mathcal{M}$ un ideal maximal, $g \in G$, si $x - g(x) \in \mathcal{M}$ para todo $x$, en particular $1 = 1 - 0 = \sum_i a_i(b_i - g(b_i)) \in \mathcal{M}$, lo que es absurdo.

$2 \Rightarrow 1$.

Sea $g \in G$, $g \neq Id$ y consideremos el ideal generado por los elementos de la forma $x - g(x)$. Por hipótesis, no está contenido en ningún ideal maximal, entonces coincide con $A$.

A partir del primer lema, se pueden encontrar elementos $a_i$, $b_i$ (que eventualmente dependen de $g$ que verifican la condición $\sum_i a_i b_i = 1$ y $\sum_i a_i g(b_i) = 1$. Pero el segundo lema nos dice como recolectar los elementos correspondientes a cada $g$ para tener la misma fórmula para los diferentes $g$, pero con el mismo paquete de elementos $a_i$, $b_i$ (la condición $|G| < \infty$ es esencial).

## 5.2. Subgrupos cíclicos

Como corolario del segundo lema se tiene la proposición siguiente:

**Proposición 5.4.** *Sea $A$ un anillo conmutativo íntegro y $G$ un subgrupo finito de automorfismos de $A$. Entonces la extensión $A|A^G$ es Galois, si y solamente si para todo subgrupo cíclico $C \subseteq G$, la extensión $A|A^C$ es Galois.*

*Demostración:* Se ha ya probado sin ninguna hipótesis una de los implicaciones (proposición 3.9).

Como se supuso integridad, no nos preocupamos de la traza. Si se buscan elementos $a_i$, $b_i$ tales que $\sum_i a_i b_i = 1$ y para todo $g$, $\sum_i a_i g(b_i) = 1$, por el lema se sabe que alcanza con encontrar tales elementos para cada $g$ en particular, y eso es posible pues se supuso para cada $g$, $A$ es una extensión Galois de $A^{\langle g\rangle}$.

**Ejemplo:** Sea $A := k[a,b,c,d]/\langle ad - bc - 1\rangle$, el álgebra de funciones regulares sobre $\mathrm{SL}(2,k)$. Sea $G$ un subgrupo finito de $\mathrm{SL}(2,k)$, y se supone también que $k$ es un cuerpo de caracteristique cero. En realidad, el ejemplo queda tal cual si se supone que el orden de $G$ sea inversible en $k$.

El grupo $G$ agctúa sobre $SL(2,K)$ por traslación a izquierda, y por lo tanto actúa por automorfismos de álgebra sobre $A$. Por ejemplo, si $g \in G$ es la matriz $\begin{pmatrix} x & y \\ z & t \end{pmatrix}$, la acción de $g$ sobre los generadores de $A$ está dada por:

$$g(a) = xa + yc \;\;;\;\; g(b) = xb + yd$$
$$g(c) = za + tc \;\;;\;\; g(d) = zb + td$$

Se afirma que esta acción es Galois.

*Demostración:* A partir de la proposición, alcanza con ver que la extensión associada a cada subgrupo cíclico es Galois. Se supone entonces, sin pérdida de generalidad, que el grupo $G$ es cíclico, generado por un elemento $g$. Por la proposición 3.6 y considerando la clausura algebraica de $k$, se puede suponer también que $k$ contiene todas los raíces $|g|$-ésimas de la unidad, por lo tanto $g$ es diagonalizable. Suponemos entonces que $g$ actúa de manera diagonal, es decir, $g = \begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix}$, donde $w$ es un raíz $|g|$-ésima primitiva de la unidad. Reescribimos la fórmula de la acción para un tal $g$:

$$g(a) = wa \;\;;\;\; g(b) = wb$$
$$g(c) = w^{-1}c \;\;;\;\; g(d) = w^{-1}d$$

Si se define el ideal $I_g := \langle x - g(x) \ : \ x \in A \rangle$, hay que ver que contiene el elemento 1.

Se toma $x_1 = a$, $x_2 = b$, entonces $x_1 - g(x_1) = (1-w)a$, $x_2 - g(x_2) = (1-w)b$. Esto muestra que $a, b \in I_g$, y entonces $1 = ad - bc \in I_g$.

Se verá en la subsección siguiente, una generalización de ese resultado, con un álgebra de Hopf conmutativa de tipo finito en lugar del anillo de funciones sobre $\mathrm{SL}(2,k)$

Le teorema 5.1 da un interpretación geométrica de la condición Galois. Se puede definir el subconjunto de maximales:

$$\mathcal{Z} := \{\mathcal{M} \subset A \text{ maximal } / \exists g \in G \text{ con } \langle (x - g(x)) : x \in A \rangle \subseteq \mathcal{M}\}$$

Por su definición misma, $\mathcal{Z}$ es un cerrado Zariski de $\mathrm{SpecMax}(A)$, de hecho $\mathcal{Z} = \cup_{g \in G} \mathcal{V}(I_g)$ donde $I_g = \langle (x - g(x)) \ : \ x \in A \rangle$.

Con esta notación, $A$ es una extensión Galois de $A^G$ si y solamente si $\mathcal{Z} = \emptyset$. En el caso general, se sabe que, si $A$ es íntegra, entonces $\mathcal{Z}$ esta contenido en una hipersuperficie de $\mathrm{SpecMax}(A)$ (ver proposición 3.8), entonces el complemento de $\mathcal{Z}$ es siempre un abierto no vacío. Si $A$ es regular, el conjunto $\mathcal{Z}/G \in \mathrm{SpecMax}(A^G)$ es un cerrado que contiene al cerrado de puntos singulares de $A^G$ (ver corolario 3.4).

**Ejemplo:** Sea $A = k[x_1, ..., x_n]$ con $k$ un cuerpo, y $G$ un subgrupo finito de $\mathrm{GL}(n,k)$ actuando naturalmente en $A$. Si $p \in A$ es un polinomio y $g \in G$, entonces el coeficiente independiente de $p$ y $g(p)$ es el mismo, es decir $p(0) = g(p)(0)$. Por lo tanto $(p - g(p)) \in \langle x_1, \ldots, x_n \rangle$ para todo $p \in A$ y para todo $g \in G$, entonces el par $(k[x_1, \ldots, x_n], G)$ no es *nunca* Galois, el cerrado $\mathcal{Z}$ contiene siempre al cero.

## 5.3. Acción por traslación de un subgrupo finito de un grupo afin

El objetivo de esta subsección es el de mostrar que si $G$ es un subgrupo finito de un grupo algebraico afin, entonces la acción de $G$ por traslacion define sobre el anillo del grupo algebraico, una acción que es Galois. El teorema principal es 5.5. Antes de abordar ese teorema, se hace un pequeño repaso sobre las álgebras de Hopf $k[G]$ y $k^{(G)}$:

Sea $k$ un cuerpo y $G$ un grupo finito, entonces el álgebra de grupo $k[G]$ es un álgebra de Hopf, con la estructura $\Delta(g) = g \otimes g$, $\epsilon(g) = 1$, y $S(g) = g^{-1}$, donde $g \in G$. Como $G$ es finito, el álgebra $k[G]$ tiene dimension finita sobre $k$, y su dual es un álgebra de Hopf, que es precisamente $k^{(G)}$. Las funciones $\{\delta_g\}_{g \in G}$ forman una base de $k^{(G)}$ que es la base dual de la base standard de $k[G]$. La comultiplicación en $k^{(G)}$ está definida por $\Delta(\delta_g) = \sum_{x \in G} \delta_{gx^{-1}} \otimes \delta_x$, la antípoda $S(\delta_g) = \delta_{g^{-1}}$, y la counidad $\epsilon(\delta_g) = \delta_g(e) = \delta_{g,e}$.

Como un álgebra es dual de la otra, la categoría de $k[G]$-módulos (a izquierda) se identifica con la categoría de $k^{(G)}$-comódulos (a derecha). Si $M$ es un $k$-espacio vectoriel, los estructuras de módulo y comódulo están ligadas por la fórmula:

$$\rho^+(m) = m_0 \otimes m_{+1} = \sum_{g \in G} g(m) \otimes \delta_g$$

Por lo tato, si comenzamos por ejemplo con $M$ un $k^{(G)}$ comódulo (a derecha), la acción de $G$ (a izquierda) sobre $M$ se reencuentra con

$$g(m) := m_0 . m_{+1}(g)$$

Si $A$ es una $k$-álgebra, la fórmula anterior establece una correspondence biunívoca entre las $k^{(G)}$-comódulo álgebras y las $k[G]$-módulo álgebras, es decir, las $k$-álgebras provistas de una acción de $G$ por automorfismos de álgebra.

Recordamos también que un álgebra $A$ que es además un $k^{(G)}$-comódulo se dice un $k^{(G)}$-comódulo álgebra si y solamente si el morfismo multiplicación $A \otimes A \to A$ es un morfismo de $k^{(G)}$-comódulos (con la estructura diagonal en $A \otimes A$).

El enunciado del teorema es el siguiente:

**Teorema 5.5.** *Sea $H$ una $k$-álgebra de Hopf commutativa de tipo finito (como $k$-álgebra), y $\pi : H \to k^{(G)}$ un epimorfismo de álgebras de Hopf ($G$ un grupo finito). Se assume también o bien* $\mathrm{ch}(k) = 0$ *o bien $H$ íntegra (i.e. el grupo algebraico asociado a $H$ conexo). Entonces, con la acción de $G$ obtenida a partir de la estructura de $k^{(G)}$-comódulo dada por $\pi$ (i.e. $\rho^+ = (Id \otimes \pi) \circ \Delta : H \to H \otimes k^{(G)}$), se tiene que $H$ es una extensión Galois de $H^G$.*

**Observaciones:** Gracias a la proposición 3.6 y considerando (de ser necesario) $\overline{k}^{(G)}$ y $H \otimes_k \overline{k}$, se puede suponer sin pérdida de generalidad que $k$ es algebraicamente cerrado.

Se va a utilizar la caracterización de extensión Galois dada por el teorema 5.1. La demostración está separada en dos lemas, pero antes de la demostración de esos dos lemas, se ve bien que si $\pi : H \to k^{(G)}$ es un morfismo de álgebras de Hopf, entonces $H$ es un $k^{(G)}$-comódulo álgebra. La acción de un elemento de $g$ sobre un elemento $a$ de $A$ está definida por

$$g(a) = a_0.a_{+1}(g) = a_1.\pi(a_2)(g)$$

Un epimorfismo de álgebras de Hopf $H \to k^{(G)}$ se corresponde con una inclusión de $G$ en el espectro maximal de $H$, es decir a un subgrupo finito del grupo algebraico afin definido por $H$. La comultiplicación en un álgebra de Hopf se corresponde a la multiplicación del grupo, entonces en nuestro caso, el morfismo de estructura de $H$ como $k^{(G)}$-comódulo se corresponde a la multiplicación por los elementos de $G$, es decir a la acción por traslación.

