Tesis Doctoral

Clases características para módulos cuadráticos

Cortiñas, Guillermo Horacio

1988

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

UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE CIENCIAS EXACTAS Y NATURALES

TITULO

CLASES CARACTERISTICAS PARA MODULOS CUADRATICOS

Autor: GUILLERMO HORACIO CORTIÑAS

Director: ORLANDO E. VILLAMAYOR

Lugar de Trabajo: DEPARTAMENTO DE MATEMATICA, F.C.E.y N.

TESIS PRESENTADA PARA OPTAR POR EL TITULO DE

DOCTOR EN CIENCIAS MATEMATICAS

- NOVIEMBRE -

1988

INTRODUCCION

En la teoría clásica de formas cuadráticas sobre un cuerpo K con $Car(K) \neq 2$ se asocian a cada módulo cuadrático (V,q) tres invariantes, a saber: su paridad, i.e. $\overline{\dim V} \in \mathbb{Z}/2\mathbb{Z}$; y si $\overline{\dim V} = 0$, su discriminante $\Delta(q) \in K^*/K^{*2}$ y su álgebra de Clifford $\overline{C(p,q)} \in Br_2(K)$. Estos invariantes no son suficientes para clasificar las formas cuadráticas, es decir, pueden existir (V,q) y (W,q_2) no isomorfas y que tengan los mismos invariantes (e.g. $K = R, q_1 = \langle 1,1,1,1 \rangle$ $q_2 = \langle -1,-1,-1,-1 \rangle$. En 1962, A. Delzant utiliza la idea de las clases de Stiefel-Whitney -proveniente de la topología- para definir nuevos invariantes

$$SW_i(V,q) \in H^n(G,\mathbb{Z}/2\mathbb{Z}) \qquad n \geq 1$$

donde G es el grupo de Galois de la clausura separable de K ([De]). (La búsqueda de invariantes en los $H^n(G, \mathbb{Z}/2\mathbb{Z})$ es natural en virtud de los isomorfismos $H^1(G,\mathbb{Z}/2\mathbb{Z}) \cong K^*/K^{*2}$ y $H^2(G,\mathbb{Z}/2\mathbb{Z}) \cong Br_2(K)$. W. Scharlau estudió la efectividad de tales clases características en 1969 [Sch]. En 1970 J. Milnor se interesó en el tema dentro del marco de la teoría K, obteniendo un diagrama conmutativo

$$\begin{array}{ccc} L(K) & \xrightarrow{SW'} & k_{**}(K) \\ & {\scriptstyle SW} \searrow \quad \swarrow {\scriptstyle \gamma} & \\ & H^{**}(G,\mathbb{Z}/2\mathbb{Z}) & \end{array}$$

donde: $H^{**}(G,\mathbb{Z}/2\mathbb{Z})$ es el grupo de unidades del anillo de cohomología de G con coeficientes en $\mathbb{Z}/2\mathbb{Z}$

- $SW(V,q) = 1 + \sum_{n \geq 1} SW(V,q)$

- $k_{**}(K)$: es el grupo de unidades del anillo $\prod_{n \geq 1} k_n(K)$ y (k_n indica Teoría K de Milnor.

- L(K): es el grupo de Witt-Grothendieck de K .

A partir de este trabajo se han iniciado diversas líneas de investigación. En primer lugar, ¿qué se puede decir si se reemplaza el grupo de Witt-Grothendieck por el grupo de Witt? Es evidente que no se puede copiar la misma construcción, la idea consiste en definir invariantes con la ayuda de la filtración clásica $W(K) > I > I^2 > \ldots$ Se trata de definir invariantes

$$w_n : I^n/I^{n+1} \rightarrow H^n(G,\mathbb{Z}/2\mathbb{Z}) \quad \text{ó} \quad k_n(G) .$$

El teorema de Mercuriev afirma que w_2 está bien definida y es un isomorfismo. De w_3 se tienen algunos resultados y no se sabe casi nada de w_4 .

Otra línea de trabajo, con el grupo de Witt, es el caso char K=2. K. Kato [K] ha estudiado el problema para formas bilineales simétricas, pero en el caso de formas cuadráticas sólo se tienen resultados parciales ([Ara]).

Hay finalmente otro tipo de problemas que es la que nos interesa aquí; la pregunta es qué pasa si se cambia K por un anillo R cualquiera. E. Hornix [H] definió clases de Stiefel-Whitney con valores en los k_n de Milnor de R cuando R es un anillo local, en 1973. En 1979, Micali y Revoy [M-R] extendieron la teoría de Hornix al caso en que R es semilocal.

El objetivo de este trabajo es definir clases de Stiefel-Whitney para módulos cuadráticos sobre anillos R con $2 \in UR$ pero con espectro más complicado que el de los anillos locales y semilocales. En todos los trabajos que hemos mencionado, el caso $2 \in UR$ es relativamente sencillo. Ello se debe a que, si R es semilocal, se tiene una sucesión exacta

$$0 \rightarrow I \rightarrow \mathbb{Z}[UR/U^2R] \longrightarrow L(R) \longrightarrow 0 .$$

donde $I = <\{\bar{a} + \bar{b} - (\bar{c} + \bar{d}) : <a,b>_R \cong <c,d>_R\}>$. El caso de anillos más generales se complica notoriamente al no tener una tal sucesión exacta. En otras palabras, no todo módulo cuadrático de rango constante, (P,q) admite una descomposición ortogonal

de rango 1, más aún, en caso de existir, dos de tales descomposiciones no necesariamente son contiguas.

Se plantea entonces el problema de encontrar una R-álgebra S tal que $(p,q) \otimes S$ admita una tal descomposición ortogonal, sin que se pierda demasiada información al pasar de R a S (lo que sucedería si localizáramos). Una condición natural es pedir S/R fielmente playa. Si miramos el problema desde el punto de vista de esquemas, el trabajo de Grothendieck [G] , sugiere tratar de imitar la construcción del fibrado bandera, en el caso cuadrático. Este es el problema de tesis que me planteó el profesor O.E. Villamayor.

Otro punto de vista posible es tratar de explotar el buen comportamiento local de las fomas cuadráticas; i.e. estudiar el prehaz definido por el funtor L sobre X=Spec R. En términos de extensiones, la tarea consiste en definir un álgebra $A = A(R)$ que tenga todas las propiedades de las localizaciones, pero que sea fielmente playa sobre R, pero atención, no es útil tomar $A = \prod_{p \in \mathrm{Spec}R} R_p$, como se ve en seguida* Este punto de vista me fue sugerido por C. Weibel (U. Rutgers) y B. Khan (U. París VII).

Este trabajo se divide de dos partes. En la primera parte se da una revisión de los resultados de formas cuadráticas y cohomología que serán usados luego. La segunda parte comienza por un § 0 en el cual se fijan las notaciones a utilizar. El §1 está dedicado a la construcción y propiedades del álgebra A(teo. 1.3.). En §2 se da una primera definición de las clases características con valores en $\overset{v}{H}^n(\chi, A, \mu_2)$ $(n \geq 0)$, cuando SpecR es localmente conexo (2.4.). En el §3 se define el fibrado bandera cuadrático. Gracias a esta construcción, y a los resultados de §2. se obtienen clases características con valores en $H^\circ(X, \overset{v}{H}^n(\chi, R, \mu_2))$ $(X = \mathrm{Spec}R)$. En el apéndice se estudia el caso en que R es ordenado, obteniéndose un resultado (A) que da la pauta de que se pueden utilizar las construcciones de este trabajo en la teoría de signaturas.

Deseo agradecer particularmente a O.E. Villamayor -quien me planteó el problema de tesis- por la confianza y el apoyo que siempre me otorgó. Agradezco también a las nu-

* Ver T.Y. Lam. Serre's Conjecture. LNM 635, pp14

merosas personas que han tenido la paciencia de dejar que les contara los problemas de mi tesis, en especial a C. Weibel, B. Khan, L. Caniglia, G. Martínez y M.E. D'Alfonso. No olvido tampoco a todos aquellos amigos sin cuyo apoyo no me habría sido posible llegar hasta aquí.

Agradezco finalmente al Señor Carlos Medrano, por la excelente impresión.

Guillermo H. Cortiñas
Buenos Aires, 25/10/88

PRELIMINARES

1. Formas cuadráticas

Consideramos fijo, a lo largo de todo este trabajo, un anillo de base R, que suponemos conmutativo y con unidad. Todo módulo sobre R se entenderá unitario. Los productos tensoriales se entenderán sobre R, salvo expresa mención.

Dado un R-módulo M, una *forma cuadrática* sobre M es una aplicación

$$q : M \to R$$

que verifica

$q_1)$ $q(\lambda x) = \lambda^2 q(x)$ $(\forall x \in M, \lambda \in R)$

$q_2)$ La aplicación $\Phi_q : M \times M \to R$

$$\Phi_q(x,y) = q(x+y) - q(x) - q(y) \qquad x,y \in M$$

es bilineal.

Si además se verifica

$q_3)$ El morfismo

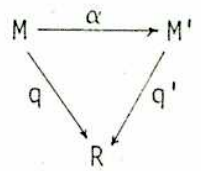
$$\varphi_q : M \to M^*$$
$$\varphi_q(X)(Y) = \Phi_q(x,y), \quad (x,y \in M)$$

es un isomorfismo

diremos que q es *regular*.

Sólo consideraremos el caso en que M es proyectivo y q es regular. Así, un *módulo cuadrático* sobre R será un par (M,q) donde M es un R-módulo proyectivo finitamente generado y $q : M \to R$ es una forma cuadrática regular.

Un *morfismo ortogonal* entre dos módulos cuadráticos (M,q) y (M',q') es un isomorfismo $\alpha : M \to M'$ que hace commutativo al diagrama



El *rango* de un módulo cuadrático (M,q) es el rango del módulo subyacente M. Denotamos el rango de (M,q) por $rk(M,q)$.

La *suma ortogonal* de dos módulos cuadráticos (M,q) y (M',q') es el módulo cuadrático cuyo módulo subyacente es $M \oplus M'$ provisto de la forma cuadrática regular dada por la aplicación:

$$q \perp q' : M \oplus M' \to R$$

$$(q \perp q')(x + x') = q(x) + q'(x')$$

Denotamos por $(M,q) \perp (M',q')$ a la suma ortogonal de (M,q) y (M',q').

Si *2 es inversible* en R el *producto tensorial* de (M,q) y (M',q') es el módulo cuadrático cuyo módulo subyacente es $M \otimes M'$ y cuya forma cuadrática $q \otimes q'$ viene dada por la fórmula

$$(q \otimes q')(x) = \frac{1}{2} \varphi''(x)(x)$$

donde

$$\varphi'' = \varphi_q \otimes \varphi_{q'} : M \otimes M' \to R .$$

Sea $\underline{Q}'R$ (respectivamente $\underline{Q}R$) la categoría cuyos objetos son los módulos cuadráticos sobre R (resp. módulos cuadráticos de rango constante) y cuyos morfismos son los morfismos ortogonales.

Entonces $(\underline{\underline{Q'R}},\perp)$(resp. $(\underline{\underline{QR}},\perp)$ es un grupoide con producto en el sentido de Bass [Ba] ; llamamos *grupo de Witt-Grothendieck* de R (respectivamente *grupo de Witt-Grothendieck de rango constante*) al grupo $K_0(\underline{\underline{Q'R}},\perp)$ (resp. $K_0(\underline{\underline{QR}},\perp)$) que denotamos por $L(R)$ (resp. $L_{cte}(R)$).

Si además 2 es inversible en R, el producto tensorial dota a los grupos $L(R)$ y $L_{cte}(R)$ de una estructura de anillo conmutativo.

Si $P \in \text{Spec } R$ y $(P,q) \in \underline{Q}'R$ podemos definir una forma cuadrática q_P sobre $P_P = P \otimes R_P$, por la fórmula

$$q\left(\frac{p}{t}\right) = \frac{1}{t^2}\, q(p) \qquad (t \notin P)$$

Observemos que q_P está bien definida. En efecto, si $p/t = p'/t' \Rightarrow$ $\exists s \notin P$ con $st'p = stp'$. Aplicando q se tiene

$$s^2t'^2\, q(p) = s^2t^2q(p') \Rightarrow \quad q_p(p/t) = q_p(p'/t')$$

Es claro que además q_P es regular; (P_p,q_P) se llama la *localización en P* de (P,q). Análogamente podemos definir la localización de (P,q) en cualquier abierto afín. De esta forma, podemos pensar a (P,q) como un haz coherente localmente trivial provisto localmente de formas cuadráticas que se pegan bien. Como veremos a continuación las formas cuadráticas sobre anillos locales tienen una estructura más sencilla que sobre anillos en general. De manera que la filosofía más adecuada va a ser ver a (P,q) como haz coherente.