**Lema 5.6.** *Mismas hipótesis que en el teorema 5.5 y se asume $k = \overline{k}$. Si $\mathcal{M}$ es un ideal maximal de $H$, y $g \in G$, entonces $g^{-1}(\mathcal{M}) = \mathcal{M}$ si y solamente si $\epsilon = \epsilon \circ g$.*

*Demostración:* $\Rightarrow$)

Como el cuerpo es algebraicamente cerrrado y $H$ es una $k$-álgebra de tipo finito, el conjunto de los ideales maximales coincide con el conjunto de los núcleos de morfismos de álgebras $\phi : H \to k$. Sea entonces $\phi$ un morfismo de álgebras tal que $\mathcal{M} = Ker(\phi)$. Como $g^{-1}(\mathcal{M}) = \mathcal{M}$ entonces $\phi = \phi \circ g$, eso implica que

$$(\phi \circ S) * \phi = (\phi \circ S) * (\phi \circ g)$$

A la izquierda se obtiene $\epsilon$, pues todo morfismo de $k$-álgebras $\phi : H \to k$ es inversible con respecto a la convolución, y su inverso es justamente $\phi \circ S$. Se aplica ahora el término a derecha en un elemento $a \in A$ y se obtiene de esta manera:

$$\epsilon(a) = \phi(S(a_1)).\phi(g(a_2)) = \phi(S(a_1).g(a_2))$$

que, con la fórmula de la acción $g(a) = a_1.\pi(a_2)(g)$ es igual a

$$\phi(S(a_1).a_2.\pi(a_3)(g)) = \phi(\epsilon(a_1).\pi(a_2)(g)) = \epsilon(a_1).\pi(a_2)(g) = \epsilon(a_1.\pi(a_2)(g)) = \epsilon(g(a))$$

$\Leftarrow$)

Se supone ahora $\epsilon = \epsilon \circ g$. Observamos que si $\mathcal{M} = Ker(\epsilon)$, la igualdad $\epsilon = \epsilon \circ g$ implica automáticamente $\mathrm{Ker}(\epsilon) = g^{-1}(\mathrm{Ker}(\epsilon))$.

Sea $\mathcal{M}$ un ideal maximal arbitrario, entonces es el núcleo de un morfismo $\phi : H \to k$. Como $\epsilon = \epsilon \circ g$, haciendo el produicto de convolución con $\phi$ se obtiene $\phi * \epsilon = \phi * (\epsilon \circ g)$. Como $\epsilon$ es la unidad con respecto a la convolución, el primer término es igual a $\phi$. El segundo, evaluado en un elemento $a$ de $H$ es igual a

$$\phi(a_1).\epsilon(g(a_2)) = \phi(a_1).\epsilon(a_2.\pi(a_3)(g)) = \phi(a_1).\epsilon(a_2).\pi(a_3)(g) =$$

$$= \phi(a_1.\epsilon(a_2).\pi(a_3)(g)) = \phi(a_1.\pi(a_2)(g)) = \phi(g(a))$$

Esto muestra que $\phi = \phi \circ g$, y en consecuencia $\mathcal{M} = \mathrm{Ker}(\phi) = \mathrm{Ker}(\phi \circ g) = g^{-1}(\mathrm{Ker}(\phi)) = g^{-1}(\mathcal{M})$.

**Lema 5.7.** *Mismas hipótesis que en el lema anterior, si $g \in G$, $g \neq e$ entonces $\epsilon \circ g \neq \epsilon$.*

*Demostración:* dado un elemento $x \in G$, como $\pi$ es sobreyectivo, se puede encontrar $a \in H$ tal que $\pi(a) = \delta_x$. Se fija un elemento $a$ con esta propiedad.

Como $g(a) = a_1.\pi(a_2)(g)$, si aplicamos $\pi$ obtenemos:

$$\pi(g(a)) = \pi(a_1.\pi(a_2)(g)) = \pi(a_1).\pi(a_2)(g) = \pi(a)_1.\pi(a)_2(g) = \sum_{y\in G} \delta_{xy^{-1}}.\delta_y(g) = \delta_{xg^{-1}}$$

A su vez, aplicando $\epsilon$ se obtiene:

$$\epsilon(\pi(g(a))) = \epsilon(\delta_{xg^{-1}}) = \delta_{xg^{-1}}(e) = \delta_{xg^{-1},e}$$

Por otra parte, si se calcula $\epsilon(a)$, como $\pi$ es un morfismo counitario:

$$\epsilon(a) = \epsilon(\pi(a)) = \epsilon(\delta_x) = \delta_x(e) = \delta_{x,e}$$

Vemos claramente que eligiendo $x = g$ (es decir $a \in H$ tal que $\pi(a) = \delta_g$) entonces $\epsilon(g(a)) = \delta_e(e) = 1$, mientras que $\epsilon(a) = \delta_g(e) = 0$ cuando $g \neq e$.

**Observación:** A partir de esos dos lemas, la demostración del teorema es casi evidente. Si se elige $\mathcal{M}$ un ideal maximal y $g \neq e$ entonces $g(\mathcal{M}) \neq \mathcal{M}$ y por lo tanto existe un elemento $m \in \mathcal{M}$ tal que $g(m) \notin \mathcal{M}$, luego $m - g(m)$ no puede pertenecer a $\mathcal{M}$.

# 6. Anillos simples

## 6.1. Simplicidad de los productos cruzados

Se recuerda aquí una proposición sobre los anillos simples que se encuentra en el Lect.N.Math. de Montgomery sobre los anillos de invariantes [Mo]:

**Teorema 6.1.** *Sea $A$ un anillo simple y $G$ un subgrupo de automorfismos de $A$ tal que no contiene automorfismos interiores, salvo la identidad. Entonces $A * G$ es simple.*

*Demostración:* Sea $I \subset A * G$ un ideal bilátero no nulo. Si $x \in I$, $x = \sum_{g\in G} x_g.g$ (suma con soporte finito), se toma $x \neq 0$ en $I$ tal que su soporte tenga cardinal mínimo.

Se elige $g \in \text{sop}(x)$, y cambiando $x$ por $x.g^{-1}$ se puede suponer que $e = 1_G \in \text{sop}(x)$, se escribe $x$ en la forma

$$x = x_e.e + \sum_{g\neq e} x_g.g$$

con $x_g \in A$, $x_e \neq 0$.

Como $A$ es simple y $x_e \neq 0$, el ideal generado por $x_e$ es igual a $A$, por lo tanto existent $a_i, b_i \in A$ tales que $\sum_{i\in I} a_i x_e b_i = 1$. Se puede cambiar (sin agrandar el soporte de) $x$ por $\sum_{i\in I} a_i x b_i$ y suponer sin pérdida de generalidad que $x_e = 1$.

Si $\text{sop}(x) = e$ entonces $x = 1 \in I$ e $I = A$. Sino, sea $a \in A$ un elemento arbitrario, como $(ax - xa) \in I$ y $\text{sop}(ax - xa) \subset (\text{sop}(x) - \{e\})$, por minimalidad del cardinal del soporte se tiene necesariamente

$$ax - xa = 0 = \sum_{g\neq e} (ax_g - x_g g(a))g$$

Entonces, para todo $g$ en el soporte de $x$ vale la igualdad

$$ax_g = x_g g(a)$$

Vemos en primer lugar que $x_g.A$ es igual a $A.x_g$, y por lo tanto igual a $A.x_g.A$, que a su vez es igual a $A$ porque $x_g \neq 0$ y $A$ es simple.

Hemos demostrado de esta manera que $x_g$ es una unidad, y podemos resolver la ecuación $ax_g = x_g g(a)$, lo que implica la fórmula

$$(x_g)^{-1} a x_g = g(a)$$

para todo $g \in \text{sop}(x)$ y todo $a \in A$. Pero $G$ no tiene automorfismos interiores salvo la identidad, entonces $g = Id$ y la demostración queda terminada.

### El ejemplo de cuerpo

Volvemos a los morfismos del contexto de Morita:

$$\mathrm{Tr} : A \otimes_{A*G} A \to A^G$$

$$\beta : A \otimes_{A^G} A \to A * G$$

Se quiere encontrar condiciones fáciles de verificar que impliquen la sobrejectividad de esos dos morfismos.

Como Tr y $\beta$ son morfismos de bimódulos, sus imágenes son ideales biláteros. La situación más simple posible para ver si al menos uno de esas morfismos es sobrejectivo es cuando no hay demasiados ideales biláteros. El ejemplo el más fácil es cuando $A$ es un cuerpo. Como un cuerpo es conmutativo, los automorfismos nunca son interiores, luego de la proposición anterior $A * G$ es simple, entonces $\beta$ (como no es nulo) es sobreyectivo. Se puede o bien utilizar el teorema de Dedekind sobre la independencia lineal de automorfismos diferentes, lo que implica $\mathrm{tr} \neq 0$, por lo tanto sobrejectivo también. O bien se puede utilizar el teorema 4.3 que nos dice que si $A$ es íntegra, la sobrejectividad de $\beta$ implica la suryectividad de tr.

Se tiene de todas maneras un ejemplo no conmutativo fundamental:

## 6.2. Ejemplo de operadores diferenciales

Sea $A$ un anillo conmutativo íntegro regular, se supone también $\mathbb{Q} \subset A$. Si $G$ es un subgrupo de automorfismos de $A$, el grupo $G$ actúa también en el álgebra de operadores diferenciales $\mathrm{Diff}(A)$. Por razones de grado de filtración, es relativamente fácil de ver que los únicos automorfismos interiores de $\mathrm{Diff}(A)$ son las conjugaciones con respecto a unidades de $A$. Pero como $A$ es conmutativo, esos automorfismos interiores, restringidos a $A$ dan la identidad. Entonces la acción de $G$ sobre $\mathrm{Diff}(A)$ (que proviene de un acción de $G$ sobre $A$) no contiene nunca automorfismos interiores.

Como se supuso $A$ íntegra regular, $\mathrm{Diff}(A)$ es simple, entonces $\mathrm{Diff}(A) * G$ es simple y se tiene que, bajo esas hipótesis, $\mathrm{Diff}(A) * G$ es *siempre* equivalente Morita a $\mathrm{Diff}(A)^G$, es decir, $\mathrm{Diff}(A)$ es una extensión Galois de $\mathrm{Diff}(A)^G$.