1.1. **Definición.** Sea R un anillo, (P,q) un R-módulo cuadrático. Si $v,w \in P$, diremos que v y w son *ortogonales*, $v \perp w$ si $\Phi(v,w) = 0$. Una base B de P se dice *ortogonal* si $B = \{v_1,\ldots,v_n\}$ es tal que $v_i \perp v_j$ $(\forall i \neq j)$. Una base $B = \{v_{11},v_{12},v_{21},v_{22},\ldots,v_{r1},v_{r2}\}$ se dice

simpléctica si

$$v_{ji} \perp v_{\ell i}, \ (\forall j \neq \ell) \quad y \quad \Phi(v_{j1}, v_{j2}) = 1 \ (\forall j).$$

1.2. **Proposición.** [M-V-1]. Si (R,M) es un anillo local y (P,q) es un módulo cuadrático sobre R, se verifican

i) Si $2 \notin M$ (P,q) tiene una base ortogonal

ii) Si $2 \in M$ (P,q) tiene una base simpléctica.

1.3. **Corolario.** Si R es una anillo no necesariamente local, y 2 no es inversible en R, se verifica

$$\text{Si } (P,q) \in \underline{\underline{Q}}(R) \Rightarrow rk(P,q) \text{ es par.}$$

1.4. **Definición.** Dos bases ortogonales B,B' de un módulo cuadrático (P,q) se dicen *contiguas* si existe una sucesión finita de bases ortogonales

$$B = B_0, B_1, \ldots, B_{k-1}, B_k = B'$$

tales que B_{i+1} difiere de B_i en a lo sumo dos elementos $(0 \leq i \leq k-1)$. Dada una base simpléctica $B = \{v_{11}, v_{12}, v_{21}, v_{22}, \ldots, v_{r1}, v_{r2}\}$ formemos $\bar{B} = \{(v_{11}, v_{12}), (v_{21}, v_{22}), \ldots, (v_{r1}, v_{r2})\}$. Si B' es otra base simpléctica, decimos que B y B' son *contiguas* si existe una sucesión finita de bases simplécticas

$$B = B_0, \ldots, B_k = B'$$

donde $\bar{B}_{i+1}$ difiere de $\bar{B}_i$ en a lo sumo dos elementos $(0 \leq i \leq k-1)$.

1.5. **Proposición** [M-R]. Sea (R,M) un anillo local, (P,q) ι R-módulo cuadrático. Se verifican

i) Si $2 \notin M$, dos bases ortogonales de (P,q) son contiguas

ii) Si $2 \in M$, dos bases simplécticas de (P,q) son contiguas.

Dado un anillo R, consideremos los siguientes conjuntos

$\alpha(R)$ = {clases de isomorfismo de módulos cuadráticos de rango 1}

$E(R)$ = {clases de isomorfismo de módulos cuadráticos de rango 2}

De las proposiciones anteriores se deduce inmediatamente el

1.6. **Teorema**. Sea (R,M) un anillo local, si $2 \notin M$ (resp. $2 \in M$), sea F el grupo abeliano libre generado por $\alpha(R)$ (resp. $E(R)$) se tiene la sucesión exacta de grupos abelianos

$$0 \to I \to F \to L(R) \to 0$$

Donde I está generado por el conjunto

$$\{\beta_1 + \beta_2 - (\beta_1' + \beta_2') : \beta_i \in \alpha(R) \quad y \quad \beta_1 \perp \beta_2 \cong \beta_1' \perp \beta_2'\}$$

(respectivamente

$$\{E_1 + E_2 - (E_1' + E_2') : E_i \in E(R) \quad y \quad E_1 \perp E_2 \cong E_1' \perp E_2'\}). \blacksquare$$

Como veremos más adelante, este resultado permite definir clases características para módulos cuadráticos sobre anillos locales, con $2 \notin M$, en forma inmediata. Se obtiene así una generalización de la teoría de clases características dada por Delzant [D] para el caso de cuerpos.

Los invariantes clásicos.

A lo largo de esta sección, consideraremos un anillo R, fijo, no necesaria-

mente local:

Observemos en primer lugar que el conjunto $\alpha(R)$ definido en la sección anterior, provisto con la operación "$\otimes$" resulta un grupo abeliano. Si ahora (P,q) es un módulo cuadrático de rango constante n,y $\varphi_q : P \to P^*$ es el isomorfismo natural, se tiene que $\det \varphi_q : \Lambda^n P \xrightarrow{\Lambda^n \varphi_q} (\Lambda^n P)^*$ define unívocamente una forma cuadrática $\Lambda^n q$ sobre $\Lambda^n P$. El par $(\Lambda^n P, \Lambda^n q)$ se llama el *determinante* de (P,q) y se denota $\det(P,q)$. Las propiedades de la potencia exterior Λ^n nos permiten demostrar la

1.7. **Proposición.** Supongamos que 2 es inversible en R. Se tiene un (único) morfismo de grupos

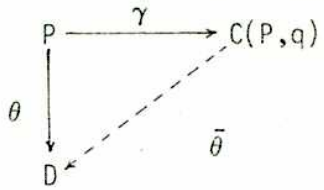
$$\gamma : L_{cte}(R) \to \alpha(R)$$

tal que $\gamma(P,q) = \det(P,q)$ $\forall (P,q) \in \underline{\underline{Q}}(R)$. γ se llamará la *aplicación determinante* de $L_{cte}(R)$ en $\alpha(R)$. Por abuso de notación escribiremos "det" en lugar de γ, de ahora en adelante. ∎

1.8. **Definición-Proposición.** Sea (P,q) un R-módulo cuadrático; el *álgebra de Clifford* de (P,q) es una R-álgebra $C(P,q)$ junto con un morfismo de R-módulos

$$\gamma : (P,q) \to C(P,q)$$
$$(\gamma(p))^2 = q(p) \quad (\forall p \in P).$$

tal que si (D,θ) es un objeto de la misma especie, existe un único morfismo de álgebras $\bar{\theta}$, que hace conmutar el diagrama:



Observemos que una tal álgebra siempre existe. En efecto, si $T(P)$ es el álgebra tensorial asociada a P, basta tomar $C(P,q) = T(P)/I$, donde I es el ideal bilátero generado por los elementos de la forma $\{x \otimes x - q(x): x \in P\}$.

1.9. **Observación.** De la construcción explícita que acabamos de dar para $C(P,q)$ se deduce que ésta es un álgebra $\mathbb{Z}/2\mathbb{Z}$-graduada.
Tenemos así que $C = C(P,q)$ se descompone de la forma

$$C = C_0 \oplus C_1$$

y se verifican

$$C_0 \cdot C_0 \subset C_0$$
$$C_0 \cdot C_1 \wedge C_1 \, C_0 \subset C_1$$
$$C_1 \, C_1 \subset C_0$$
$$\gamma(P) \subset C_1 \, .$$

Notación. Dada una R-álgebra C denotamos su centro por ZC.

1.10. **Proposición** [M-V-1]. Sean (P,q) un R-módulo cuadrático de rango constante $n = rk(P,q)$; y $C(P,q)$ su álgebra de Clifford. Se verifican

i) Si n es par $ZC = R$

ii) Si n es impar $ZC_0 = R$.

1.11. **Definición.** Sea A una R-álgebra, y considérese la sucesión exacta:

$$0 \to I(A|R) \to A^e \xrightarrow{\mu} A \to 0 \qquad (1.12)$$

donde:

$A^e = A \otimes_R A^{op}$ es el *álgebra envolvente* de A.

$\mu(a \otimes b) = a.b$ es la multiplicación de A.

$I(A|R) = \operatorname{Ker} \mu$.

Podemos entonces considerar (1.12) como sucesión de A^e-módulos. Diremos que A *es separable* si la sucesión de A^e-módulos (1.12) se escinde, o equivalentemente si A es un A^e-módulo proyectivo. Si además A es central, proyectivo y fiel como R-módulo, diremos que A es de *Azumaya*.

1.13. **Proposición** [Ba]. Sean A y B R-álgebras de Azumaya. Se verifican

i) A^{op} y $A \otimes_R B$ son álgebras de Azumaya

ii) $A \otimes_R A^{op} \cong \operatorname{End}_R(A)$, el anillo de endomorfismos del R-módulo proyectivo A. Si P es un R-módulo proyectivo, finito y fiel, $\operatorname{End}_R(P)$ es de Azumaya.

iii) Diremos que A es *equivalente* a B si existen módulos proyectivos finitos y fieles, P y Q tales que

$$A \otimes_R \operatorname{End}_R(P) \cong B \otimes_R \operatorname{End}_R(Q).$$

El conjunto de clases de isomorfismo de álgebras de Azumaya dividido por la relación de equivalencia precedente forma un grupo para la operación "$\otimes$". Este grupo se denomina el *grupo de Brauer* de R, $Br(R)$: su 2-torsión se denota por $Br_2(R)$.

Tenemos ahora todo lo necesario para enunciar el

1.14. **Teorema** [M-V-1]. Sea (P,q) un módulo cuadrático de rango n; $C = C(P,q)$ su álgebra de Clifford. Se tienen

i) C es separable proyectiva y de rango 2^n.

ii) Si n es par, C es de Azumaya. Más aún, $C \in Br_2(R)$ y ZC_o es separable y proyectiva de rango 2.

iii) Si n es impar, C_o es de Azumaya y $C_o \in Br_2(R)$. Además $Z(C)$ es separable y proyectiva de rango 2.

Dado un módulo cuadrático de rango par, (P,q) tenemos ahora un nuevo invariante, v.g. su álgebra de Clifford, $C(P,q) \in Br_2(R)$. Observemos sin embargo que la aplicación $(P,q) \mapsto C(P,q)$ no respeta la suma. En efecto, se tiene la

1.15. **Proposición.** Sean (P,q), (P',q') módulos cuadráticos. Se verifica

$$C((P,q) \perp (P',q')) = C(P,q) \hat{\otimes} C(P',q') \quad \blacksquare$$

El segundo miembro de la igualdad anterior es la R-álgebra cuyo módulo subyacente es $C(P,q) \otimes C(P',q')$ y cuyo producto está definido por la fórmula

$$a \,.\, b = (-1)^{i+j}\, a \otimes b \qquad \begin{matrix} a \in C_i(P,q) \\ b \in C_j(P',q') \end{matrix} \quad 0 \leq i,j \leq 1$$

Por otro lado el teorema 1.14 nos permite asociar a cada $(P,q) \in \underline{\underline{Q}}R$ de rango par un álgebra separable de rango 2, ZC_o. Si 2 es inversible, podemos representar localmente a (P,q) en forma diagonal (cf.1.2): $\langle a_1,\ldots,a_n \rangle$ $2n = rk\ P$.

Si escribimos $\Delta = (-1)^n \prod_{i=1}^{2n} a_i = (-1)^n \det(P,q)$ es un elemento inversible definido módulo cuadrados. Se tiene entonces un isomorfismo

$$ZC_0 \cong R[\sqrt{\Delta}]$$

Δ se denomina el *discriminante* de (P,q) y ZC_0 es el *invariante de Arf* de (P,q). El discriminante es más útil que el determinante cuando se está interesado en estudiar formas cuadráticas módulo isotropía. Por otra parte, el invariante de Arf está definido también en el caso en que 2 no es inversible. Si (R,M) es un anillo local con $2 \in M$, y $rk(P,q) = 2$, sea $\{e_1,e_2\}$ una base simpléctica de (P,q). Si $a = q(e_1)\,q(e_2)$ se tiene el isomorfismo

$$ZC_0 \cong \frac{R[X]}{\langle x^2 - x + a \rangle}$$

Por otro lado, se tiene la relación $1 - 4a = \Delta = -\det(P,q)$; de manera que $1 - 4a \notin M$. Si $R^0 = \{r \in R \,/\, 1 - 4r \notin M\}$ vemos que $a \in R^0$; podemos construir un grupo a partir de R^0 como sigue. Dados $r,s \in R^0$ se define una operación

$$r \circ s = r + s - 4r.s \ .$$

Con esta operación R^0 resulta grupo abeliano. Definimos sobre R^0 una relación de equivalencia

$$r \sim s \quad \text{sii} \quad (\exists\, x \in R)/s = r - (x^2 - x)(1-4r)$$

El grupo abeliano $(R^0/\sim, o)$ se denota por $G(R)$ [M-V-1]; $a = a(q)$ está bien definido como elemento de $G(R)$. Si R es ahora un anillo no necesariamente local tenemos definido un invariante $a(P,q) \in \Gamma(\text{Spec } R, G)$. Se puede verificar que en el caso en que 2 es inversible ambas definiciones coinciden. Cuando

veamos extensiones de Galois volveremos sobre este tema. Allí se verá como es posible dar una definición completamente global del grupo de extensiones cuadráticas de rango 2.

Nota histórica. Hemos visto que la aplicación que asigna a cada módulo cuadrático de rango par su álgebra de Clifford como elemento del grupo de Brauer no es aditiva. Este problema se puede arreglar cambiando Br R por el grupo de álgebras de Azumaya graduadas, cuyo producto es el producto graduado $\hat{\otimes}$. El resultado es lo que se conoce como *grupo de Brauer-Wall*, BW(R). H. Bass estudió el BW(R) para el caso en que 2 es inversible ([Ba]), utilizando métodos de teoría K obtuvo una sucesión exacta larga que relaciona BW(R), L(R) y el grupo ortogonal. A. Micali y O. E. Villamayor estudiaron el subgrupo de BW(R) generado por las álgebras de Clifford, $\mathcal{H}_0(R)$([M-V-1,2,3]). De los resultados que obtienen se desprende, grosso modo, que tener el invariante en $\mathcal{H}_0(R)$ es como tener el discriminante y álgebra de Clifford en Br R. Tales invariantes no son suficientes en general; por ejemplo las formas $\langle 1,1,1,1\rangle$ y $\langle -1,-1,-1,-1\rangle$ sobre el cuerpo de los números reales, tienen los mismos invariantes clásicos, y sin embargo no son isomorfas. Este problema motiva la búsqueda de nuevos invariantes; se han hecho numerosos trabajos en tal sentido. Destacamos aquí el trabajo fundamental de J. Milnor [Mil], en el cual se definen clases de Stieffel-Whitney para módulos cuadráticos, sobre un cuerpo R con char R $\neq$ 2. E. Hornix generalizó la teoría para R local [H], que luego extendieron A. Micali y P. Revoy para R semilocal [M-R].

Los invariantes definidos por Micali y Revoy se pueden definir con no mucho más que los elementos que hemos dado en la sección precedente. La obra citada es también una buena referencia para los resultados básicos sobre formas cuadráticas en anillos locales y semilocales. Otro tratado en este sentido es el libro de Baeza [Bae].

2. Teoría de Galois

2.1. Extensiones de Galois

2.1.1. **Definición.** Sea T un anillo conmutativo con 1, R un subanillo (con la misma unidad). Entonces T se dice una *extensión de Galois de* R *con grupo* G si G es un grupo finito de automorfismos de T tal que $R = T^G$ (i.e. R es el conjunto de elementos de T invariantes bajo la acción de G).
Se sigue que T es un módulo finitamente generado sobre R ([V-Z-1]).

2.1.2. **Ejemplo.** Extensiones cuadráticas

Caso local. Sean (R,M) local con $2 \notin M$ y $a \in R$ tal que $a \notin M$. La extensión $T = \dfrac{R[X]}{\langle X^2 - a\rangle} = R[\sqrt{a}]$ es separable. En efecto $e = \dfrac{1 + \sqrt{a} \otimes (1/\sqrt{a})}{2} \in T \otimes T$ es su idempotente de separabilidad.
Además, si definimos $\sigma : T \to T$ como el único morfismo de R-álgebras tal que $\sigma(\sqrt{a}) = -\sqrt{a}$, vemos que $T^\sigma = R$. Por tanto, T es de Galois con grupo $G = \{1,\sigma\} \cong \mathbb{Z}_2$. Si ahora $\tau \in \mathrm{Aut}_R(T)$, i.e. τ es un R-automorfismo de T, se tiene que $[\tau(\sqrt{a})]^2 = a$. Escribimos $\tau(\sqrt{a}) = x + y\sqrt{a}$, se tienen las ecuaciones

$$\begin{cases} x^2 + y^2 a = a \\ 2xy = 0 \end{cases}$$

Por cálculo directo se verifica que las únicas soluciones posibles son $(0,1)$, $(0,-1)$ y $(x,0)$ con $x^2 = a$. En los dos primeros casos se obtiene que $\tau \in \{1,\sigma\}$ mientras que el tercero se descarta pues contradice la hipótesis $\sigma \in \mathrm{Aut}_R(T)$. Hemos probado entonces que si T es de la forma $R[\sqrt{a}]$, para (R,M) local con $2 \notin M$, T es de Galois con grupo $G = \{1,\sigma\} = \mathrm{Aut}_{\quad}(\quad)$. Recíprocamente,

si T es separable sobre R y $\{1,x\}$ es base de T, x^2 se escribe de única forma como combinación lineal de 1 y x, de donde se obtiene que T es de la forma $\frac{R[X]}{\langle x^2 + bx + c\rangle}$. Es claro que si $\Delta = b^2 - 4c \notin M$, podemos reemplazar $x^2 + bx + c$ por $x^2 - \Delta$, obteniéndose así una extensión del tipo $R[\sqrt{\Delta}]$ como antes. Si en cambio $\Delta \in M$, $\frac{R}{M}[X] / \frac{R}{M}$ es una extensión puramente inseparable de $k = R/M$ apelando ahora a [DeM-Math 7.1.], resulta que T no es separable sobre R, lo que contradice nuestra hipótesis. Hemos probado que toda extensión separable y proyectiva T, de rango 2 sobre un anillo local (R,M) con $2 \notin M$ es de Galois, con grupo $G = \mathrm{Aut}_R(T) \cong \mathbb{Z}_2$. El mismo resultado es válido aunque $2 \in M$; en efecto, todo polinomio mónico de grado dos y discriminante inversible se puede llevar a la forma $X^2 - x + m$; independientemente de si 2 está o no en M. La demostración se sigue como en el caso $2 \notin M$.

Caso global. Si T es una extensión separable de R y T es proyectivo con $\mathrm{rk}\ T = 2$, sea $\sigma \in \mathrm{Aut}_R(T)$. Considérese la aplicación

$$f_\sigma(P) = \begin{cases} 1 & \text{si } \sigma_p \neq \mathrm{id}. \\ 0 & \text{si } \sigma_p = \mathrm{id}. \end{cases}$$

(Aquí denotamos por σ_p la localización de σ en P). Es claro que f_σ es continua, es decir podemos ver a f_σ como un elemento idempotente de R. Se tiene así una función

$$\begin{array}{ccc} \mathrm{Aut}_R(T) & \xrightarrow{f} & I_pR = \{e \in R / e^2 = e\} \\ \sigma & \longmapsto & f_\sigma \end{array}$$

que claramente es inyectiva. Gracias al isomorfismo local entre $\mathrm{Aut}_R(T)$ y $\mathbb{Z}_2$ se obtiene que, dotando a IpR de la suma booleana $\hat{+}$; $(e \hat{+} e' = e + e' - 2ee')$,

f resulta un monomorfismo. Es claro que si $X = \operatorname{Spec} R$ es conexo, i.e. si $I_p R = \mathbb{Z}_2$; f es isomorfismo. Al efecto de estudiar f en general, observemos que en virtud de [V-Z-1] se tiene $T = R \oplus P$ con P un R-módulo proyectivo de rango 1. Vamos a suponer por simplicidad que 2 es inversible en R, i.e. $2 \in UR = \{\text{unidades de } R\}$. Sea U un cubrimiento finito por abiertos afines de X, $U = \{U_i : i \in I\}$ tal que $P|_{U_i}$ es libre ($\forall i \in I$). Entonces $T|_{U_i}$ es el cociente de $R|_{U_i}[X]$ por algún polinomio mónico de grado 2; sea Δ_i su discriminante. Entonces Δ_i es una unidad - lo es en cada punto de U_i - y podemos pensar a $T|_{U_i}$ en la forma $R|_{U_i}[\sqrt{\Delta}]$. Si $e \in Ip(U_i) = Ip(R|_{U_i})$ $\sigma : T|_{U_i} \to T|_{U_i}$ definido por $\sigma(\sqrt{\Delta}) = (1-2e)\sqrt{\Delta}$ es un automorfismo. Si ahora $e \in IpR$, e define un automorfismo σ_i sobre cada U_i, $i \in I$, de forma tal que $\sigma_i|_{U_i \cap U_f} = \sigma_j|_{U_i \cap U_j}$, luego un automorfismo $\sigma \in \operatorname{Aut}_R(T)$. Así, f es sobreyectiva, y por tanto f es un isomorfismo. En particular hay un único $\sigma \in \operatorname{Aut}_R(T)$ tq $\sigma_p \neq id$ ($\forall p \in X$). Es claro que $T^{\sigma} = R$; luego T es Galois sobre R con grupo $\mathbb{Z}/2\,\mathbb{Z}$. Resumimos lo probado en el siguiente

2.1.3. **Teorema**. Sea T una extensión separable de R, proyectiva y de rango 2 como R-módulo. Entonces T es Galois con grupo $\mathbb{Z}/2\,\mathbb{Z}$.

2.1.4. **Corolario**. Si S y T son extensiones cuadráticas con grupos $G_1 = \{1, \sigma\}$ y $G_2 = \{1, \tau\}$ respectivamente,

$$S * T = (S \otimes T)^{\sigma \otimes \tau}$$

es también cuadrática. El conjunto de clases de isomorfismo de extensiones cuadráticas provisto de la operación $*$ resulta ser un grupo abeliano, $\beta(R)$. Si $2 \in UR$, $\beta(R) \cong \alpha(R)$.

2.1.5. **Observaciones.** i) Ahora podemos definir la invariante de Arf en forma global, i.e. si $(P,q) \in \underline{Q}(R)$, $Arf(P,q) = \overline{ZC_0(P,q)} \in \beta(R)$.

ii) De 2.1.4 se concluye que $(S \otimes T)^{G_1 \times G_2} = R$. En efecto, si $x \in (S \otimes T)^{G_1 \times G_2} \Rightarrow X \in S * T$ y es fijado por $\sigma \otimes 1$ y $1 \otimes \tau$. Localmente, si $S = R[\sqrt{\Delta_1}] \wedge T = R[\sqrt{\Delta_2}] \Rightarrow S * T = R[\sqrt{\Delta_1 \Delta_2}]$. Luego, $\sigma \otimes 1|_{S*T} = \tau \otimes 1|_{S*T}$ es el único automorfismo que corresponde al idempotente 1. Así, $(S*T)^{\sigma \otimes 1} = R$; luego $(S \otimes T)^{G_1 \times G_2} = R$, como se quería. Concluímos que si $S,T \in \beta(R)$, $S \otimes T$ es de Galois con grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$

En el caso en que R y S no tienen idempotentes no triviales, el teorema Fundamental de la teoría de Galois para cuerpos vale sin modificaciones. Tal teorema se debe a Chase-Harrison y Rosenberg [CH-R]; Villamayor y Zelinsky ([V], [VZ 1 y 2]) extendieron los resultados, con las debidas modificaciones al caso general. Enunciamos aquí el caso más sencillo. Una demostración puede encontrarse en [DeMe-In].

Teorema. Sea $T \supset R$ de Galois con grupo $G = Aut_R(T)$ y supongamos que T no tiene idempotentes no triviales, i.e. $I_p R \cong \mathbb{Z}/2\,\mathbb{Z}$. Entonces

1) G es finito y $[G : 1] = rk_R T$

2) Hay una correspondencia biyectiva

$$H \mapsto T^H \qquad S \to \{\sigma \in G / \sigma(x) = x \ \forall x \in S\}$$

entre los subgrupos de G y las subextensiones de T. El subgrupo H es normal en B si y sólo si la subextensión correspondiente S lo es, i.e. si y sólo si $S^{Aut_R(S)} = R$.

2.2. Cohomología de Galois

2.2.1. **Definición.** Sea G un grupo; A un grupo abeliano. Diremos que A *es un* G-*módulo* si está provisto de una acción

$$G \times A \to A$$
$$(g,a) \mapsto g.a$$

que verifica

$$(g.h).a = g.(h.a)$$
$$g.(a+b) = g.a + g.b$$
$$1.a = a \ .$$

2.2.2. **Ejemplos.** i) Sea S una extensión de Galois de un anillo R, con grupo G. Se consideran los grupos

US: el grupo de unidades - elementos inversibles - de S.

$\mu_2 S$: el grupo de raíces cuadradas de la unidad en S.

IpS: el grupo de idempotentes de S (con la suma booleana).

U^2S: $\{u^2/u \in US\}$ y $\dfrac{US}{U^2S}$.

Observemos que todos ellos son G-módulos por la acción $(\sigma,x) \mapsto \sigma(x)$.

ii) Sea $\mathrm{Pic}\ S$ el grupo de Picard de S, es decir, el grupo de clases de isomorfismo de S-módulos de rango 1 (con la operación "$\otimes$"). Si $\bar{X} \in \mathrm{Pic}\ S$ definimos $\sigma.\bar{X} = \overline{X_\sigma}$, donde X_σ es isomorfo a X como R-módulo y si $x \in X_\sigma$, $s \in S$ entonces $s.x = \sigma(s)X$ ■

2.2.3. **Observación.** Observemos que de la definición de G-módulo se deduce que es lo mismo que A sea un G-módulo a que sea un $\mathbb{Z}[G]$-módulo. En particular, el morfismo

$$\mathbb{Z}[G] \twoheadrightarrow \mathbb{Z}$$

$$g \mapsto 1 \qquad (g \in G)$$

dota a $\mathbb{Z}$ de una estructura de G-módulo. Tiene entonces sentido considerar los grupos $\mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z},A)$. Definimos

$$H^n(G,A) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z},A)$$

Decimos que $H^n(G,A)$ es el n-*ésimo grupo de cohomología del grupo* G *con coeficientes en* A.

Es un hecho conocido ([McL]) que los $H^n(G,A)$ pueden definirse equivalentemente como los grupos de cohomología del complejo de cocadenas

$$(2.2.4) \qquad C_o \xrightarrow{\partial} C_1 \xrightarrow{\partial} C_2 \xrightarrow{\partial} \cdots \xrightarrow{\partial} C_n \xrightarrow{\partial} C_{n+1} \xrightarrow{\partial} \cdots$$

donde

$C_n := \{f : G^n \to A\}$ es el conjunto de funciones de G en A.