## 6.3. Ejemplo con matrices I

Observamos que en el teorems 6.1 la hipótesis de que $G$ no tenga automorfismos interiores no es técnica, sino en general necesaria. Se tiene el ejemplo siguiente:

Sea $k$ un cuerpo (característica arbitraria), $A := M_2(k)$, los matrices $2 \times 2$ con coeficientes en $k$. El anillo $A$ es simple (por ejemplo porque es equivalente Morita a $k$). Sea $G = \mathbb{Z}/2\mathbb{Z}$, designamos $\sigma$ a su generador, que por definición lo hacemos actuar en $A$ por conjugación por la matriz

$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Observamos que $\mathrm{Aut}_k(M_3(k)) = \mathrm{InAut}(M_3(k))$. (Una razón es por ejemplo la equivalencia Morita, aplicada a $\mathrm{Pic}_k(M_n(k)) = \mathrm{Pic}_k(k) = \{1\}$ y sabiendo que para cualquier $k$-álgebra $A$, $\mathrm{Aut}_k(A)/\mathrm{InAut}(A) \hookrightarrow Pic_k(A)$.)

De manera elemental, se ve que si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, entonces $XMX = \begin{pmatrix} d & c \\ b & a \end{pmatrix}$. Las matrices invariantes son entonces aquellas que verifican $a = d$ y $b = c$, es decir, las que son de la forma $a.I + b.X$. Forman una subálgebra de dimensión (sobre $k$) igual a dos. Se tiene evidentemente un isomorfismo de $k$-álgebras $A^G \cong k[X]/(X^2 - 1)$, y como el polinomio $X^2 - 1$ se factoriza sobre $\mathbb{Z}$, entonces para cualquier cuerpo $k$, $A^G$ *no* es simple.

Si se calcula la traza de la matriz $E_{11}$ (la matriz que tiene ceros en todos lados salvo en el lugar 11, donde hay un 1), se obtiene $\mathrm{tr}(E_{11}) = E_{11} + XE_{11}X = E_{11} + E_{22} = I$. Se ve por lo tanto que el morfismo tr es suryectivo, aún en característica 2.

Nos preguntamos si $A * G$ es o no simple. Si $A * G$ fuera simple, entonces $\beta$ sería suryectiva, y por lo tanto $A * G$ seria equivalente Morita a $A^G$. Pero $A^G$ no es simple, y la simplicidad es un invariante Morita, eso es absurdo y por lo tanto $A * G$ *no* es simple.

Queda aún sin respomder el problema de determinar si $A^G$ y $A * G$ son equivalentes Morita o no, y la respuesta es si.

Para estudiar la sobreyectividad de $\beta$ planteamos lo mismo que en los ejemplos sobre $k[x]$, es decir, se encuentran generadores de $A$ como $A^G$-módulo (por ejemplo a derecha) y asi se reduce la escritura de un elemento típico de $A \otimes_{A^G} A$. En ese caso, si se consideran los matrices $E_{11}$ y $E_{12}$, se pueden verificar las identidades siguientes:

$$XE_{11}X = E_{22} = 1 - E_{11}$$

$$XE_{12}X = E_{21} = X - E_{12}$$

$$E_{11}^2 = E_{11} \ ; \ E_{12}^2 = 0$$

$$XE_{11} = E_{21} = X - E_{12} \ ; \ E_{11}X = E_{12}$$

$$XE_{12} = E_{22} = 1 - E_{11} \ ; \ E_{12}X = E_{11}$$

En particular, $A = I.A^G \oplus E_{11}A^G$ como $A^G$-módulos a derecha, y todo elemento de $A \otimes_{A^G} A$ puede se escribir (y de manera única) $I \otimes M + E_{11} \otimes N$, con $M$ y $N$ en $A$. Hay que resolver entonces el sistema de ecuaciones:

$$M + E_{11}N = I$$

$$M + XE_{11}XN = 0$$

De la segunda ecuación obtnemos $M = -E_{22}N$, si se reemplaza en la primera se tiene

$$-E_{22}N + E_{11}N = I$$

Y vemos claramente que $-E_{22}N + E_{11}N = (E_{11} - E_{12})N = I$ tiene solución, con $N = E_{11} - E_{22}$. Si se toma ahora $a_1 = I$, $a_2 = E_{11}$, $b_1 = -E_{22}(E_{11} - E_{22}) = E_{22}$, $b_2 = E_{11} - E_{22}$ se tiene que los $a_i$, $b_i$ que implican la sobreyectividad de $\beta$.

## Ejemplo con Matrices II

Este contra-ejemplos fue tomado de [A-R-S].

Sea $A = M_3(k)$ con $k$ un cuerpo de característica 2, $G = \mathbb{Z}/2\mathbb{Z}$, que actúa sobre $A$ por conjugación por la matriz

$$X := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

Se verifica $X^2 = 1$, entonces esta matriz define una acción de $G$. Se puede hacer el cálculo explícito de esta acción:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} . \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} . \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} a+c & b+c & c \\ d+f & e+f & f \\ a+d+g+c+f+i & b+e+h+c+f+i & c+f+i \end{pmatrix}$$

Si se llama $M$ a la matriz genérica anterior, se ve que $\mathrm{tr}(M) = M + XMX =$

$$\begin{pmatrix} c & c & 0 \\ f & f & 0 \\ a+d+c+f+i & b+e+c+f+i & c+f \end{pmatrix}$$

lo que muestra que la traza de ningún elemento de $M_3(k)$ es igual a uno.

De todas maneras, uno se puede preguntar por los $a_i$ y $b_i$. Observamos primero que

$$M_3(k)^G = \left\{ \begin{pmatrix} a & b & 0 \\ a+i & b+i & 0 \\ g & h & i \end{pmatrix} \ : \ a, b, g, h, i \in k \right\}$$

Si llamamos

$$B_1 := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad B_1' := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad B_2 := \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad B_3 := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

es claro que generan $A = M_3(k)$ como $A^G$-módulo a izquierda. De hecho, $B_1'$ pertenece al $A^G$-submódulo generado por $B_1$, y por lo tanto si existen $a_i$, $b_i$ de la definición de Galois, se puede suponer que los $b_i$ son los $B_i$ que acabamos de definir.

Con exactamente las mismas técnicas que en el ejemplo anterior se llega a ecuaciones para los $A_i$, salvo que en este caso no hay unicidad. Pero de todas maneras, se puede verificar que, por ejemplo con

$$A_1 := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} \quad A_2 := \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad A_3 := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

se tiene $A_1.B_1 + A_2.B_2 + A_3.B_3 = 1$ y $A_1.X.B_1.X + A_2.X.B_2.X + A_3.X.B_3.X = 0$.

Este contra-ejemplo muestra que la sobreyectividad de Tr no es una consecuencia de la sobreyectividad de $\beta$, y por lo tanto que el enunciado no conmutativo análogo al teorema 4.3 es falso. Un enunciado verdadero que generalice el teorema 4.3 no es evidente.

### Ejemplo con los cuaterniones

Sea $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ el álgebra (de división) de los números cuaterniones. Es decir, $\mathbb{H}$ es el $\mathbb{R}$-espacio vectorial de dimensión 4, con base $\{1, i, j, k\}$, con la multiplicación determinada por $\mathbb{R}$-bilinealidad, 1 es el elemento neutro, $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$.

Si consideramos $\sigma$ la transformación $\mathbb{R}$-lineal determinada por $\sigma(1) = 1$, $\sigma(i) = i$, $\sigma(j) = -j$, y $\sigma(k) = -k$, se puede ver de manera elemental que $\sigma$ es multiplicativa, y que $\sigma^2 = Id$, por lo tanto $\sigma$ define una acción por automorfismos de $\mathbb{Z}/2\mathbb{Z}$ en $\mathbb{H}$. Siendo la acción "diagonal", rapidamente vemos que $\mathbb{H}^\sigma = \mathbb{R} \oplus \mathbb{R}i = \mathbb{C}$.

Si consideramos $a_1 = 1$, $b_1 = 1/2$ $a_2 = j$, $b_2 = j/2$, obtenemos:

$$a_1b_1 + a_2b_2 = 1{,}1/2 + j(-j/2) = 1/2 + 1/2 = 1$$

y a su vez

$$a_1\sigma(b_1) + a_2\sigma(b_2) = 1{,}1/2 + j.j/2 = 1/2 - 1/2 = 0$$

por lo tanto, $\mathbb{H}$ es una extensión Galois de $\mathbb{C}$.

Si nos preguntamos en qué medida es posible "reconstruir" a $\mathbb{Z}/2\mathbb{Z}$ a partir de $\mathbb{H}$ y $\mathbb{C}$, vemos que la forma naïve no funciona. Con esto queremos decir lo siguiente:

Es claro que $\sigma \in \mathrm{Aut}(\mathbb{H})$ y que $\sigma|_{\mathbb{C}} = Id_{\mathbb{C}}$, pero si buscamos todos los automorfismos con esa propiedad, vemos que hay muchos mas.

En principio, si $u \in \mathbb{H}$ es una unidad (o sea $u \neq 0$, porque $\mathbb{H}$ es un anillo de división), se tiene el automorfismo interior asociado $a \mapsto uau^{-1}$. Este automorfismo restringido a $\mathbb{C}$ dará la identidad si y sólo si $u \in \mathbb{C}$. A su vez, los elementos que inducen automorfismos interiores triviales son los del centro, que en este caso es $\mathbb{R}$, por lo tanto los automorfismos interiores que fijan $\mathbb{C}$ forman un grupo isomorfo a $\mathbb{C}^*/\mathbb{R}^* \cong S^1/\{\pm 1\} \cong S^1$, que es un grupo infinito.

Por otra parte, *todos* los automorfismos de $\mathbb{H}$ son interiores (porque por ejemplo $\mathrm{Pic}_{\mathbb{R}}(\mathbb{H}) = \mathrm{Pic}_{\mathbb{R}}(\mathbb{R}) = \{1\}$), por lo tanto, si consideramos "triviales"a los automorfismos interiores, nos quedamos sin automorfismos, es decir $\mathrm{Out}_{\mathbb{R}}(\mathbb{H}) = \{1\} \neq \mathbb{Z}/2\mathbb{Z}$.

Notamos finalmente que $\sigma$ coincide con la conjugación por $i$.

## 7. Separabilidad

El punto de vista adoptado por Ingraham y Demeyer en [D-I] es el de generalizar, para los anillos conmutativos, la noción de separabildad y normalidad, y entonces definir una extensión Galois como una extensión "normal y separable".

En el caso no conmutativo, la separabildad es más o menos clara, pero la noción de normalidad (con la que se quiere principalmente obtener $\mathrm{Aut}_{A^G}(A) = G$) es menos clara (ver el ejemplo de los cuaterniones).