$C_n \xrightarrow{\partial} C_{n+1}$ está definida por

$$(\partial f)(\alpha_1,\ldots,\alpha_{n+1}) = \alpha_1(f(\alpha_2,\ldots,\alpha_{n+1})) + \sum_{i=1}^{n} (-1)^i f(\alpha_1,\ldots,\alpha_i\cdot\alpha_{i+1},\ldots,\alpha_{n+1}) + (-1)^{n-1} f(\alpha_1,\ldots,\alpha_n)$$

2.2.5. **Ejemplos.** i) Si $S \supset R$ es una extensión de Galois y S,R son *cuerpos*, el Teorema 90 de Hilbert asegura que $H^1(\mathrm{Gal}(S/R),US) = 0$.

ii) S,R como en i) sea $\mathrm{Br}(S/R) = \mathrm{Ker}(\mathrm{Br}(R) \to \mathrm{Br}(S))$, entonces, si $G = \mathrm{Gal}(S/R)$

$$H^2(G,US) \cong \mathrm{Br}(S/R). \text{ (cf. [Sel])}$$

iii) Sea R un cuerpo, E su clausura separable. Entonces ([Bal]) $\mathrm{Br}(E/R) = \mathrm{Br}(R)$. Además si $G = \varprojlim_{S \text{ de Galois}} \mathrm{Gal}(S/R)$ se tiene que

$$H^2(G,UE) = \varinjlim_{S \text{ Galois}} H^2(\mathrm{Gal}(S/R),US) = Br(R).$$

iv) Sean R,E y G como antes, con char $R \neq 2$. Considérese la sucesión exacta de G-módulos

$$0 \to \mathbb{Z}/2\,\mathbb{Z} = \mu_2 E \to UE \xrightarrow{2} UE \to 1$$

donde el símbolo "2" representa la flecha $x \to x^2$. La definición de cohomología implica la existencia de una sucesión exacta larga. Nos interesan sus primeros términos:

$$0 \to H^0(G,\mathbb{Z}/2\,\mathbb{Z}) \to H^0(G,UE) \xrightarrow{2} H^0(G,UE) \to H^1(G,\mathbb{Z}_2) \to H^1(G,UE) \xrightarrow{2} H^1(G,UE) \to$$
$$\to H^2(G,\mathbb{Z}/2\,\mathbb{Z}) \to H^2(G,UE) \xrightarrow{2} H^2(G,UE)$$

Dado que para cualquier G-módulo A (y cualquier G) $H^0(G,A) = A^G$ en virtud de i) y de la sucesión exacta anterior se tienen:

$$H^0(G,\mathbb{Z}_2) = \mathbb{Z}_2 \; ; \; H^0(G,UE) = UR$$
$$H^1(G,\mathbb{Z}_2) = UR/U^2R \; ; \; H^2(G;\mathbb{Z}/2\,\mathbb{Z}) = Br_2(R)$$

2.2.6. **Producto cup.** Consideremos el producto "cup" (ver [McL, VIII-9])

$$U : H^n(G,A) \otimes H^m(G,B) \to H^{n+m}(G,A \otimes_{\mathbb{Z}} B).$$

Nos interesa en especial el caso en que $A = B = \mathbb{Z}_2$ y la acción de G es la trivial; damos la fórmula explícita en términos del complejo (2.2.4)

$$f \cup g\,(\alpha_1,\ldots,\alpha_{n+m}) = f(\alpha_1,\ldots,\alpha_n)g(\alpha_{n+1},\ldots,\alpha_{n+m}) \qquad f \in C_n, \quad g \in C_m$$
$$a_i \in G, \quad 1 \leq i \leq n+m.$$

Es inmediato que $(\partial f) \cup g = f \cup \partial g = \partial(f \cup g)$ lo que permite pasar a los H^n.

2.2.7. Clases características de Delzant.

Gracias a 2.2.5, en el caso en que R es un cuerpo con $\operatorname{char} R \neq 2$, la sucesión exacta de 1.6 puede reescribirse, si G es como en 2.2.5, de la siguiente manera

$$0 \to I \to \mathbb{Z}[H^1(G, \mathbb{Z}_2)] \to L(R) \to 0 .$$

Sea $AC(G, \mathbb{Z}_2) = \coprod_{n \geq 0} H^n(G, \mathbb{Z}_2)$; provisto con la multiplicación dada por el producto "cup" (2.2.6), se convierte en un anillo.

Sea $\widetilde{AC}$ el grupo de unidades de $AC = AC(G, \mathbb{Z}_2)$.

Hay un único morfismo

$$\mathbb{Z}[H^1(G, \mathbb{Z}/2\,\mathbb{Z})] \xrightarrow{D} \widetilde{AC}$$

$$D(a) = 1 + a \qquad (a \in H^1(G, \mathbb{Z}_2)) .$$

Para ver que D define un morfismo desde $L(R)$, debemos ver que D se anula en los generadores de I. En virtud de 1.6 ello equivale a verificar que el producto

$$(1+a)(1+b) = 1 + (a+b) + a\ b \in \widetilde{AC} \qquad a,b \in H^1(G, \mathbb{Z}/2\,\mathbb{Z})$$

no depende más que de la clase de isomorfismo de la forma cuadrática $\langle \bar{a}, \bar{b} \rangle$ (recuérdese el isomorfismo $H^1(G, \mathbb{Z}_2) \cong UR/U^2R$).

Ahora bien, se tienen las fórmulas

$$\overline{a + b} = \bar{a}\,\bar{b} = \det \langle a,b \rangle \in UR/U^2R .$$

$$a \cup b = C(\langle a,b \rangle) \in Br_2(R).$$

La primera de ellas es inmediata, la segunda se probará en un contexto algo más general, en el § 2.

Quedan así definidas las clases de Delzant (cf. [Del]); que han sido estudiadas entre otros por Scharlau.

Si deseamos construir una teoría de invariantes semejante en el caso general de

anillos necesitamos dar alguna interpretación cohomológica al grupo de Brauer. El teorema siguiente ilustra la situación.

2.2.8. **Teorema** (Chase-Harrison-Rosenberg). Sea R un anillo conmutativo y S una extensión de Galois de R con grupo $G = \mathrm{Aut}_R(S)$. Hay una sucesión exacta natural

$$1 \to H^1(G,US) \to \mathrm{Pic}\ R \to \mathrm{Pic}\ S \to H^2(G,US) \to Br(S/R) \to H^1(G,\mathrm{Pic}\ S)$$

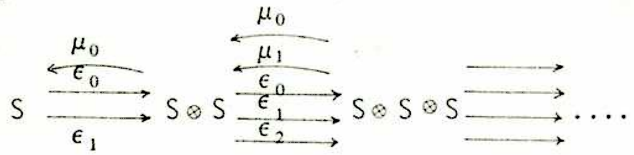
2.2.9. **Corolario** (Teorema 90 de Hilbert). Si $\mathrm{Pic}\ R = 1 \Rightarrow H^1(G,US) = 1$.

2.2.10. **Corolario.** Si $\mathrm{Pic}\ S = 1$ entonces $Br(S/R) = H^2(G,US)$.

La versión del teorema de Chase-Harrison y Rosenberg que acabamos de dar es la que está en el curso de [DeMe-In] Su versión original se encuentra en [C-H-R]. El teorema anterior restringe bastante el tipo de extensión que podemos tomar. Ahora bien, si queremos obtener una sucesión exacta como la de 2.2.8 para una extensión más general, necesitamos cambiar la cohomología de Galois por otra que se pueda definir en tal caso. Sobre ese tema trata la sección siguiente.

3. Cohomología de Amitsur

Sea S/R un álgebra conmutativa con unidad. Se considera el complejo simplicial de R álgebras



Donde, si denotamos por $S^{\otimes n}$ la n-ésima potencia tensorial de S, se tiene

$$\epsilon_i : S^{\otimes n} \to S^{\otimes(n+1)}$$

$$s_1 \otimes \ldots \otimes s_n \mapsto s_1 \otimes \ldots \otimes s_i \otimes 1 \otimes s_{i+1} \otimes \ldots \otimes s_n.$$

$$\mu_i : S^{\otimes(n+1)} \to S^{\otimes n}$$

$$s_1 \otimes \ldots \otimes s_{n+1} \mapsto s_1 \otimes \ldots \otimes s_i \otimes s_{i+1}\ s_{1+2} \otimes s_{i+3} \otimes \ldots \otimes s_{n+1}$$

Los morfismos ϵ_i son las *caras* y los μ_i las *degeneraciones* del complejo. Nuestro interés se centrará en los ϵ_i. Dado un funtor covariante F, de anillos en grupos abelianos, se obtiene un complejo de cocadenas $\{C(S/R,F),\partial\}$ donde

$$C_n = C(S/R,F)_n = F(S^{\otimes(n+1)}) \qquad n \geq 0$$

$$\partial : C_n \to C_{n+1}$$

$$\partial = \sum_{i=0}^{n+1} (-1)^i F(\epsilon_i)$$

Es decir, el complejo de cocadenas asociado a todo complejo simplicial de grupos abelianos. La cohomología de tal complejo se denomina la *cohomología de* F *relativa a* S/R. El n-ésimo grupo de la cohomología relativa se denota por $H^n(S/R,F)$.

3.1. **Ejemplo.** En el caso en que S es de Galois sobre R con grupo G, podemos también considerar funtores con valores en la categoría de G-módulos, y por ende el complejo $C(G,F(S))$ 2.2.4. En el caso en que R y S son cuerpos y $F = U,\mu_2,Ip$ Amitsur probó que ambos complejos son isomorfos [Am]. En [C-H-R] se extiende el resultado a extensiones galoisianas de anillos con $G = Aut_R(S)$. La demostración de Amitsur es completamente general y sus morfismos son naturales. El punto crucial es el lema 6.2 (pp.98); este lema no es válido para extensiones de Galois generales.

3.2. **Teorema** [V-Z-3]. Para toda extensión de anillos conmutativos S/R hay una sucesión exacta natural

$$0 \to H^1(S/R,U) \to H^1(J) \to H^0(S/R,Pic) \to \ldots$$
$$\to H^n(S/R,U) \to H^n(J) \to H^{n-1}(S/R,Pic) \to H^{n+1}(S/R,U) \to \ldots$$

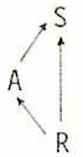
Más aún, si S es fiel proyectivo y finito como R módulo s

$$H^2(J) = Br(S/R) \text{ y } H^1(J) = Pic\ R.$$

Aquí el $H^n(J)$ es complicado de definir. Sólo diremos que es un cierto subcociente del K_0 de Bass relativo al funtor de borde $\underline{Pic}\ S^{\otimes n} \xrightarrow{\partial} \underline{Pic}\ S^{\otimes n+1}$.

Dado un anillo R, se consideran la categoría $\chi' = \chi'(R)$ cuyos objetos son las álgebras separables, conmutativas y proyectivas como módulo; las flechas de χ' son los morfismos separables. En virtud de la

3.3. **Proposición** [DeMe-In]. Supongamos que se tiene un diagrama conmutativo



de anillos conmutativos con unidad. Se satisfacen:

i) Si S/R es separable $\Rightarrow$ A/R es separable

ii) Si S/A y R/A son separables $\Rightarrow$ S/R es separable

iii) Si T/R es otra extensión separable $\Rightarrow$ $S \otimes T/R$ es separable ■

Se tiene entonces que $\chi' = \chi'(R)$ satisface los axiomas de una categoría con suma directa. El lector informado observará que la categoría opuesta χ'^{op} constituye una topología de Grothendieck. Por abuso de notación llamaremos a χ' la *topología separable* de R. Análogamente se define $\chi = \chi(R)$, la *topología separable de rango constante*.

Si G es un funtor covariante de anillos en grupos abelianos podemos definir, dado $A \in \chi'(R)$(ó $\chi(R)$), los grupos de cohomología $H^n(A/R,G)$, como al principio de este §.

Dado un diagrama conmutativo como en 3.3 con $S \in \chi'$(ó $\in \chi$) la funtorialidad de G produce un morfismo natural de grupos $H^n(A/R,G) \to H^n(S/R,G)$ $n \geqslant 0$. Si G es exacto a izquierda, en virtud de 3.3 iii) y de [Ar-Prop.3.4] los $H^n(A/R,G)$ ($A \in \chi'$ (ó $\in \chi$)) forman un sistema dirigido. El límite se denota por $\check{H}^n(\chi',R,G)$ (resp. $\check{H}^n(\chi,R,G)$) y se denomina el n-*ésimo grupo de cohomología de Čech de* G *sobre* $\chi'(R)$ *(resp.* $\chi(R)$*)*.

La proposición siguiente asegura la funtorialidad de $H^n(\chi',.,G)$ (y de $H^n(\chi,.,G)$)

3.4. **Proposición** [DeMe-In]. Sean S_1 y S_2 álgebras conmutativas sobre R. Sean A_1/S_1 y A_2/S_2 extensiones separables. Entonces $A_1 \otimes A_2$ es naturalmente separable sobre $S_1 \otimes S_2$ ■

Observemos que la proposición anterior nos permite también considerar $\varinjlim_{i \in I} H^n(X', R_i, G)$, dado un sistema directo de anillos $\{R_i : i \in I\}$.
Estas propiedades se explotarán en el parágrafo siguiente.

Si deseamos definir clases características para módulos cuadráticos sobre un anillo R con $2 \in UR$, los grupos $\check{H}^n(X', R, Ip) \cong \check{H}^n(X', R, \mu_2)$ parecen ser una traducción adecuada al caso general, de la cohomología $H^n(G, \mathbb{Z}_2)$ para el caso de cuerpos (ver 2.2.7). Necesitamos un producto cup, para completar la analogía Es claro que basta definirlo para los grupos relativos $H^n(S/R)$, con $S \in X'$ ó X. La aplicación

$$\begin{aligned} Ip(S^{\otimes n+1}) \times Ip(S^{\otimes m+1}) &\xrightarrow{U} Ip(S^{\otimes (n+m+1)}) \\ (x,y) &\longmapsto (\epsilon_0^m x).(\widetilde{\epsilon}_n)(y), \end{aligned}$$

donde $\widetilde{\epsilon}_n = \epsilon_{n+m} \circ \epsilon_{n+m-1} \circ \ldots \circ \epsilon_{m+1}$, verifica la fórmula

$$X \cup \partial Y = \partial X \cup Y = \partial(X \cup Y)$$

y define por tanto un producto cup en la cohomología. En el caso en que S es una extensión de Galois finita con grupo G, el isomorfismo de Amitsur lleva el producto cup de la cohomología de G en el producto cup que acabamos de definir. Esto puede verificarse por cálculo directo o bien aplicando el teorema de unicidad de Eilenberg-Zilber [McL].

§0. NOTACIONES Y DEFINICIONES BASICAS.

0.1. Todos los anillos que consideraremos en este trabajo se entenderán conmutativos y con unidad. Sea entonces R un anillo, consideraremos las siguientes topologías de Grothendieck:

$\chi' = \chi'(R)$: la topología de las álgebras separables sobre R que son proyectivas (por tanto finitas) como R-módulos.

$\chi = \chi(R) \subset \chi'$: la topología de las álgebras en χ' que tienen rango constante.

Observemos que $\chi' = \chi$ sii R no posee idempotentes no triviales. Si ahora G es un haz de grupos sobre χ' (respectivamente sobre χ) denotamos por

$$H^n(\chi';R,G) \quad (\text{resp } H^n(\chi,R,G)) \qquad n \geq 0$$

al n-ésimo grupo de cohomología de Čech de G. Si además G es un haz de anillos, escribiremos

$$AC(\chi,R,G) = \prod_{i\geq 0} H^i(\chi,R,G)$$

$AC(\chi,R,G)$ resulta entonces un anillo, provisto del producto cup, que denotaremos, como es usual, por el símbolo "$\cup$". Estudiamos especialmente los haces:

μ_2: raíces cuadradas de la unidad
U : elementos inversibles
Ip: elementos idempotentes

Observemos que IpR tiene estructura de anillo y cuando $2 \in UR$, $\mu_2 R$ es isomorfo como grupo a IpR. Por tanto, cuando $2 \in UR$, consideramos μ_2 como haz de anillos.

0.2. Sea P un R-módulo; una <u>forma cuadrática</u> sobre P es una función

$$q: P \to R$$

que verifica

$q_1)$ $q(\lambda x) = \lambda^2 q(x)$ $\forall$ $\lambda \in R$, $x \in P$.

$q_2)$ $\Phi_q : P \times P \to R$
$(x,y) \to q(x+y) - q(x) - q(x)$
es bilineal.

Si además se satisface que

$q_3)$ $\varphi_q : P \to P^*$
$x \to \Phi_q(x,\cdot)$ es un isomorfismo

Decimos que q es regular. Un R-módulo cuadrático es un par (P,q) donde

$(P,q)_1)$: P es un R-módulo proyectivo finitamente generado.
$(P,q)_2)$: $q : P \to R$ es una forma cuadrática regular.

El rango de (P,q) -$rk(P,q)$- es por definición el rango de P.

Sean las categorías:

$\underline{\underline{P}} = \underline{\underline{P}}(R)$: la categoría de los módulos proyectivos finitamente generados de rango constante sobre R .

$\underline{\underline{Q}} = \underline{\underline{Q}}(R)$: la categoría de los módulos cuadráticos (P,q) con $P \in \underline{\underline{P}}(R)$.

es claro que $\underline{\underline{P}}$ con la suma directa, $\oplus$, y $\underline{\underline{Q}}$ con la suma ortogonal $\perp$ son categorías con producto. En particular, si P y Q denotan respectivamente el conjunto de clases de isomorfismo de $\underline{\underline{P}}$ y $\underline{\underline{Q}}$, se tiene que P y Q son funtores de la categoría de anillos en la categoría de monoides abelianos.

0.3. Si $(P,q) \in \underline{\underline{Q}}R$ y P es libre, una base ortogonal de (P,q) es una base de P

$B = \{ V_i : 1 \leq i \leq n \}$ con $\Phi_q(V_i, V_j) = 0$ si $i \neq j$.

Si $\mathrm{rk}\, P = 2n$ una <u>base simpléctica</u> de (P,q) es una sucesión

$B = \{(V_{1i}, V_{2i}): 1 \leq i \leq n\}$ con $\overline{B} = \{V_{1i}, V_{2i} : 1 \leq i \leq n\}$ base de P_1 que verifica

B_1: Si $1 \leq i \neq j \leq n$ los submódulos $\langle V_{1i}, V_{2i}\rangle$ y $\langle V_{1j}, V_{2j}\rangle$ son ortogonales.

B_2: $\Phi_q(V_{1i}, V_{2i}) = 1$ $(\forall\ 1 \leq i \leq n)$.

Dos bases ortogonales (resp. simplécticas) de (P,q) se dicen <u>contiguas</u> si existe una familia finita de bases ortogonales (resp. simplécticas) $B_0 = B, B_1, \ldots, B_k = B'$ tales que B_{k+1} difiere de B_k en a lo sumo dos elementos.

§1. EL ANILLO $A(R)$; CONSTRUCCION Y PROPIEDADES.

1.0. En esta sección se considera un anillo fijo, conmutativo, con unidad, que denotaremos por R. Sea $X = \mathrm{Spec}R$ el esquema afín asociado a R, supondremos que X es localmente conexo. Esta hipótesis se verifica, por ejemplo, cuando X es noetheriano. Consideremos la clase de todos los cubrimientos finitos de X, cuyos elementos son abiertos, afines y conexos, que denominaremos $C_1 = C_1(X)$. A cada $Z = \{U_i : i \in I\} \in C_1$ le asociamos el esquema afín $X_Z = \sum_{i\in I} U_i$, i.e. el espectro del anillo $R_Z = \prod_{i\in I} \Gamma(U_i, O_X)$. ($\Sigma$ representa unión disjunta, $\Gamma(\cdot, O_X)$ es el funtor de secciones del haz estructural O_X). Sea $C_2(X) =$

$= \bigcup_{Z\in C_1(X)} C_1(X)$, y en general, $C_{n+1}(X) = \bigcup_{V\in C_n(X)} C_1(X_Z)$. Sea $D_0(X) = \{X\}$ y dado $n \in \mathbb{N}$, $D_n(X) = \{X_Z : Z \in C_n(X)\}$, $D(X) = \sum_{n\geq 1} D_n(X)$, y dados $Y \in D_n$, $Z \in D_{n+1}$, ponemos $D(Z,Y) = \begin{cases} \iota_{Z,Y} & \text{si } \exists\ V \in C_{n+1}(Y) \text{ tal que } Z = Y_V \\ \emptyset & \text{en otro caso.} \end{cases}$

Donde, si $V = \{V_j : j \in J\}$, $\iota_{Z,Y}$ es la suma sobre j de las inclusiones $V_j \overset{\iota_j}{\subset} Y$, i.e.

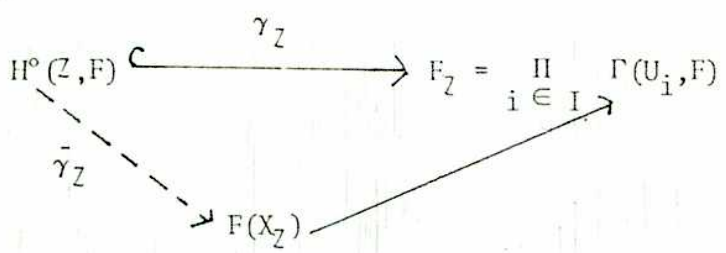
$$\iota_{Z,Y} : Z \overset{\sum_{j\in J} \iota_j}{\to} Y$$

Si ahora $Z,Y \in D_n(X)$ ponemos $D(Z,Y) = \emptyset$ y si $Z \in D_m(X)$, e $Y \in D_n(X)$ con $m > n$, los elementos de $D(Z,Y)$ son todas las composiciones de flechas sobre todos los caminos que unen Z con Y . Es fácil ver entonces que D es un sistema filtrante inverso, i.e. que podemos tomar límite inverso sobre D en la categoría de esquemas afines. En efecto, si reemplazamos $D_n(X)$ por $E_n(X) = \{\Gamma(X_Z,\theta_{X_Z}) : X_Z \in D_n(X)\}$ e inclusiones por restricciones, obtenemos un sistema directo de anillos, denotamos su límite por $A = A(R)$, si $M = \mathrm{Spec}A$, es claro que $M = \varinjlim_D X_Z$ en la categoría de esquemas afines.

BORRAR

Proposición 1.1. Sea F un funtor contravariante de la categoría esquemas afines en la categoría de monoides abelianos, y supongamos que

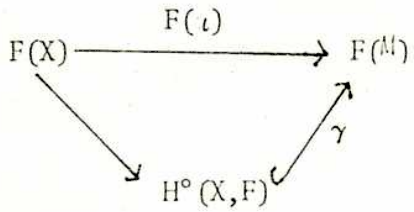
i) $\forall\ Z \in C(X) = \sum_{n\geq 1} C_n(X)$ $\quad Z = \{U_i \ i \in I\}$ hay un diagrama conmutativo natural(*)



ii) $F(\varprojlim_D X_Z) = \varinjlim_D F(X_Z) = F(M)$

Se tiene entonces un diagrama conmutativo:

(*) Consideramos a F como haz de grupos abelianos sobre X .



En particular, si denotamos por $F_p = \varinjlim_{p \in U} F(U)$, $(p \in X)$, se tiene

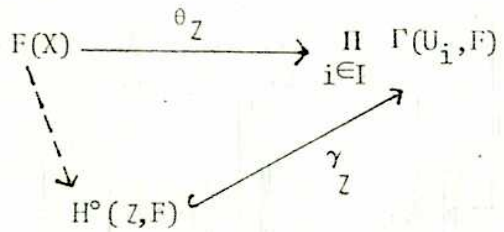
$$\operatorname{Ker} F(\iota) = \bigcap_{p \in X} \operatorname{Ker}(F(X) \to F_p)$$

Demostración:

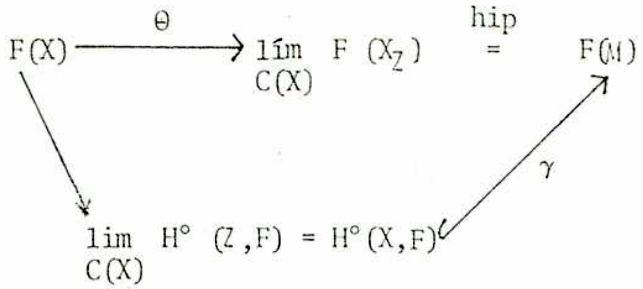
Sea $\mathcal{Z} \in C(X)$, $\mathcal{Z} = \{U_i : i \in I\}$; $H^\circ(\mathcal{Z},F)$ es el núcleo del par $(\varepsilon_0, \varepsilon_1)$, donde ε_k es la cara i-ésima en el complejo simplicial de Čech asociado a $\mathcal{Z}$ en nivel $1, k = 0,1$, es decir, la siguiente es una sucesión exacta:

$$H^\circ(\mathcal{Z},F) \xrightarrow{\gamma_{\mathcal{Z}}} \prod_{i \in I} \Gamma(U_i,F) \underset{\varepsilon_1}{\overset{\varepsilon_0}{\rightrightarrows}} \prod_{i,j \in I} \Gamma(U_i \cap U_j,F)$$

Es claro entonces que el morfismo de restricción, $\theta_{\mathcal{Z}}$, se factoriza a través de $H^\circ(\mathcal{Z},F)$, i.e. se tiene un diagrama conmutativo:



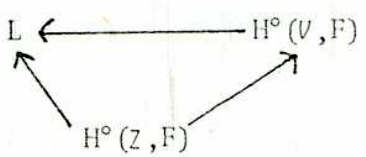
Por hipótesis, $\gamma_{\mathcal{Z}}$ se factoriza a través de $(\bigcup_{i \in I} U_i)$. Ahora pasamos al límite; se obtiene el diagrama conmutativo:



Sólo resta aclarar la igualdad en el nivel inferior del triángulo anterior. En primer lugar observemos que, si U es un abierto cualquiera en $\mathrm{Spec}R$, podemos definir $F(U) = F(\mathrm{Spec}\Gamma(U,\mathcal{O}_X))$, sea U afín o no, y esta definición nos permite mirar a F como prehaz sobre $\mathrm{Spec}R$, aunque F no esté definido para esquemas no afines. Hecha esta observación, es claro que, en virtud de las hipótesis sobre X, podemos tomar límite sobre la colección, F, de todos los cubrimientos afines, conexos y finitos, ordenada parcialmente por la relación "ser más fino que". Por otro lado, todo $Z \in C(X)$ puede mirarse como cubrimiento de X, y si $Z \ll V$ en $C(X)$, V es más fino que Z como cubrimiento de X, luego, se tiene un morfismo canónico:

$$L = \lim_{C(X)} H^\circ(Z,F) \quad \to \quad L' = \lim H^\circ(Z,F) \ .$$

Para definir una flecha en sentido contrario, basta observar que si $Z, V \in F$, son tales que V es más fino que Z, el siguiente diagrama es conmutativo:



Pero tal conmutatividad se deduce inmediatamen de la propiedad filtrante de $\ll$. La verificación de que ambas composiciones dan . identidad es trivial. ■ □

Corolario 1.2.