Se recuerda que si $f : R \to S$ es un morfismo de anillos conmutativos, se dice que $S$ es $R$ separable si $S$ es un $S \otimes_R S$-módulo proyectivo. Observamos que en el caso no conmutativo, si la imagen de $f$ no está contenida en el centro de $S$, entonces $S \otimes_R S^{op}$ no es (al menos de manera evidente) un anillo. Hay, de todas formas, propiedades parecidas a la "separabildad" cuando $R$ no es conmutativo. De cualquier manera, en el caso conmutativo, se tienen los resultados siguientes:

**Teorema 7.1.** *Sea $A$ un anillo conmutativo, $G$ un grupo finito de automorfismos de $A$ tal que $A$ es una extensión Galois de $A$, entonces $A$ es $A^G$-separable.*

*Demostración:* por hipótesis, $\beta : A \otimes_{A^G} A \to A * G$ es un isomorfismo de $A * G$-bimódulos, en particular es un isomorfismo de $A$-bimódulos. A traves de este isomorfismo, la multiplicación $m : A \otimes_{A^G} A \to A$ se identifica con la proyección $A * G = \oplus_{g \in G} A.g \to A.Id = A$ en la componente de la identidad. Este morfismo claramente se escinde como morfismo de $A$-bimódulos, $A$ es un sumando directo de $A \otimes_{A^G} A$ y por lo tanto $A \otimes_{A^G} A$-proyectivo.

Remarcamos que la inclusión $A \to \oplus_{g \in G} A.g = A * G$ que funciona como sección de la multiplicación $A \otimes_{A^G} A \to A$ (luego de la identificación que da $\beta$) se escribe como $a \mapsto a.Id \mapsto a \sum_i a_i \otimes b_i$. Por lo tanto la condición de separabilidad sigue siendo verdadera si se utiliza solamente la mitad de la definición de Galois correspondiente a los $a_i$, $b_i$. El elemento $e := \sum_i a_i \otimes b_i$ es un elemento de separabildad de $A \otimes_{A^G} A$.

Para el caso no conmutativo en general, se recuerda un enunciado que se encuentran en [A-R-S], pero sin demostración. Damos aquí también la demostración (que está contenida en [C-Q]).

**Proposición 7.2.** *Sea $f : R \to S$ un morfismo de anillos (no necesariamente conmutativos). Utilizando las estructuras de $R$-módulo (a derecha, a izquierda, o de bimódulo) de $S$ obtenidas via $f$, los condiciones siguientes son equivalentes:*

1. *La multiplicación $S \otimes_R S \to S$ admite una sección que es $S$-lineal a izquierda y a derecha simultaneamente.*
2. *Para todo $S$-módulo a izquierda $N$, existe un sección natural (con respecto a $N$) del morfismo de estructura $S \otimes_R N \to N$.*
3. *Para todo $S$-bimódulo $M$, si $D : S \to N$ es un derivación que se anula sobre $R$, entonces $D$ es interior.*

*Demostración:*

$1 \Rightarrow 2$. Sea $s : S \to S \otimes_R S$ un morfismo de $S$-bimódulos que escinda a la multiplicación. Denotamos $s(1) = \sum_i a_i \otimes b_i$, se tiene que para todo $x \in S$, $s(x) = xs(1) = s(1)x$, o bien

$$\sum_i xa_i \otimes b_i = \sum_i a_i \otimes b_i x$$

Si $N$ es un $S$-módulo a izquierda, se define

$$\begin{aligned} s_N : N &\to S \otimes_R N \\ n &\mapsto \sum_i a_i \otimes b_i n \end{aligned}$$

que es una sección del morfismo de estructura, pero además $s_N$ es $S$-lineal, de hecho, si $x \in S$ y $n \in N$:

$$s_N(xn) = \sum_i a_i \otimes b_i xn = \sum_i xa_i \otimes b_i n = xs_N(n)$$

La naturalidad con respecto a $N$ también es clara.

$2 \Rightarrow 1$. Tomamos $N = {}_SS$ como $S$-módulo a izquierda. Por hipótesis, existe una sección de la multiplicación

$$s_S : S \to S \otimes_R S$$

Que es $S$-lineal a izquierda. La linealidad a derecha es una consecuencia de la naturaldad, pues si $x \in S$, se puede considerar $r_x : S \to S$ la multiplicación a derecha por $x$, que es un morfismo $S$-lineal a izquierda. La naturaldad de la sección nos dice que $(Id \otimes r_x) \circ s_S = s_S \circ r_x$. Si se aplica esta identidad a un elemento $y \in S$ se obtiene $s_S(y)x = s_S(yx)$.

$1 \Rightarrow 3$ Con las mismas notaciones, $s(1) = \sum_i a_i \otimes b_i$ verifica $\sum_i a_i b_i = 1$ y $\sum_i xa_i \otimes b_i = \sum_i a_i \otimes b_i x$ para todo $x \in S$.

Se recuerda la construcción del $\Omega_R^{nc}(S)$, el bimódulo de 'diferenciales no conmutativos'.

Sea $M$ un $S$-bimódulo y $D : S \to M$ un derivación que es nula sobre $R$. Existe un bimódulo universal que se llama $\Omega_R^{nc}(S)$, que está definido por $\Omega_R^{nc}(S) := \mathrm{Ker}(m : S \otimes_R S \to S)$. La aplicación $d : S \to \Omega_R^{nc}(S)$ definida por $d(x) = 1 \otimes x - x \otimes 1$ es un derivación, que se anula sobre $R$, y la propiedad universal expresa la representatibildad del funtor de derivaciones $\mathrm{Der}_R(S, M) := \{D : S \to M$ derivación tal que $D(r) = 0 \ \forall r \in R\}$:

$$\mathrm{Hom}_{S\ bimod}(\Omega_R^{nc}(S), M) \cong \mathrm{Der}_R(S, M)$$

$$f \longmapsto f \circ d$$

Si $D : S \to M$ es una derivación que se anula sobre $R$, y $\sum_i x_i \otimes y_i \in \Omega_R^{nc}(S)$ (i.e. $\sum_i x_i y_i = 0$), el morfismo asociada es $\widetilde{D}(\sum_i x_i y_i) := \sum_i x_i D(y_i)$.

Observamos que como $\sum_i x_i y_i = 0$ y $D$ es una derivación, entonces $0 = D\left(\sum_i x_i y_i\right) = \sum_i x_i D(y_i) + \sum_i D(x_i) y_i$, de donde el se obtiene la fórmula

$$\widetilde{D}(\sum_i x_i y_i) = \sum_i x_i D(y_i) = -\sum_i D(x_i) y_i$$

Esto implica que $\widetilde{D}$ es $S$-lineal a derecha.

Se considera ahora nuetro caso, donde se tienen elementos $a_i$, $b_i$ en $S$ tales que $\sum_i xa_i \otimes b_i = \sum_i a_i \otimes b_i x$ para todo $x \in S$ y $\sum_i a_i b_i = 1$.

Sea $x \in S$, $D : S \to M$ una derivación que se anula sobre $R$, $\widetilde{D} : \Omega_R^{nc}(S) \to M$ el morfismo de $S$-bimódulos correspondiente.

Gracias a los propiedades de los $a_i$ y $b_i$ se tiene que, para todo $x \in S$, $\sum_i xa_i \otimes b_i = \sum_i a_i \otimes b_i x$, y trivialemente

$$\sum_i xa_i \otimes b_i - x \otimes 1 = \sum_i a_i \otimes b_i x - x \otimes 1$$

La ventaja de la última igualdad es que es una igualdad en $\Omega_R^{nc}(S)$. Aplicando $\widetilde{D}$ a los dos términos obtenemos

$$\sum_i xa_i D(b_i) - xD(1) = \sum_i a_i D(b_i x) - xD(1)$$

Como $D$ es una derivación $D(1) = 0$ y $D(b_i x) = b_i D(x) + D(b_i)x$, entonces

$$\sum_i xa_i D(b_i) = \sum_i a_i D(b_i)x + (\sum_i a_i b_i) D(x)$$

Como $\sum_i a_i b_i = 1$, si se llama $m_D := \sum_i a_i D(b_i)$, la fórmula anterior se convierte en

$$D(x) = x.m_D x - m_D.x = [x, m_D]$$

$3 \Rightarrow 1$

La derivación universal $d : S \to \Omega_R^{nc}(S)$ definida por $d(x) = 1 \otimes x - x \otimes 1$ se anula sobre $R$, luego por hipótesis es interior. Existe entonces $w \in \Omega_R^{nc}(S)$ tal que $d(x) = xw - wx$. Tenemos la igualdad

$$1 \otimes x - x \otimes 1 = xw - wx$$

que es cierta para todo $x \in S$. Como $w \in \Omega_R^{nc}(S)$, por definición de $\Omega_R^{nc}(S)$ se sabe que $m(w) = 0$. Denotemos $e := (1 \otimes 1) + w$, entonces $m(e) = 1$, y la ecuación anterior es equivalente a $xe = ex$. Una sección $S$-lineal a derecha y a izquierda de la multiplicación está dada entonces por $s(x) := x.e$.

**Corolario 7.3.** *Sea $A$ un anillo conmutativo, $M$ un $A$-módulo simétrico, $G$ un grupo finito de automorfismos de $A$ tal que $A$ es una extensión Galois de $A^G$. Entonces toda derivación $A^G$-lineal $D : A \to M$ es nula.*

Como segundo corolario, se obtiene el resultado siguiente:

**Corolario 7.4.** *Sea $A$ un anillo conmutativo, $G$ un grupo finito de automorfismos de $A$, y supongamos que $A$ es una extensión Galois de $A^G$. Si $D : A \to A$ es un derivación, entonces $D$ está unívocamente determinada por su restricción a $A^G$.*

*Demostración:* Sean $D$ y $D'$ dos derivaciones de $A$ en $A$ tales que $D|_{A^G} = D'|_{A^G}$. Entonces $D'' := D - D'$ se anula sobre $A^G$, o sea que $D$" es $A^G$-lineal. Como $A$ es $A$-simétrica, entonces $D - D' \equiv 0$, es decir $D = D'$.

Mostremos otro resultado sobre las extensiones separables que sera utilizado luego:

**Proposición 7.5.** *Sea $R$ un anillo conmutativo, $S$ una $R$-álgebra $R$-proyectiva que además es $R$-separable (i.e. $S$ es $S \otimes_R S^{op}$-proyectivo). Si $M$ es un $S$-módulo $R$-simétrico, y $d : R \to M$ un derivación, entonces existe $D : S \to M$ tal que $D|_R = d$.*

*Demostración:* Sea $B = S \oplus M$ que se considera como un anillo con multiplicación

$$(s, m)(se, m') := (ss', sm' + ms')$$

Como $M^2 = 0$ y $d : R \to M$ es un derivación, entonces el morfismo $\phi : R \to B$ definido por $\phi(r) = (r, d(r))$ es un morfismo de anillos y, via $\phi$, $B$ es una $R$-álgebra. La proyección

$$\pi : B \to S$$

$$(s, m) \mapsto s$$

es un morfismo de $R$-álgebras, con núcleo $M$. Como las extensiones $R$-splits de núcleo un $S$-bimódulo $M$ de cuadrado nulo de la $R$-álgebra $S$ están clasificadas por $H_R^2(S, M) = \mathrm{Ext}^2_{S \otimes_R S^{op}}(S, M)$, al suponer $S$ separable (i.e. $S \otimes_R S^{op}$-proyectivo) tenemos $H_R^2(S, M) = 0$ y la extensión de $R$-álgebras que se acaba de definir es trivial. Esto quiere decir que la proyección $B \to S$ admite una sección $f : S \to B$ donde $f$ es un morfismo de $R$-álgebras.

Notar que la proyección $B \to S$ es $R$-split porque $S$ se supuso $R$-proyectivo.

Como $f$ es una sección de la proyection, $f(s)$ se escribe necesariamente en la forma $f(s) = (s, D(s))$, y el hecho de que $f$ sea multiplicativo implica que $D : S \to M$ es una derivación. Pero además, como $f$ es un morfismo de $R$-álgebras, entonces $f|_R = \phi$, es decir, para todo $r \in R$, $f(r) = (r, D(r)) = \phi(r) = (r, d(r))$, o sea $D|_R = d$.

**Corolario 7.6.** *Sea $A$ un anillo conmutativo, $G$ un grupo finito de automorfismos de $A$, y supongamos que $A$ es una extensión Galois de $A^G$. Si $d : A^G \to A^G$ es un derivación, entonces su (única) extensión $D : A \to A$ verifica $gD = Dg$ para todo $g \in G$*

*Demostración:* A partir de la proposición anterior, se sabe que una extensión existe, pero se sabe también que está determinada por su valor sobre $A^G$.

Si $g \in G$, la aplicación $g^{-1}Dg : A \to A$ es también una derivación, y toma los mismos valores sobre $A^G$ (se utiliza que $d(A^G) \subseteq A^G$), entonces $D = g^{-1}Dg$.

# 8. Derivaciones invariantes, operadores diferenciales

Para las extensiones de Galois conmutativas, se tiene el resultado siguiente:

**Teorema 8.1.** *Sea $A$ un anillo conmutativo, $G$ un grupo finito de automorfismos de $A$, y supongamos que $A$ es una extensión Galois de $A^G$. Entonces la restricción induce un isomorfismo de $A^G$-módulos* $\mathrm{Der}(A)^G \cong \mathrm{Der}(A^G)$.

*Demostración:* Si $D \in \mathrm{Der}(A)^G$ (i.e. $Dg = gD\ \forall g \in G$), entonces $D(A^G) \subseteq A^G$. Esto muestra que la restricción define siempre (sin ninguna hipótesis) un morfismo $\mathrm{Der}(A)^G \to \mathrm{Der}(A^G)$. Ahora si se utiliza la hipótesis Galois, el resultado de extensión (Proposition 7.5) y de unicidad (Corolario 7.4, y 7.6 ) de derivaciones nos dice que ese morfismo es respectivamente suryectivo e inyectivo.

En el caso "geométrico", se tiene el resultado siguiente para los operadores diferenciales.

**Teorema 8.2.** *Sea $A$ un anillo íntegro y regular, $\mathbb{Q} \subseteq A$, $G$ un grupo finito de automorfismos de $A$, y supongamos que $A$ es una extensión Galois de $A^G$. Entonces* $\mathrm{Diff}(A^G) = \mathrm{Diff}(A)^G$.

*Demostración:* Existe siempre un morfismo de restricción $\mathrm{Diff}(A)^G \to \mathrm{Diff}(A^G)$, se verá que es inyectivo y sobreyectivo.

Como $A$ es regular y se está en característica cero, $\mathrm{Diff}(A)$ es simple, eso implica que $\mathrm{Diff}(A) * G$ es simple, y por invariancia Morita $\mathrm{Diff}(A)^G$ es simple también, entonces el morfismo restricción tiene que ser inyectivo.

La imagen de ese morfismo contiene a $A^G$ y las restricciones de $\mathrm{Der}(A)^G$, pero se sabe que $\{D|_{A^G} : D \in \mathrm{Der}(A)^G\} = \mathrm{Der}(A^G)$, entonces la imagen contiene a $A^G$ y a $\mathrm{Der}(A^G)$. Se sabe además que como $A$ es regular, bajo la condición Galois $A^G$ es también regular, esto implica que $\mathrm{Diff}(A^G)$ está generada (como álgebra) por $A^G$ y $\mathrm{Der}(A^G)$, y por lo tanto el morfismo es sobreyectivo.

El resultado de localización 3.8 hace que el corolario siguiente sea interesante:

**Corolario 8.3.** *Sea $A$ un anillo conmutativo íntegro, $G$ un subrupo finito de automorfismos de $A$. Sea $f \in A^G$ tal que $(A[f^{-1}], G)$ es Galois, entonces el núcleo y el conúcleo de la flecha natural* $\mathrm{Diff}(A)^G \to \mathrm{Diff}(A^G)$ *son $A^G$-módulos de $f$-torsión.*

*Demostración:* es una consecuencia inmediata del teorema anterior, y del hecho de que la localización de los operadores diferenciales se identifica con los operadores diferenciales del anillo localizado.

Observemos además que si $A$ es regular, por el argumento de la demostración anterior $\mathrm{Diff}(A)^G$ es simple, luego el morfismo restricción $\mathrm{Diff}(A)^G \to \mathrm{Diff}(A^G)$ es monomorfismo.

## Una generalización de los resultados sobre los derivaciones

Se han visto algunos resultados sobre los derivaciones en el caso Galois, pero qué se puede decir en el caso no necesariamente Galois?

Por ejemplo Levasseur muestra [Le] que si $A$ es un álgebra de polinomios a $n$ variables sobre un cuerpo $k$, y $G$ es un subgrupo finito de $\mathrm{GL}(n, k)$, toda derivación de $A$ en $A$ que es $A^G$ lineal, es nulo. Se sabe que en este ejemplo, $A$ no es nunca una extensión Galois de $A^G$, la demostración de Levasseur utiliza el hecho que $A$ sea suave (o que $\Omega^1(A)$ sea proyectivo, y por lo tanto sin torsión). Se propone una generalización de ese resultado, que utiliza solamente la integridad:

**Proposición 8.4.** *Sea $A$ un anillo conmutativo íntegro, $G$ un grupo finito de automorfismos de $A$. Si $M$ es un $A$-módulo simétrico sin torsion, entonces* $\mathrm{Der}_{A^G}(A, M) = 0$, *en particular* $\mathrm{Der}_{A^G}(A) = 0$.

*Demostración:* Por la proposición 3.8 existe $0 \neq f \in A^G$ tal que $A[f^{-1}]$ es una extensión Galois de $A^G[f^{-1}]$. Se tiene que $A[f^{-1}]$ es $A^G[f^{-1}]$ separable, entonces la homología de Hochschild de $A[f^{-1}]$ relativa a $A^G[f^{-1}]$ es nula para los grados positivos. En particular $\Omega^1_{A^G[f^{-1}]}A[f^{-1}] = 0$.

Como el módulo $\Omega^1$ es compatible con localización, se sabe que

$$0 = \Omega^1_{A^G[f^{-1}]}A[f^{-1}] = \Omega^1_{A^G}A[f^{-1}] = A[f^{-1}] \otimes_A \Omega^1_{A^G}A$$

Esto quiere decir que si $adb \in \Omega^1_{A^G}A$ entonces $\frac{a}{1}db = 0$ en $A[f^{-1}] \otimes_A \Omega^1_{A^G}A$, es decir que existe $n \in \mathbb{N}$ tal que $f^n adb = 0$. Hemos demostrado entonces que $\Omega^1_{A^G}A$ es de $f$-torsión.

Si $M$ es un $A$-módulo (simétrico) sin torsión, $\mathrm{Hom}_A(\Omega^1_{A^G}A, M) = 0$ por el siguiente argumento:

La multiplicación por $f$ es un monomorfismo en $M$, y si $\phi \in \mathrm{Hom}_A(\Omega^1_{A^G}A, M)$, dados $adb \in \Omega^1_{A^G}A$, $f^n adb = 0$ para $n \gg 0$ y

$$\phi(f^n adb) = f^n \phi(adb)$$

Esto que implica que $\phi(adb) = 0$ pues $f$ es un monomorfismo en $M$. Se tiene asi probado que $0 = \mathrm{Hom}_A(\Omega^1_{A^G}A, M) = \mathrm{Der}_{A^G}(A, M)$.

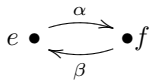
**Observación:** La generalización naïve de una fórmula para $\mathrm{Der}(A^G)$ análoga a la del teorema 8.1 en el caso Galois pero $A$ no necesariamente conmutativo (i.e. $\mathrm{Der}(A^G) = \mathrm{Der}(A)^G$) es falsa.

La dirección en la que se obtienen resultados es considerndo $\mathrm{Der}(A)/\mathrm{InnDer}(A) = HH^1(A)$, en vez de $\mathrm{Der}(A)$. Por invariancia morita, en el caso Galois, el resultado sobre cohomología de Hochchild nos dice que

$$\mathrm{Der}(A^g)/Inder(A^G) = \bigoplus_{\langle g \rangle \in \langle G \rangle} (\mathrm{Der}(A, A.g)/\mathrm{InnDer}(A, A.g))^{\mathcal{Z}_g}$$

No hay ninguna razón a priori para suponer que $H^1(A, A.g) = 0$ cuando $g \neq Id$. Veremos en la sección siguiente que este sí es el caso cuando $A$ es conmutativo. Para $A$ no conmutativo tenemos el siguiente ejemplo:

**Ejemplo:** Consideremos un quiver con dos vértices y dos flechas, cada una llendo de uno de los vértices hacia el otro.




Sea $k$ un cuerpo arbitrario y consideremos el algebra asociada al quiver anterior, con radical cuadrado cero.

Es decir, sea $A$ la $k$-álgebra de dimensión (sobre $k$) igual a 4 con base $\{e, f, \alpha, \beta\}$, con relaciones:

$$\begin{cases} e^2 = e & f^2 = f \\ ef = fe = 0 & e + f = 1 \\ e\alpha = \alpha = \alpha f & f\beta = \beta = \beta e \end{cases}$$

Y todos los demás productos igual a cero.

Consideremos $G$ el grupo cíclico de orden 2, $G = \{Id, t \ / \ t^2 = Id\}$ que hacemos actuar en $A$ a través de $t(e) = f$, $t(f) = e$, $t(\alpha) = \beta$ y $t(\beta) = \alpha$.

Esta acción es Galois porque

$$\mathrm{tr}(e) = e + t(e) = e + f = 1$$

por lo tanto hay un elemento de traza uno (sin importar la característica). Además

$$e.e + f.f = 1$$

$$e.t(e) + f.t(f) = 0$$

Caclularemos derivaciones en $A$, módulo derivaciones interiores.