Sea F un funtor contravariante de esquemas afines en grupos abelianos y $n \geq 0$. Se tiene

$$\check{H}^n(X,F) = \varinjlim_{Z \in C(X)} H^n(Z,F)$$

Demostración.

Es análoga a la dada más arriba para el caso $n = 0$.

Teorema 1.3.:

Sea R un anillo en las hipótesis enunciadas al comienzo de esta sección. Con todas las notaciones y definiciones anteriores se tiene que $A = A(R)$ verifica las siguientes propiedades:

i) A es una R-álgebra fielmente playa.

ii) Todo A-módulo proyectivo finitamente generado de rango constante es libre.

iii) Sea (P,q) un A-módulo cuadrático de rango constante. Si $2 \in UR$ (resp. si $2 \in RadR$) (P,q) tiene una base ortogonal (resp. simpléctica) y dos de tales bases son contiguas.

iv) Los funtores $F_1 = P$ y $F_2 = Q$ definidos en 0.1 verifican las hipótesis de la proposición anterior. En particular,

$$\mathrm{Ker}(F_i(R) \to F_i(A)) = \bigcap_{p \in \mathrm{Spec}R} \mathrm{Ker}(F_i(R) \to F_i(R_p)) \qquad i = 1,2$$

v) Sea χ el funtor que asigna a cada anillo la topología de las extensiones separables que son proyectivas como módulos. $S_1 = U$, $S_2 = \mu_2$, $S_3 = Ip$ los haces sobre χ de unidades, raíces cuadradas de 1 e idempotentes respectivamente $\forall\, n \geq 0$, el funtor

$$H^n(\chi,\cdot,S_i) \qquad i = 1,2,3$$

verifica las hipótesis de la proposición anterior. En particular

$$\mathrm{Ker}(H^n(\chi,R,S_i) \to H^n(\chi,A,S_i)) = \bigcap_{P\in \mathrm{Spec}R} \mathrm{Ker}(H^n(\chi,R,S_i) \to H^n(\chi,R_p,S_i)$$

Demostración:

i) Que A es playo se deduce de que cada R_Z lo es, en vista de la exactitud del límite directo y de la conmutatividad entre este último y $\otimes$. Sea M ideal maximal en R, $M^e = MA$ su extensión en A, debemos ver $M^e \neq (1)$. Supóngase que $1 \in M$, existen entonces m_i $(1 \leqslant i \leqslant r)$ $m_i \in m^e$ con $1 = \sum_{i=1} m_i$. Cada m_i es a su vez una combinación lineal finita de elementos de m con coeficientes en A; $m_i = \sum_{j=1}^{s_i} a_{ij}\, m_{ij}$. Dado que los a_{ij} son finitos existe un R_Z tal que todo a_{ij} puede mirarse como elemento de R_Z.
Dado que $\sum_{i=1}^{r} \sum^{s_i}_{j=1} a_{ij}\, m_{ij} = 1$ en A, existe $V \gg Z$ tal que la igualdad vale en R_V; pero R_V es fielmente playo, contradicción.

ii) Sea P un A-módulo proyectivo finitamente generado, entonces P es sumando directo de A^n para algún $n \geqslant 1$. Si Π es un proyector con $\mathrm{Im}\ \Pi = P_1$, y sea M la matriz de Π en la base canónica, podemos mirar a M en algún R_Z donde se verifica $M^2 = M$. Es decir que M define un proyector $\Pi_Z : R_Z^n \to R_Z^n$ a cuya imagen denominamos P_Z; es claro que $P_Z \otimes_{R_Z} Z = P$. Si ahora P tiene rango constante r, resulta que $\mathrm{rk}\ P_Z = r$, pues como vimos en la demostración de i), A es fielmente playo como R_Z-álgebra. Ahora basta tomar un $V \in C(X)$ con $V \gg Z$ tal que $P_V = P_Z \otimes_{R_Z} R_V$ sea libre.

iii) Supongamos $2 \in UR$; la demostración para $2 \in \mathrm{Rad}R$ es idéntica. Sea q una forma cuadrática regular sobre A^n, cuya matriz en la base canónica es M. Como en ii) podemos tomar R_Z tal que los coeficientes de M

estén en R_Z y que $\det M \in UR_Z$. Existe entonces, [(M-R)] un $V \in C(X)$ tal que $V \gg Z$ y $C \in Gl_n(R_V)$ con $C M C^{-1}$ diagonal, lo que prueba la existencia de una base ortogonal para q.
Si ahora B y B' son dos bases ortogonales de (A^n,q), podemos pensarlas como bases de (R_Z^n, q_Z) para algún Z, y podemos repetir el procedimiento anterior [M-R].

iv) Veamos el caso cuadrático en primer lugar. Un elemento de $H^0(Z,Q)$ es, a través de γ_Z, una I-upla $((\overline{P_i,q_i}))_{i\in I}$ tal que $(\overline{P_i,q_i}) = (\overline{P_j,q_j})$ sobre $U_i \cap U_j$. Entonces $(P,q) = \bigoplus_{i\in I} (P_i,q_i)$ es un módulo cuadrático de rango constante sobre R_Z, con lo que se obtiene la factorización deseada, y la misma demostración vale para P. Vamos entonces a la segunda hipótesis, y comencemos nuevamente por el caso cuadrático.
Sea (P,q) un módulo cuadrático sobre A de rango constante, según la demostración de iii) $(\exists\ Z \in C(X))$ y (P_Z,q_Z) módulo cuadrático sobre R_Z con $(P,q) = (P_Z,q_Z) \otimes_{R_Z} A$. Esto prueba que la aplicación natural

$$\varinjlim_{E(X)} Q(R_Z) \to Q(A) \qquad (1.3.1)$$

es sobreyectiva. Para ver la inyectividad, observemos que dos elementos del miembro izquierdo de (1.3.1) siempre se pueden mirar como módulos cuadráticos libres sobre un mismo $R_Z \in E(X)$. Sean entonces (P,q) y (P',q') módulos cuadráticos libres sobre R y supongamos que se tiene un isomorfismo $\alpha : (P,q) \otimes_{R_Z} A \xrightarrow{\sim} (P',q') \otimes_{R_Z} A$. Entonces α está representado por una matriz finita y razonando como en ii) e iii) se encuentra $V \gg Z$ con $(P,q) \otimes_{R_Z} R_V \cong (P',q') \otimes_{R_Z} R_V$ lo que prueba la inyectividad. Es claro que la misma demostración vale para el funtor P. Sólo resta observar que la fibra del prehaz F_i en un punto $p \in X$, coincide con $F_i(R_p)$ $(i = 1,2)$.

v) Es claro que cada uno de los haces en cuestión preserva productos finitos, es decir, si G es uno de ellos y B_1, B_2 son dos anillos, resulta que $G(B_1 \times B_2) = G(B_1) \times G(B_2)$. Verificaremos la hipótesis i) de la proposición 1.1. para $\check{H}^n(\chi,\cdot,G)$ cuando G preserva productos finitos. Sea $R_i = \Gamma(U_i,\theta_\chi)$ $(i \in I)$; un elemento de $\prod_{i\in I}\Gamma(U_i, \check{H}^n(\chi,U_i,G))$ se puede mirar como una I-upla $c = (\bar{c}_i)_{i\in I}$ donde cada $\bar{c}_i$ es la clase de un n-cociclo en $G(B_i \otimes_{R_i}^{n+1})$. En consecuencia c define un cociclo en $G(\prod B_i \otimes_{R_i}^{n+1}) = \prod G(B_i \otimes_{R_i}^{n+1})$; es un hecho trivial que el complejo simplicial evidente que tiene a $\prod B_i \otimes_{R_i}^{n+1}$ en el lugar n es isomorfo al complejo simplicial de Amitsur asociado a la R_Z-álgebra $\prod_{i\in I} B_i$. Hemos definido entonces un morfismo

$$\prod_{i\in I} \check{H}^n(\chi,R_i,G) \quad \to \quad \check{H}^n(\chi',R_Z,G) \qquad (1.3.2)$$

donde χ' es la topología de las álgebras separables y proyectivas tal como fue definida en 0.1. Pero es fácil de ver que $\chi(R_Z)$ es cofinal en $\chi'(R_Z)$, así que en el miembro derecho de (1.3.2) podemos reemplazar χ' por χ, y ahora es claro que (1.3.2) es la inversa del morfismo natural en sentido opuesto. Hemos demostrado entonces que $\check{H}^n(Y,R_Z,G)$ es naturalmente isomorfo a $\prod_{i\in I} \check{H}^n(Y,R_i,G)$, y en particular se verifica la hipótesis i) de la proposición.

La verificación de la hipótesis ii) es consecuencia trivial de la parte a) de la proposición 1.4. Sólo nos resta ver entonces que, para i=1,2,3, la fibra del prehaz $\check{H}^n(\chi,\cdot,S_i)$ sobre cada punto $p \in X$ coincide con $\check{H}^n(\chi,R_p,S_i)$. Es claro que si $B \in \chi(X)$, $S_i(B)$ define un haz sobre X cuya fibra en cada $p \in X$ es $S_i(B_p)$. Sea G un funtor con tal propiedad. Dado $\bar{c} \in \check{H}^n(\chi,R_p,G)$ lo podemos mirar en $H^n(B/R_p,G)$ para algún $B \in \chi(R_p)$. Como

se ve en la demostración de a) existe U entorno afín y conexo de p y $B_U \in \chi(\Gamma(U,O_X))$, tales que, si ponemos $R(U) = \Gamma(U,O_X)$, se tiene que $B = B_U \otimes_{R_U} R_p$, y que hay un $c' \in G(B_U \otimes_{R_U}^{n+1})$ cuya imagen en $G(B^{\otimes_{R_p}^{n+1}})$ es c. Entonces $\partial c' \in G(B_U^{\otimes_{R_U}^{n+1}})$ coincide con 0 (el elemento neutro de G) en el punto p, y por tanto hay un V entorno de p con $V \in U$ y $\partial c' = 0$. Así, la aplicación natural

$$\lim_{p \in U} \overset{v}{H}^n(\chi,R(U),G) \rightarrow \overset{v}{H}^n(\chi,R_p,G) \qquad (1.3.3)$$

es sobreyectiva. Un elemento del miembro izquierdo de 1.3.3. es de la forma $\overline{c} \in H^n(B/R(U),G)$; supongamos que su imagen es cero. Existe entonces $B' \in \chi(R_p)$ que extiende a $B \otimes R_p$ y tal que $c = \partial c'$, con $c' \in (B')^{\otimes_{R_p}^n}$. Podemos encontrar $V \subset U$ entorno de p y $B'' \in \chi(R(V))$ extensión de $B \otimes_{R(U)} R(V)$ tal que $B'' \otimes_{R(V)} R_p = B'$ y c,c' estén definidos en V. Dado que $c - \partial c'$ coincide con 0 en p, podemos tomar ahora un $W \subset V$ sobre el cual c coincida con $\partial c'$, y entonces $\overline{c} = 0 \in H^n(Y,R(W),G)$ ∎

Proposición 1.4.

Sea χ el funtor definido en 1.3.v), G un funtor de anillos en grupos abelianos tal que para todo anillo S, el prehaz definido por G sobre $\mathrm{Spec}S$ es un haz y G preserva productos finitos.

i) $\chi(A) = \lim_{E(\chi)} \chi(R_Z)$

ii) Sea $n \geq 1$, el funtor $F = \overset{v}{H}^n(\chi,\cdot,G)$ satisface las hipótesis de la proposición 1.1.

Demostración.