Sea $D : A \to A$ una derivación. Si escribimos $D(e) = ae + bf + c\alpha + d\beta$, utilizando $e^2 = e$ obtenemos

$$D(e) = D(e^2) = eD(e) + D(e)e$$

esta ecuación se escribe como

$$ae + bf + c\alpha + d\beta = (ae + c\alpha) + (ae + d\beta)$$

y por lo tanto $a = b = 0$, es decir $D(e) = c\alpha + d\beta$.

Si consideramos la derivacion interior $D' := [-c\alpha + d\beta, -]$, tenemos $D'(e) = c\alpha + d\beta$, luego $D - D'$ se anula en $e$. Esto nos dice que, módulo una derivacion interior, podemos suponer que $D$ se anula en $e$.

Como $f = 1 - e$ y toda derivacion se anula en 1, se sigue que $D$ se anula en $f$. Concluimos entonces que $D$ es $ke \oplus kf$-lineal.

Si calculamos ahora $D(\alpha)$, por linealided sabemos que $D(\alpha) = D(e\alpha f) = eD(\alpha)f$, lo que implica que $D(\alpha)$ es un múltiplo de $\alpha$, digamos $D(\alpha) = \lambda\alpha$. De manera análoga $D(\beta) = \mu\beta$.

Si calculamos $D'' = [-, e]$ tenemos que $D''$ se anula en $e$ y en $f$, y que $D''(\alpha) = \alpha$, $D''(\beta) = -\beta$.

En característica distinta de dos esto nos dice que, módulo interiores, podemos suponer que $D(\alpha) = \lambda\alpha$ y $D(\beta) = \lambda\beta$, por lo tanto $\dim_k(\mathrm{Der}(A)/\mathrm{InnDer}(A)) \leq 1$.

Por otra parte $[-, f] = -[-, e]$, y los conmutadores con $\alpha$ o con $\beta$ *no* se anulan en $e$ y $f$, y *si* se anulan en $\alpha$ y $\beta$ asi que no nos sirven para modificar los valores de $D$ en $\alpha$ o en $\beta$. Se puede concluir entonces que $\dim_k(\mathrm{Der}(A)/\mathrm{InnDer}(A)) = 1$. A su vez, la derivacion hallada es $G$-invariante, asi que $\dim_k HH^1(A)^G = 1$.

En característica dos, tenemos que $D(\alpha) = \lambda\alpha$, $D(\beta) = \mu\beta$. La acción de $G$ intercambia $\lambda$ con $\mu$, que es una acción trivial módulo interiores (basta sumar $(\lambda + \mu).[-, e]$ para ir de una a la otra), por lo tanto $\dim HH^1(A)^G = \dim HH^1(A) = 1$.

Calculemos ahora $\mathrm{Der}(A^G)$. Como $A^G = k,1 \oplus k.(\alpha + \beta)$, llamemos $x := \alpha + \beta$, tenemos $A^G \cong k[x]/\langle x^2\rangle$.

Si $D : A^G \to A^G$ es una derivación, $D(1) = 0$, falta calcular $D(x) = a + bx$.

Aquí nuevamente hay diferencias dependiendo de la característica de $k$. Si $k$ tiene característica distinta de dos, entonces la ecuación $0 = D(x^2) = 2xD(x)$ equivale a $0 = xD(x) = ax$, por lo tanto $a = 0$, $D(x) = bx$ y obtenemos $\dim HH^1(A^G) = \dim \mathrm{Der}(A^G) = 1$.

Si $\mathrm{ch}(k) = 2$, tenemos $D(x^2) = 2xD(x) = 0$ sin importar el valor de $D(x)$, por lo tanto en este caso $\dim \mathrm{Der}(A^G) = 2$. Esto dice que $\mathrm{Der}(A^G)$ es estrictamente mayor que $(\mathrm{Der}(A)/\mathrm{InnDer}(A))^G$ pues este último tiene dimensión uno.

# 9. Homología de Hochschild, derivaciones, módulo de diferenciales, homología de De Rham

En esta sección se calculan los invariantes homológicos para extensiones de Galois conmutativas. El teorema siguiente se encuentra en [Lo], indicando a su vez que es una consecuencia del resultado principal en [G-W]. Aquí damos una demostración alternativa, en donde exhibimos una homotopía explícita para demostrar que ciertos grupos de homología son cero.

**Teorema 9.1.** *Sea $B$ un anillo conmutativo que contiene $\mathbb{Q}$, y $G$ un subgrupo finito de automorfismos de $B$ tal que $B$ es una extensión Galois de $B^G$. Entonces*

$$HH_*(B^G) = HH_*(B)_G$$

$$HH^*(B^G) = HH^*(B)^G$$

*para todo anillo de base $k \subset A^G$.*

Como $B$ es una extensión Galois de $B^G$ entonces $HH_*(B^G) = HH_*(B * G)$ y $HH^*(B^G) = HH^*(B * G)$. Para calcular la homología y cohomología de un producto cruzado se tiene una sucesión espectral, que en característica cero degenera en un isomorfismo:

$$HH_*(B * G) = \oplus_{<g>\in<G>} H_*(B, B.g)_{\mathcal{Z}_g}$$

$$HH_*(B * G) = \oplus_{<g>\in<G>} H^*(B, B.g)^{\mathcal{Z}_g}$$

donde $\mathcal{Z}_g$ es el centralisador de $g$ en $G$. La demostración del teorema se seguirá de la demostración de que los términos de esta suma correspondientes a los $g \neq 1$ son todos nulos.

Le lema fundamental es el siguiente:

**Lema 9.2.** *Sea $B$ una $k$-álgebra conmutativa, $g$ un automorfismo de $k$-álgebras de $B$ tal que existen elementos $a_i, b_i$ en $B$ ($i \in I$ un conjunto finito) con $\sum_{i\in I} a_i b_i = 1$ y $\sum_{i\in I} a_i g(b_i) = 0$. Entonces $H_n(B, B.b) = 0 = H^n(B, B.g)$ para todo $n$.*

*Demostración:* Se exhibe una homotopía de contracción en el complejo standard. El cálculo homológica es completamente análogo al cálculo cohomológico, se harán los calculos explícitos en el caso homológico.

Recordemos que la homología de $B$ a coeficientes en $B.g$ es la homología del complejo

$$\cdots \to B.g \otimes B^{\otimes n} \to \cdots \to B.g \otimes B \to B.g \to 0$$

con el diferencial dado por

$$b(ag, c_1, \ldots, c_n) = (ag(c_1), c_2, \ldots, c_n)+$$
$$+\sum_{i=1}^{n-1}(-1)^i(ag, c_1, \ldots, c_ic_{i+1}, \ldots, c_n) + (-1)^n(c_nag, c_1, \ldots, c_{n-1})$$

Se define la homotopía

$$s : Bg \otimes B^{\otimes n} \to Bg \otimes B^{\otimes n+1}$$
$$s(ag, c_1, \ldots, c_n) := \sum_{i\in I, k=1}^{n+1}(-1)^k(a_iag, c_1, \ldots, c_{k-1}, b_i, c_k, \ldots, c_n)$$

(en esta notación, el primer término es $(a_iag, b_i, c_1, \ldots, c_n)$ y el término $n+1$ es $(a_iag, c_1, \ldots, c_n, b_i)$.)

Antes de hacer el cálculo en general veamos qué sucede en los grados bajos:

A un elemento $ag$ en $Bg$ le corresponde el elemento

$$ag \mapsto \sum_{i\in I}(-1)(a_iag, b_i) \mapsto -\sum_{i\in I}a_iag(b_i) + \sum_{i\in I}b_ia_iag = ag$$

El cálculo en general no tiene sorpresas:

$$b(s(a, c_1, \ldots, c_n)) = b\left(\sum_{i\in I, k=1}^{n+1}(-1)^k(a_iag, c_1, \ldots, c_{k-1}, b_i, c_k, \ldots, c_n)\right) =$$

$$= \sum_{i\in I}\left(-(a_iag(b_i), c_1, \ldots, c_n) + \sum_{k=2}^{n+1}(-1)^k(a_iag(c_1), c_2, \ldots, c_{k-1}, b_i, c_k, \ldots, c_n)+\right.$$
$$+\sum_{k=1}^{n+1}\sum_{l=1}^{k-2}(-1)^k(-1)^l(a_iag, c_1, \ldots, c_lc_{l+1}, \ldots, c_{k-1}, b_i, c_k, \ldots, c_n)+$$
$$+\sum_{k=1}^{n+1}(-1)^k((-1)^k(a_iag, c_1, \ldots, c_{k-1}b_i, c_k, \ldots, c_n) + (-1)^{k+1}(a_iag, c_1, \ldots, c_{k-1}, b_ic_k, \ldots, c_n))+$$
$$+\sum_{k=1}^{n+1}\sum_{l=k}^{n-1}(-1)^k(-1)^{l+1}(a_iag, c_1, \ldots, c_{k-1}, b_i, c_k, \ldots, c_lc_{l+1}, \ldots, c_n)+$$
$$\left.\sum_{k=1}^{n}(-1)^{n+1}(-1)^k(c_na_iag, c_1, \ldots, c_{k-1}, b_i, c_k, \ldots, c_{n-1}) + (-1)^{n+1}(-1)^{n+1}(b_ia_iag, c_1, \ldots, c_n)\right)$$

Se puede ver que el último término es la identidad, el primer término es nulo, el término del medio se anula con el término de la izquierda.

Si se reescriben las sumas dobles se tiene que $bs(ag, c_1, \ldots, c_n) =$

$$= \sum_{i\in I}\left(\sum_{k=2}^{n+1}(-1)^k(a_iag(c_1), c_2, \ldots, c_{k-1}, b_i, c_k, \ldots, c_n)+ \qquad (I)\right.$$
$$\left.+\sum_{1\le l\le k-1\le n+1}(-1)^{k+l}(a_iag, c_1, \ldots, c_lc_{l+1}, \ldots, c_{k-1}, b_i, c_k, \ldots, c_n) + \quad (II)\right.$$

$$+\sum_{1\le k\le l\le n-1}(-1)^{k+l+1}(a_iag,c_1,\dots,c_{k-1},b_i,c_k,\dots,c_lc_{l+1},c_n)+\qquad (III)$$

$$\sum_{k=1}^{n}(-1)^{n+1}(-1)^k(c_na_iag,c_1,\dots,c_{k-1},b_i,c_k,\dots,c_{n-1})\Bigg)+(ag,c_1,\dots,c_n)\quad (IV)$$

Se calcula ahora la composición en el otro sentido:

$$s(b(a,c_1,\dots,c_n))=s(ag(c_1),c_2,\dots,c_n)+$$

$$+\sum_{l=1}^{n-1}(-1)^ls(ag,c_1,\dots,c_lc_{l+1},\dots,c_n)+(-1)^ns(c_nag,c_1,\dots,c_{n-1})=$$

$$=\sum_{i\in I}\sum_{k=2}^{n+1}(-1)^{k-1}(a_iag(c_1),c_2,\dots,c_{k-1},b_i,c_k,\dots,c_n)+\qquad (i)$$

$$+\sum_{i\in I}\sum_{l=1}^{n-1}\Bigg(\sum_{k=1}^{l}(-1)^l(-1)^k(a_iag,c_1,\dots,c_{k-1},b_i,c_k,\dots,c_lc_{l+1},\dots,c_n)+\qquad (ii)$$

$$+\sum_{k=l+2}^{n+1}(-1)^l(-1)^{k-1}(a_iag,c_1,\dots,c_lc_{l+1},\dots,c_{k-1},b_i,c_k,\dots,c_n)\Bigg)+\qquad (iii)$$

$$+\sum_{i\in I}\sum_{k=1}^{n}(-1)^n(-1)^k(a_ic_nag,c_1,\dots,c_{k-1},b_i,c_k,\dots,c_{n-1})\qquad (iv)$$

El término (i) corresponde a (I), el (iv) a (IV). El término (ii) se en va con (III) y el (iii) con (II).