La parte ii) fue probada en la demostración de la parte v) del teorema anterior Veamos entonces la parte i). Sea $B \in \chi(A)$; como vimos en 1.3.i) B es un A-módulo libre. Por tanto podemos mirar a B como el A-módulo A^n, (n = rkB) con una multiplicación conmutativa y asociativa

$$A^n \otimes_A A^n \xrightarrow{\mu} A^n$$

y dos elementos distinguidos, $1\!\!1 = (X_1,\ldots,X_n) \in A^n$ y $e = (Y_{ij})_{1\leq i,j\leq n} \in$

$\in A^{n^2} \cong A^n \otimes A^n$ que satisfacen:

$$(1.4.1.) \quad \begin{cases} \mu(\alpha \otimes 1\!\!1) = \mu(1\!\!1 \otimes \alpha) = \alpha \quad \forall\, \alpha \in A^n \\ e^2 = e,\ \mu(e) = 1\!\!1 \quad (\alpha \otimes 1\!\!1)e = (1\!\!1 \otimes \alpha)\, e \quad \forall\, \alpha \in A^n \ . \end{cases}$$

Sea $(V_i)_{1\leq i\leq n}$ la base canónica de A^n, y pongamos $b_{ij} = \mu(V_i \otimes V_j) \in A^n$, $1 \leq i,j \leq n$. Podemos tomar $Z \in C(X)$ donde 1,e y $(b_{ij})_{1\leq i,j\leq n}$ estén definidos. En virtud de la inyectividad del morfismo canónico $R_Z \to A$(1.3(i)) las propiedades (1.4.1.) se verifican en R_Z, para la definición evidente de R_Z. Resulta así un $B' \in \chi(R_Z)$ con $B = B' \otimes_{R_Z} A$. Si ahora $f:B \to C$ es un morfismo en $\chi(A)$, con las identificaciones anteriores, si M es la matriz de f en la base canónica (m = rkC) se tiene el diagrama conmutativo (μ' es la multiplicación de C):

$$\begin{array}{ccc} A^n \otimes A^n & \xrightarrow{M \otimes M} & A^m \otimes A^m \\ \downarrow \mu & & \downarrow \mu' \\ A^m & \xrightarrow{M} & A^m \end{array}$$

Como antes, podemos encontrar $Z \in C(X)$ con M, B' y C' definidos sobre Z, y la conmutatividad (1.1.i) se verifica por la inyectividad del morfismo $R_Z \to A$. *Hemos probado que el morfismo canónico*

13. \

$$\lim_{E(X)} \quad \chi(R_Z) \quad \rightarrow \quad \chi(A)$$

es sobreyectivo. La demostración de la inyectividad es completamente análoga. ■

§2. CLASES CARACTERISTICAS.

Del teorema 1.3. se deduce una sucesión exacta:

$$0 \to I \to \mathbb{Z} \to UA/U^2A \to L_{cte}(A) \to 0$$

donde

$\mathbb{Z}[UA/U^2A]$ es el anillo de grupo

$L_{cte}(A)$ es el grupo de Grothendieck de la categoría de módulos cuadráticos de rango constante sobre A.

I es el ideal generado -como grupo- por los elementos de la forma $\bar{a} + \bar{b} - \bar{c} - \bar{d}$ con $\langle a,b\rangle \cong \langle c,d\rangle$.

Observemos además que $UA/U^2A \cong \overset{v}{H}{}^1(\chi,A,\mu_2)$.

Estas propiedades nos van a permitir dar una teoría de clases características para R-módulos cuadráticos con valores en la cohomología $\overset{v}{H}{}^n(\chi,A,\mu_2)$. Sólo necesitamos el siguiente

Teorema 2.1.

Sean S un anillo conmutativo con unidad y $2 \in US$; (P,q) un S-módulo cuadrático de rango n, junto con una descomposición ortogonal

$$(P,q) = \perp_{1\leq i\leq n} (P_i,q_i) \qquad rk(P_i,q_i) = 1 \ (1 \leq i \leq n).$$

Sea, para cada i, c_i la clase de (P_i,q_i) en $\overset{v}{H}{}^1(\chi,S,\mu_2)$. Entonces:

i) La suma $\sum_{i=1}^{n} c_i \in \overset{v}{H}{}^1(\chi,S,\mu_2)$ coincide con la imagen de $\det(P,q) = (\Lambda^n P, \Lambda^n q)$, el determinante de (P,q). (Λ^n es la forma cuadrática asociada a $\Lambda^n \varphi_q$, donde $\varphi_q : P \to P^*$ es el isomorfismo asociado a q).

iii) $\quad (\overline{P,q}) \in \mathrm{Ker}(\check{H}^1(X,S,\mu_2) \to \check{H}^1(X,B,\mu_2)) = \check{H}^1(B/S,\mu_2)$.

Más aún, $(\overline{P,q})$ coincide, a través de la identificación ii) con la clase del 1-cociclo

$$f: \mathbb{Z}/2\mathbb{Z} \to \mu_2 B$$
$$f(1) = -1 \quad f(0) = 1$$

Demostración:

B es evidentemente un módulo proyectivo, y es localmente de la forma $S_p[x]/(x^2-a)$ con $P \in \mathrm{Spec}S$ y $a \in US_p$. Por tanto B es separable y localmente de Galois con generador σ_p definido por la fórmula $\sigma_p(\bar{x}) = -\bar{x}$. Podemos tomar un cubrimiento finito por abiertos afines conexos -en virtud de la hipótesis sobre S- tales que denotando por B_i y S_i las respectivas restricciones a U_i $(i \in I)$ se tiene

$$(2.2.1) \quad B_i \cong \frac{S_i[x]}{\langle x^2-a_i \rangle} \qquad (a_i \in US_i)$$

Se ve entonces que

$\sigma_i : B_i \to B_i$ es el único automorfismo

$\bar{x} \xrightarrow{\sigma_i} -\bar{x}$ de B_i/S_i distinto de la identidad

En efecto, $\sigma_i(\bar{x})$ debe ser de la forma $s+t\bar{x}$ con $t \neq 0$; si $P \in U_i$, resulta entonces que $\sigma_{i,p}(\bar{x}) = -\bar{x}$, luego $t = -1$ y $s = 0$. Si ahora $P \in U_j \cap U_i$, $\sigma_{j,p} \equiv \sigma_{i,p}$ por tanto $\sigma_i \mid U_i \cap U_j \equiv \sigma_j \mid U_i \cap U_j$ es decir que la I-upla $\{\sigma_i\}_{i\in I}$ determina un único automorfismo de B/S, σ digamos. Es claro entonces

que $\sigma^2 = 1$ y además $B^\sigma = S$. En efecto, si $\pi B \to P$ es el proyector de núcleo S y $b \in B$, la igualdad $\tau b = b$ implica que πb es localmente nulo, y por ende lo es globalmente, es decir que $b \in S$. Hemos probado así la parte i). Veamos ahora ii).

En su trabajo [A] Amitsur da un isomorfismo entre los complejos de cocadenas respectivos. Se observa que el punto crucial consiste en probar la siguiente propiedad:

Sea $e \in B \otimes B$ el idempotente de separabilidad de B,

$$e_\sigma = (\sigma \otimes 1)\ e \quad , \qquad e_1 = e$$

entonces

$$1 = e_1 + e_\sigma$$

En nuestro caso tal propiedad se satisface en cada localización de S, y por construcción ello implica que se satisface globalmente. En cuanto a iii) la primera afirmación es fácil de ver ([MV-III]) ; se obtiene un isomorfismo

$$\theta : (P,q) \otimes B \to (B,1)$$

donde el miembro de la derecha es la forma cuadrática trivial de rango 1 sobre B, la imagen de (P,q) en $\check{H}^1(B/S,U_2)$ es la clase de cociclo $(\varepsilon_1\theta \cdot \varepsilon_0\theta^{-1})(1\otimes 1) = t \in \mu_2\ B \otimes B$. Ahora bien, en virtud de lo anterior

$$t = te_1 + te_\sigma$$

En cada $P \in \mathrm{Spec}S$ $B \cong S\ [\sqrt{a_p}]$ según vimos más arriba; con esa identificación se tiene

$$t_p = \sqrt{a_p} \otimes 1/\sqrt{a_p}$$

$$e_{1,p} = \frac{1 + t_p}{2}$$

$$e_{\sigma,p} = \frac{1 - t_p}{2}$$

Por tanto resulta que $t = e_1 - e_\sigma$ y, siguiendo [A] se obtiene el cociclo pedido. ■

Demostración de 2.1.ii): Sean B_1 y B_2 las S-álgebras del lema anterior para $(P,q) = (P_i,q_i)$ $i = 1,2$ respectivamente.
Se tiene entonces que $B = B_1 \otimes_S B_2$ es de Galois con grupo $G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ [DeMe-In]
Con el lema anterior obtenemos dos cociclos:

$$f_i: G \to \mu_2 B \qquad i = 1,2$$

$$f_1(\alpha,\beta) = \begin{cases} -1 & \text{si } \alpha = 1 \\ 1 & \text{en otro caso} \end{cases}$$

$$f_2(\alpha,\beta) = \begin{cases} -1 & \text{si } \beta = 1 \\ 1 & \text{en otro caso} \end{cases}$$

Sea ahora

$$f: G \times G \to \mu_2 B$$

$$f(\alpha_1,\beta_1,\alpha_2,\beta_2) = \begin{cases} -1 & \text{sii } \alpha_1 = \beta_2 = 1 . \\ 1 & \text{en otro caso.} \end{cases}$$

Es claro que la clase de f en $H^2(B/S,\mu_2)$ coincide con el producto cup $c_1 \cup c_2$.
La imagen de f en $Br(B/S)$ es el B-módulo libre A con generadores $\{u_\alpha : \alpha \in G\}$ y multiplicación definida por

$$(bu_\alpha)(cu_\beta) = b\ \alpha\ (c)\ u_{\alpha\beta} \qquad \alpha,\beta \in G .$$

Para ver que A es el álgebra de Clifford de (P,q) necesitamos un S-morfismo $\theta: P \to A$ con $\theta(p)^2 = q(p)$. Un tal θ se define identificando P con el S-sub-módulo

$$P_1 \otimes (0,1) \oplus P_2 \otimes (1,0)$$

La universalidad se deduce inmediatamente. ∎

Corolario 2.3.: El anillo $A = A(R)$ satisface i) y ii) del teorema anterior.
Demostración:
Solo es necesario probar ii). Por 1.3. se tiene que (P,q), (P_1,q_1) y (P_2,q_2) se pueden mirar sobre algún R_Z. Dado que $\mathrm{Spec}R_Z$ es localmente conexo, ii) se satisface para R_Z; el resultado se sigue ahora por naturalidad de los morfismos en ii). ∎

Definición 2.4.
Sea (P,q) un R-módulo cuadrático de rango n, $\{(P_i,q_i): i=1,\ldots,n\}$ una descomposición ortogonal de $(P,q) \otimes A$ es decir

$$(P,q) \otimes A = \overset{n}{\underset{i=1}{\perp}} (P_i,q_i) \qquad \mathrm{rk}(P_i,q_i) = 1.$$

Sea $AC(A)$ el anillo de cohomología del haz μ_2 sobre la topología χ-definida en 0.1.-**La clase total de (P,q) es*

$$C(P,q) = \prod_{i=1}^{n} (1 + (\overline{P_i,q_i})) \in \widetilde{AC}(\chi,A,\mu_2) = U(AC(\chi,A,\mu_2))$$

Análogamente la clase i-ésima de (P,q) es la coordenada $c_i(P,q)$ de $c(P,q)$ en $\overset{v}{H}^i(\chi,A,\mu_2)$.

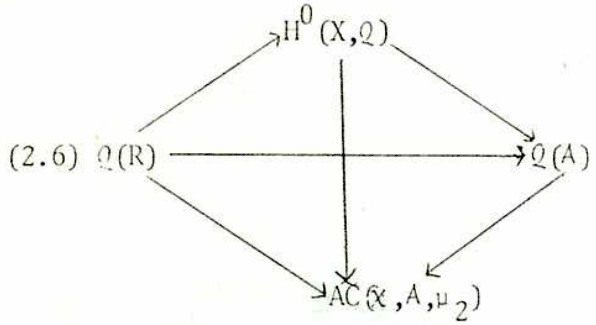
Observación 2.5.
Del teorema 1.3. y la definición anterior se tiene un diagrama conmutativo

---

* : 1 denota el elemento neutro para el producto " "

**: Cohomología de $\overset{v}{\text{Cech}}$

(2.6)



Observemos además que la aplicación c en 2.4. verifica

i) Si $rk(P,q) = n$, $c_i(P,q) = 0 \quad \forall \; i > n$.

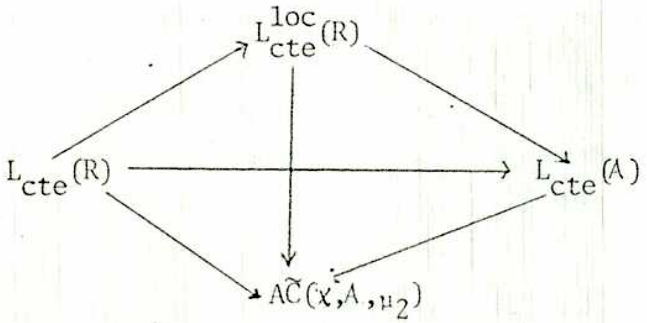
ii) $c_0(P,q) = -1 \in \mu_2 A$

iii) Si (P,q) se descompone como suma ortogonal $(P,q) = (P_1,q_1) \perp (P_2,q_2)$ se tiene

$$c(P,q) = c(P_1,q_1) \cup c(P_2,Q_2) \; .$$

Llamando $L^{loc}_{cte}(R)$ al grupo de Grothendieck asociado al monoide $H^0(X,Q)$, el diagrama 2.6. nos da, en virtud de iii) un diagrama conmutativo

(2.6.')



Observación 2.6.