**Observaciones:**

1. Si $M$ es un $B$-bimódulo, se dice que $M$ es $g$-central si y solamente si $m.b=g(b).m$ para todo $b\in B$, $m\in M$. Si $M$ es un tal bimódulo, el lema sigue siendo válido (con idéntica demostración) si se reemplaza $HH_*(B,B.g)$ por $HH_*(B,M)$ y $HH^*(B,B.g)$ por $HH^*(B,M)$.
2. La demostración del teorema 9.1 está terminada.

Como consecuencia inmediata, mirando $HH^1(A^G)$ se reencuentra que $\mathrm{Der}_k(A^G)=\mathrm{Der}_k(A)^G$. Además (con el $HH_1$) $\Omega^1_k(A^G)=\Omega^1_k(A)_G$.

Para las extensiones de anillos íntegros en general (i.e. no necesariamente Galois) se tiene el resultado siguiente:

**Corolario 9.3.** *Sea $A$ un anillo conmutativo íntegro, $G$ un subgrupo finito de automorfismos de $A$. Entonces la flecha*

$$HH_n(A^G)\to HH_n(A)^G$$

*tiene por núcleo y conúcleo $A^G$-módulos de $f$-torsión, para todo $f\in A^G$ tal que $A[f^{-1}]$ sea un extensión Galois de $A^G[f^{-1}]$.*

Observamos que $f$'s no triviales existen gracias a la Proposición 3.8.
*Demostración:* Se utiliza el teorema anterior para $A[f^{-1}]$, y el hecho de que que la localización es un funtor exacto, y que conmuta con la homología de Hochschild.

La generalización siguiente a las álgebras quasi-conmutativas permitira verificar, para las extensiones de Galois conmutativas suaves, fórmulas análogas para la homología de De Rham:

**Teorema 9.4.** *Sea $C$ una $k$-álgebra filtrada con $\mathbb{Q}\subseteq k$, se supone la filtración positiva y exhaustiva, y $G$ un subgrupo finito de automorfismos ($k$-lineales) que preservan la filtración. Si $\mathrm{gr}(C)$ es conmutativo y $\mathrm{gr}(C)$ es una extensión Galois de $\mathrm{gr}(C)^G$, entonces $HH_*(C^G)=HH_*(C)_G$.*

*Demostración:* Como el anillo $\mathrm{gr}(C)$ es un anillo graduado y los morfismos evidentes $\mathrm{gr}(C) \to C_0$, y $C_0 \to gr(C)$ son $G$-equivariantes, se sigue que $\mathrm{gr}(C)$ es una extensión Galois de $\mathrm{gr}(C)^G$ si y solamente si $C_0$ es una extensión Galois de $C_0^G$, y eso implica que $C$ es una extensión Galois de $C^G$.

Por invariancia Morita, $HH_*(C^G) = HH_*(C * G)$ y

$$HH_*(C * G) = \oplus_{<g>\in<G>} H_*(C, C.g)_{\mathcal{Z}_g}$$

Para calcular $H_*(C, C.g)$ se considera la sucesión espectral que proviene de la filtración de $C$. Se llama $B := \mathrm{gr}(C)$, y por el teorema anterior $H_*(B, B.g) = 0$ para todo grado (si $g \neq 1$). Pero esos grupos de homología constituyen el primer término de la sucesión espectral asociada a la filtración de $C$, por lo tanto $H_*(C, C.g) = 0$ y la demostración del teorema está terminada.

**Corolario 9.5.** *Sea $A$ un $k$-álgebra commutativa suave íntegra que contiene $\mathbb{Q}$ y $G$ un subgrupo finito de automorfismos de $A$. Se supone que $A$ es una extensión Galois de $A^G$, entonces $H^*_{dR}(A^G) = H^*_{dR}(A)_G$.*

*Demostración:* Como $A$ es suave, la condición de Galois nos dice que $A^G$ es suave también. Por el teorema Wodzicki-Brylinski (Ver [Wo] o [Br]) $H^*_{dR}(A^G) = HH_{2d-*}(\mathrm{Diff}(A^G))$. Pero bajo esas hipótesis, $\mathrm{Diff}(A^G) = \mathrm{Diff}(A)^G$, y como $A$ es suave $\mathrm{Diff}(A)^G$ es siempre equivalente Morita a $\mathrm{Diff}(A) * G$, por lo tanto $HH_{2d-*}(\mathrm{Diff}(A^G)) = HH_{2d-*}(\mathrm{Diff}(A)^G) = HH_{2d-*}(\mathrm{Diff}(A) * G)$. Se puede por lo tanto utilizar el teorema anterior para $C = \mathrm{Diff}(A)$; en este caso, $\mathrm{gr}(\mathrm{Diff}(A))_0 = A$ es una extensión Galois de $A^G$, entonces $HH_{2d-*}(\mathrm{Diff}(A) * G) = HH_{2d-*}(\mathrm{Diff}(A))_G$. Se utiliza otra vez el resultado de Wodzicki-Brylinski en el sentido inverso y se obtiene $HH_{2d-*}(\mathrm{Diff}(A))_G = H^*_{dR}(A)_G$.

# 10. Algebras simplécticas y de Poisson

Consideramos ahora el caso siguiente: $C$ una $k$-álgebra no conmutativa filtrada, tal que $\mathrm{gr}(C)$ es conmutativa, y $G$ un subgrupo de automorfismos de $A$ que respeta la filtración (y por lo tanto induce una acción en $\mathrm{gr}(C)$).

El caso $\mathrm{gr}(C)$ una extensión Galois de $\mathrm{gr}(C)^G$ lo hemos visto antes, y es equivalente al hecho de que $C_0$ sea una extensión Galois de $C_0^G$. Pero qué se puede decir cuando $C$ es una extensión Galois de $C$ pero no valga lo mismo necesariamente para $\mathrm{gr}(C)$?

El ejemplo fundamental es el siguiente: sea $A$ una $k$-álgebra suave y $C := \mathrm{Diff}(A)$. Entonces *siempre* $C$ es una extensión Galois de $C^G$, sin embargo $\mathrm{gr}(C)$ es una extensión Galois de $\mathrm{gr}(C)^G$ si y sólo si $A$ es extensión Galois de $A^G$.

En el contexto planteado en esta sección, si $C$ es filtrada y $S := \mathrm{gr}(C)$ es conmutativa, entonces es sabido que $S$ admite una estructura de Poisson, que es la que proviene de los conmutadores de $C$. En el caso $C = \mathrm{Diff}(A)$ con $A$ regular, $\mathrm{gr}(C) = S_A(\mathrm{Der}(A))$, es el anillo de funciones regulares del fibrado cotangente al espacio afín definido por $A$, que es, de hecho, un álgebra simpléctica.

Recordamos brevemente la definición de esta estructura:

**Definición 10.1.** *Un álgebra conmutativa $S$ junto con una aplicación $\{-,-\} : S \times S \to S$ se dice un álgebra de* **Poisson** *si $(S, \{,-,-\})$ es un álgebra de Lie, y $\{-,-\}$ es una biderivación con respecto a la multiplicación de $S$.*

En el caso de las álgebras de Poisson, se tiene definida una flecha

$$\begin{aligned} \mathrm{Ham} : \Omega_1(S) &\to \mathrm{Der}(S) \\ adb &\mapsto a\{b,-\} \end{aligned}$$

**Definición 10.2.** *Un álgebra de Poisson $S$ se dice* **simpléctica** *si y sólo si* Ham *es un isomorfismo.*

**Ejemplos:** 1. Sea $A = k[x_1, \ldots, x_n]$, entonces $\mathrm{Diff}(A) = A_n(k)$ la n-ésima álgebra de Weyl, y $S := \mathrm{gr}(\mathrm{Diff}(A)) = k[x_1, \ldots, x_n, y_1, \ldots, y_n]$, la estructura de Poisson en $S$ está determinada por $\{x_i, x_j\} = 0 = \{y_i, y_j\}$ y $\{x_i, y_j\} = \delta_{ij}$. Es un álgebra simpléctica.

2. Sea $G$ un subgrupo finito de $\mathrm{Sp}(2n, k)$, que actúa en $S$ por automorfismos lineales. Como $G \subset \mathrm{Sp}(2n, k)$, $\{gp, gq\} = g(\{p, q\})$ para todo $g \in G$, $p, q \in S$, por lo tanto $S^G$ con $\{-,-\}|_{S^G}$ es un álgebra de Poisson, que en general no será nunca simplectica (a menos que $G = 1$).

**Observación:** De hecho, como $G \subset \mathrm{Sp}(2,k)$, $S^G$ será un anillo con singularidades, y $S = k[x_1, \ldots, x_n, y_1, \ldots, y_n]$ es obviamente suave, por lo tanto la extensión $\mathrm{gr}(C)|\mathrm{gr}(C)^G$ no es Galois. Sobre regularidad de álgebras de Poisson podemos citar el siguiente resultado de Farkas:

**Teorema 10.3.** *Sea $S$ una $k$-álgebra conmutativa noetheriana íntegra, $\mathrm{ch}(k) = 0$, y supongamos que $S$ es Poisson simple. Entonces $S$ es regular.*

Recordamos que un **ideal de Poisson** $I$ es por definición un ideal del álgebra asociativa $S$ tal que a su vez $\{I, S\} \subseteq I$. Un álgebra de Poisson se dice **Poisson simple** si no tiene ideales de Poisson propios.

La demostración del teorema de Farkas se basa en un criterio de proyectividad de ciertos módulos "de Poisson", y de esa manera se llega a demostrar que $\Omega^1_k(S)$ es proyectivo, y en carcterística cero eso es equivalente a la regularidad. Recordemos que en el caso simplectico y suave, los ideales de Poisson coinciden con los $\mathrm{Diff}(S)$-submódulos de $S$, y $S$ es un $\mathrm{Diff}(S)$-módulo simple.

Con vistas en el teorema anterior, veremos que la noción de ser simpléctica, o Poisson simple, es estable por extensiones de Galois.

De aquí al final, $S$ será una $k$-álgebra de Poisson con corchete $\{-,-\}$, $G$ un subgrupo de automorfismos del álgebra de Poisson de $A$, es decir para todo $g \in G$, $g$ es morfismo de $k$-álgebras y $\{g(a), g(b)\} = g(\{a,b\})$ para todo $a,\ b\ \in S$.

**Proposición 10.4.** *Sea $S$ un álgebra simpléctica y $(S,G)$ Galois. Entonces $S^G$ es simpléctica.*

*Demostración:* Se tiene el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \Omega^1(S^G) & \xrightarrow{\mathrm{Ham}} & \mathrm{Der}(S^G) \\ \downarrow & & \uparrow \\ \Omega^1(S)^G & \xrightarrow{\mathrm{Ham}} & \mathrm{Der}(S)^G \end{array}$$

Como $S$ es simpléctica, $\mathrm{Ham} : \Omega^1(S) \cong \mathrm{Der}(S)$, por lo tanto también se tiene un isomorfismo inducido $\Omega^1(S)^G \cong \mathrm{Der}(S)^G$, finalmente la condición Galois asegura que las flechas verticales del diagrama son isomorfismos.

Con respecto a la Poisson simplicidad se tiene también el resultado análogo:

**Proposición 10.5.** *Sea $S$ un álgebra de Poisson simple y $(S,G)$ Galois. Entonces $S^G$ es Poisson simple.*

La demostración se basa en el siguiente lema:

**Lema 10.6.** *Sea $S$ un álgebra de Poisson, $(S,G)$ Galois, entonces para cada $a \in S$, existen $a_i \in S$ y $b_i \in S^G$ tales que $\{a,-\} = \sum_i a_i\{b_i,-\}$.*

*Demostración:* Consideramos la aplicacion hamiltoniana $\Omega^1(S) \to \mathrm{Der}(S)$ definida por $fdg \mapsto f\{g,-\}$. Uno sabe que la multiplicación induce un isomorfismo $\Omega^1(S) = S \otimes_{S^G} \Omega^1(S^G)$. Considerando $da \in \Omega^1(A)$, bajo el isomorfismo anterior uno sabe que $da = \sum_i a_i db_i$ con los $b_i \in A^G$, Entonces la derivacion $\{a,-\}$ coincide con la derivacion $\sum_i a_i\{b_i,-\}$.

Como consecuencia, se tiene una caracterización similar para corchetes sucesivos:

**Corolario 10.7.** *Sea $(S,G)$ Galois, $S$ un álgebra de Poisson, $a_1, \ldots, a_n \in S$, entonces el operador diferencial $\{a_1, \{a_2, \{\ldots, \{a_n, -\}\ldots\}$ se puede escribir como combinacion lineal con coeficientes en $S$ de operadores diferenciales de la forma $\{b_1, \{b_2, \{\ldots, \{b_k, -\}\ldots\}$ con $b_i \in S^G$ y $k \leq n$.*

**Ejemplo:** Sea $n = 2$, consideremos $\{a, \{a', -\}\}$ con $a$ y $a'$ en $S$. Por el lema anterior $\{a', -\} = \sum_i a'_i\{b'_i, -\}$ con $b'_i \in A^G$, entonces

$$\{a, \{a', -\}\} = \sum_i \{a, a'_i\{b'_i, -\}\} = \sum_i \{a, a'_i\}\{b'_i, -\} + \sum_i a'_i\{a, \{b'_i, -\}\}$$

En la primer sumatoria aparecen términos como uno buscaba, para el segundo termino se vuelve a usar el lema anterior pero para $a$, escribimos $\{a,-\} = \sum_j a_j\{b_j,-\}$ con los $b_j \in A^G$, entonces

$$\sum_i a'_i\{a,\{b'_i,-\}\} = \sum_{i,j} a_j a'_i\{b_j,\{b'_i,-\}\}$$

La demostracion en general es por induccion en $n$, llendo "de adentro hacia afuera" como se hizo en el ejemplo de recién.

Ahora podemos demostrar la proposición. Sea entonces $S$ Poisson simple, $(S,G)$ Galois, queremos ver que $S^G$ es poisson simple.

Consideramos $x \in S^G$ no nulo, en particular $x \in A$, y el mínimo ideal de Poisson de $S$ que contiene a $x$ coincide con $S$, por lo tanto podemos escribir

$$1 = ax + a'\{b'x\} + \cdots + \sum_{i_1,\ldots,i_n} a_{i_1..i_n}\{b_{i_1},\{b_{i_2},\{\ldots,\{b_{i_k},x\}\ldots\}$$

Por el lema anterior podemos suponer que todos los $b_i$ estan en $A^G$. Llamando $p : S \to S^G$ al morfismo promedio, i.e. $p = \frac{1}{|G|}\sum_{g\in G} g$, como $p$ es $A^G$-lineal y $p(1) = 1$, aplicando $p$ a la formula anterior, y usando que $x \in A^G$ y los $b_i \in A^G$ tenemos:

$$1 = p(a)x + p(a')\{b'x\} + \cdots + \sum_{i_1,\ldots,i_n} p(a_{i_1..i_n})\{b_{i_1},\{b_{i_2},\{\ldots,\{b_{i_k},x\}\ldots\}$$

Esto dice que el ideal Poisson de $A^G$ generado por $x$ contiene al uno, luego $A^G$ es Poisson simple.

Notar que si no se está en característica cero pero sí se está en situación Galois, en vez de escribir al uno como combinación lineal de corchetes sucesivos de $x$, escribimos a un elemento $a$ de traza uno como una combinación de ese estilo, después en vez de promediar, calculamos la traza.

**Corolario 10.8.** *Sea $S$ Poisson simple, y $G$ un grupo finito de automorfismos de Poisson, sin ser necesariamente Galois, entonces todo ideal de Poisson propio de $S^G$ tiene soporte incluido en $\cup_{g\in<G>}\mathcal{V}(I_g)$, donde $I_g = S^G \cap \langle x - g(x) \ : \ x \in S\rangle$.*

*Demostración:* Sabemos que $(S_T, G)$ es Galois para todo subconjunto multiplicativo $T$ tal que $\langle x - g(x) \ : \ x \in S\rangle_T = S$.

Si a $T$ se lo supone contenido en $S^G$ (tomandole normas a sus elementos por ej.) entonces $(S_T)^G = (S^G)_T$, y como $(S_T, G)$ es Galois uno sabe que $S_T^G$ es poisson simple.

Sobre los ideales $I_g$ observamos que "ven" la estructura Poisson, en el sentido de que dan -en el caso de que $S^G$ sea Poisson simple- esencialmente los únicos ideales de Poisson, o mejor dicho, todo otro ideal Poisson de $S^G$ define una subvariedad que esta necesariamente incluida en la union de los $\mathcal{V}(I_g)$. En realidad nos falta chequear que efectivamente los $I_g$ son ideales de Poisson, esto es lo que haremos a continuación:

Sea $S$ un álgebra de Poisson, $g$ un automorfismo de Poisson, $I(g) := \langle x - g(x) : \ \ x \in S\rangle$. Si la acción de $\langle g\rangle$ es Galois y $g \neq Id$, entonces $I(g) = S$. Recíprocamente, $(S,G)$ es Galois si y sólo si $I(g) = S$ para todo $g \neq Id$. Afirmamos que $I_g := I(g) \cap S^G \subset S^G$ es un ideal de Poisson.

Para esto calculamos $\{a.(x - g(x)), b\} = \{a, b\}.(x - g(x) + a.\{(x - g(x), b\} = \{a, b\}.(x - g(x) + a.(\{x, b\} - \{g(x), b\}$. Si asumimos $b \in S^G$, tenemos que $\{x, b\} - \{g(x), b\} = \{x, b\} - g(\{x, b\})$ y por lo tanto hemos demostrado que $\{I(g), S^G\} \subseteq I(g)$.

Pero si ahora tomamos un elemento de $I_g = I(g) \cap S^G$, por un lado sabemos que que $\{I(g), S^G\} \subseteq I(g)$, pero también es claro que $\{S^G, S^G\} \subseteq S^G$, por lo tanto $\{I_g, S^G\} \subseteq I_g$.

# Referencias


[A-F] F. Anderson - K.Fuller: Rings and categories of modules. 2. ed. Graduate Texts in Mathematics. 13. New York: Springer-Verlag.

[A-R-S] M. Auslander, I. Reiten, S. Smalo: Galois actions on rings and finite Galois coverings. Math. Scand. 65, No.1, 5-32 (1989).

[Br] J.L.Brylinski: A differential complex for Poisson manifolds. J. Differ. Geom. 28, No.1, 93-114 (1988).

[C-H-R] S. Chase, D. Harrison, A. Rosenberg: Galois theory and Galois cohomology of commutative rings. Mem. Am. Math. Soc. 52, 15-33 (1965).

[C-F-M] M.Cohen, D.Fischman, S. Montgomery: Hopf Galois extensions, smash products, and Morita equivalence. J. Algebra 133, No.2, 351-372 (1990).

Ver también: M.Cohen: A Morita context related to finite automorphism groups of rings. Pac. J. Math. 98, 37-54 (1982).

[C-Q] J.Cuntz, D. Quillen: Cyclic homology and nonsingularity. J. Am. Math. Soc. 8, No.2, 373-442 (1995).

[D-I] F. Demeyer, E. Ingraham: Separable algebras over commutative rings Berlin - Heidelberg - New York: Springer-Verlag, 157 (1971).

[Fe] M. Ferraro: On the Galois theory of non-commutative rings. Osaka J. Math. 7, 81-88 (1970).

[G-W] S. Geller, C. Weibel: Étale descent for Hochschild and cyclic homology. Comment. Math. Helv. 66, No.3, 368-388 (1991).

[K-T] H. Kreimer, M. Takeuchi: Hopf algebras and Galois extensions of an algebra. Indiana Univ. Math. J. 30, 675-692 (1981).

[Le] T. Levasseur: Anneaux d'opérateurs différentiels. L.N.Math. Springer 867 (1981), 157-173.

[Lo] M. Lorenz: On Galois descent for Hochschild and cyclic homology. Comment. Math. Helv. 69 (1994), no. 3, 474-482 (1994).

[Mo] S. Montgomery: Fixed rings of finite automorphism groups of associative rings. Lecture Notes in Mathematics, 818. Berlin - Heidelberg - New York: Springer-Verlag.

[Wo] M. Wodzicki: Cyclic homology of differential operators. Duke Math. J. 54, 641-647 (1987).