Dado un módulo cuadrático (P,q) con $rk(P,q) = n$, podemos encontrar $Z \in C(X)$ tal que $(P,q) \otimes_R R_Z$ tenga una base ortogonal. $c(P,q)$ queda entonces definido

en $\widetilde{AC}(\chi, R_Z, \mu_2)$. Otra descomposición ortogonal sobre R_Z nos dará un $c' \in \widetilde{AC}(\chi, R_Z, \mu_2)$; c y c' van a coincidir en un $V \gg Z$ que es en particular un cubrimiento de $X_Z = \mathrm{Spec} R_Z$. Resulta entonces que para cada $m\ i \geq 0$, c_i y c'_i dan el mismo elemento en $H^0(X_Z, \overset{\vee}{H}{}^i(\chi, R_Z, \mu_2))$. Se tiene entonces que, en principio, para cada (P,q), las clases características están bien definidas en $\prod_{n\geq 0} H^0(X, \overset{\vee}{H}{}^n(\chi, R_Z, \mu_2))$ para un Z que depende de (P,q), pero que no está completamente determinado por aquél. Sin embargo, con el mismo razonamiento vemos que si (P,q) admite una descomposición como suma ortogonal de R-módulos cuadráticos de rango 1, $c(P,q)$ está bien definido en $\prod_{n\geq 0} H^0(X, \overset{\vee}{H}{}^n(\chi, R, \mu_2))$.

Observación 2.7.

Las clases características que acabamos de definir verifican la versión cuadrática natural de los axiomas de Grothendieck ([G], 3.1.). En efecto, los axiomas ii) y iii) son consecuencia directa de la definición, i) es inmediata a partir de la obvia funtorialidad de la construcción $R \to AR$.

Observación 2.8.

Del diagrama 2.6.', se sigue que las clases características no distinguen entre formas localmente isomorfas. En particular, si (P,q) es una forma de rango n localmente trivial, i.e. localmente isomorfa a la forma trivial de rango n, resulta $c(P,q) = 1$. Interesa entonces estudiar el tipo de anillos S tales que existe un S-módulo cuadrático no trivial pero localmente trivial. Un ejemplo de tal situación es el siguiente:

Sea R un anillo sin idempotentes no triviales, $2 \in UR$ y $a \in UR$ tal que $\bar{1} \neq \bar{a} \in UR/U^2R$; y consideremos la R-álgebra

$$S = \frac{R[X,Y,Z]}{\langle ax^2 - y^2, a(x+1)^2 - z^2 \rangle}$$

Es evidente que a es localmente un cuadrado en S: es decir que la forma de rango 1 definida por la fórmula $q(s) = as^2 (s \in S)$ es lo[illegible]nte trivial. Veamos que q

no es trivial; i.e. a no es un cuadrado. En efecto, sean $R' = R[\sqrt{a}]$, $S' = S \otimes R'$; si $s \in S$ es tal que $s^2 = a$, su imagen en S' será de la forma $\mu\sqrt{a}$, con $\mu \in \mu_2 S'$. Se afirma que $\mu_2(S') = \{1,-1\}$; es claro que de ser cierta la afirmación, no puede existir tal s; en efecto, el conjunto $\{1,\sqrt{a}\}$ S' es linealmente independiente sobre S.
Probemos entonces la afirmación. Observemos en primer lugar que el espectro de S' es de la forma: (*)

$$(2.9)\quad \mathrm{Spec}S' = (V(\sqrt{a}X-Y) \cup V(\sqrt{a}X+Y)) \cap (V(\sqrt{a}(X+1)-Z) \cap V(\sqrt{a}(X+1)+Z))$$

Como $2 \in U S'$, basta ver que $\mathrm{Ip}S' = \{0,1\}$; sea entonces $e \in \mathrm{Ip}S'$ y supongamos $e \neq 1$. Existe por tanto $P \in \mathrm{Spec}S'$ con $e \in P$. Por (2.9.) P contiene a alguno de los ideales

$$I_1 = \langle \sqrt{a}X-Y\ ,\ \sqrt{a}(X+1) - Z \rangle$$

$$I_2 = \langle \sqrt{a}X-Y\ ,\ \sqrt{a}(X+1) + Z \rangle$$

$$I_3 = \langle \sqrt{a}X+Y\ ,\ \sqrt{a}(X+1) - Z \rangle$$

$$I_4 = \langle \sqrt{a}X+Y\ ,\ \sqrt{a}(X+1) + Z \rangle$$

Sea $1 \leq j_0 \leq 4$ tal que $P \in I_j$; como $S'/I_{j_0} \cong R'[X]$, se sigue que I_{j_0} $e \in I_{j_0}$. Ahora, cada I_j representa una recta en $A_3(R')$; evaluando e en las intersecciones se sigue que $e \in \bigcap_{j=1} I_j$. Luego e es nilpotente e idempotente, por tanto $e = 0$.
Hemos probado la

Proposición 2.10.:
Sea R tal que $UR/U^2R \neq (1)$ y $\mathrm{Ip}R = \{0,1\}$. Existe un R-álgebra de tipo finito, S y un S-módulo cuadrático localmente trivial que no es trivial.

(*) Usamos la notación de Atiyah-MacDonald: Algebra Conmutativa.

Demostración: ver observación 2.8.

§3. Fibrado bandera cuadrático y clases características.

3.1. Sea (P,q) un R-módulo cuadrático de rango n, $S(P)$ el álgebra simétrica asociada a P, Φ la forma bilineal asociada a q y $\varphi P \to P^*$ el isomorfismo definido por Φ. Consideremos la cadena de isomorfismos

$$\mathrm{Hom}(P \otimes P, R) \cdot \quad P^\vee \otimes P^\vee \overset{\varphi^{-1} \otimes \varphi^{-1}}{\cong} P \otimes P .$$

Con $P^\vee = \mathrm{Hom}(P,R)$, el dual de P.

Φ define un morfismo $\overline{\Phi}: P \otimes P \to R$ y a través de las identificaciones precedentes define también un elemento en $P \otimes P$, pasando al cociente obtenemos un elemento $Q \in S_2(P)$. Observemos que, localmente, Q es el polinomio homogéneo definido por q. En efecto, si P es libre con base $B = \{V_i : 1 \leq i \leq n\}$ y ponemos $M = (A_{ij})_{1 \leq i,j \leq n}$ la matriz de Φ y $B^* = \{\gamma_i : 1 \leq 1 \leq n\}$ la base dual, entonces la imagen de Φ en $P^* \otimes P^*$ será $\sum_{1 \leq i,j \leq n} a_{ij}\ \gamma_i \otimes \gamma_j$. Sea $B' =$

$= \gamma^{-1}(B^*)$, y escribamos $B' = \{X_i : i \in I\}$. Entonces $Q = \sum_{1 \leq i,j \leq n} a_{ij} X_i X_j \in S_2(P) \subset S(P)$

donde identificamos $S(P)$ con el anillo de polinomios $R[X_1,\ldots,X_n]$ mediante la base B'.

Consideremos ahora el esquema $Z = \mathrm{Proj}(S(P))$ y dentro de éste el abierto afín $D(Q) = \{P \in \mathrm{Proj}(S(P)) : P \not\in Q\}$. Si O_Z es el haz estructural sobre Z, sea $S(P,q) = \Gamma(D(Q), O_Z)$.

Proposición 3.2.

Sea (P,q) un R-módulo cuadrático de rango n $S=S(P,q)$ la R-álgebra definida en 1.1. Se tiene una descomposición ortogonal

$$(P,q) \otimes S = (L_1, q_1) \perp (P',q')$$

donde $\operatorname{rk} L_1 = 1$.

Demostración:

Con las notaciones de 1.1., si $f:Z \to X$ es la proyección natural hay un epimorfismo

$$f^*(P) \twoheadrightarrow \mathcal{O}_Z(1)$$

Restringiendo a $D(Q)$ y tomando duales se tiene un monomorfismo

$$\mathcal{O}(-1)\Big|_{D(Q)} \xrightarrow{i} f^*(P^\vee)\Big|_{D(Q)} = P^\vee \otimes S .$$

Sea L_1 la imagen de la composición $\varphi^{-1} \circ i$; entonces $\operatorname{rk}(L_1) = 1$. Basta entonces verificar que $q_1 = q \otimes S\Big|_{L_1}$ es una forma cuadrática regular. Dado el carácter local de esa propiedad, podemos suponer que P es libre; sea $B = \{e_i : 1 \leq i \leq n\}$ una base de P, B^* y B' como en 1.1., e identifiquemos $S(P) \cong R[X_1,\ldots,X_n]$ mediante la base B'. Entonces S se identifica con la R-álgebra $(R[X_1,\ldots,X_n]_Q)_0$, donde el subíndice "0" indica la parte de grado 0 en la graduación natural de $R[X_1,\ldots,X_n]_Q$, i.e. todo elemento de S es una fracción $\frac{f}{Q^n}$ con $\deg f = 2n$. En $Y = D(Q) = \operatorname{Spec}$ consideramos el cubrimiento

$\{Y_i = D(Q) \cap D(X_i) : i=1,\ldots,n\}$; tenemos que $S_i = \Gamma(Y_i,O_Y) = R\left[\frac{X_1}{X_i},\ldots,\frac{X_n}{X_i}\right]_{Q_i}$ donde

Q_i es la deshomogeneización de Q en X_i . Supongamos, sin pérdida de generalidad, $i = 1$; resulta $Q_1 = Q(1,\frac{X_2}{X_1},\ldots,\frac{X_n}{X_1})$. Ahora $q \otimes S_1(V) = Q_1$, que es inversible en S_1 , y por tanto q_1 es regular, como queríamos.

Observación 3.3.

Aplicando iteradamente el procedimiento de 1.1. se obtiene, en el paso n-1, una R-álgebra T y una descomposición ortogonal

$$(P,q) \otimes T = \perp_{i=1}^{n} (L_i,q_i)$$

donde cada (L_i,q_i) es un T-módulo cuadrático de rango 1 .

Proposición 3.4.:

Sea S como en 1.1. se tiene:

i) S es una R-álgebra fielmente playa; si además R es noetheriano, $Y = \mathrm{Spec}S$ es localmente conexo.

Si ahora R es noetheriano se tiene además

ii) La aplicación natural $\overset{\vee}{H}^n(X,AR,\mu_2) \to \overset{\vee}{H}^n(X,AS,\mu_2)$ es inyectiva para todo $n \geq 1$.

iii) El diagrama:

$$\begin{array}{ccc} H^0(X,\overset{\vee}{H}^n(X,R,\mu_2)) & \to & \overset{\vee}{H}^n(X,AR,\mu_2) \\ \downarrow & & \downarrow \\ H^0(Y,\overset{\vee}{H}^n(X,S,\mu_2)) & \to & \overset{\vee}{H}^n(X,AS,\mu_2) \end{array}$$

es cartesiano.

Demostración:

i) Basta verificarlo localmente; sea S_i como en 3.2., S_i es una localización de un anillo de polinomios sobre R, luego es playo. Ahora tomemos por ejemplo $i=1$, y sea $P \in \mathrm{Spec}R$; $\overline{P}$ su extensión en $R[\frac{X_2}{X_1},\ldots,\frac{X_n}{X_1}]$. Es claro que $\overline{P}$ es un ideal primo, afirmo que $Q_1 \notin \overline{P}$. Si tal afirmación es cierta, resulta que la contracción de $\overline{\overline{P}} = \overline{P}\,S_1$ en $R[\frac{X_2}{X_1},\ldots,\frac{X_n}{X_1}]$ es $\overline{P}$ y por tanto la contracción de $\overline{\overline{P}}$ en R coincide con P, lo que prueba que S_1 es fielmente playo sobre R. Análogamente se ve que S_i es fielmente playo para cada i y concluímos que S lo es.

Probemos entonces la afirmación. Dado que q es regular, $\det q \in UR$, pero según vimos en 3.1. Q tiene la forma $\sum_{1\leq i,j\leq n} a_{ij} X_i X_j$ donde $(a_{ij})_{1\leq i,j\leq n}$ es la matriz de q en una base. Se concluye que el ideal generado por los coeficientes de Q_1 contiene una unidad, luego $Q_1 \notin \overline{P}$ para ningún $P \in \mathrm{Spec}R$. Si además R es noetheriano, es claro que S lo es y por tanto Y es localmente conexo.

ii) Sea $Z \in C(X)$, $Z = \{U_i : i \in I\}$; notaremos por R_i el anillo de secciones del haz estructural sobre U_i, i.e. $R_i = \Gamma(U_i, O_X)$. Podemos suponer, sin pérdida de generalidad que U es diagonalizante, es decir que $(P,q) \otimes R_i$ tiene una base ortogonal $(\forall\, i \in I)$, y fijemos una elección de tales bases para cada $i \in I$. Sea Z^* el cubrimiento de $Y = \mathrm{Spec}S$ obtenido por imagen inversa de Z. Si $c \in \check{H}^n(\mathcal{X}, R_Z, \mu_2) = \check{H}^n(\mathcal{X}, R_Z, \mu_2)$ (cf.1.3.2.) va a cero en $\check{H}^n(X, AS, \mu_2)$, existe $V \gg Z^*$ $V \in C(Y)$ tal que c pertenece al núcleo de la composición:

$$\check{H}^n(\mathcal{X}, R_Z, \mu_2) \rightarrow \check{H}^n(X, S_{Z^*}, \mu_2) \rightarrow \check{H}^n(X, S_V, \mu_2)$$

Por otro lado, dado que hemos fijado una descomposición ortogonal de $(P,q) \otimes R_i$,

tenemos una identificación $\Gamma(Y,\mathcal{O}_Y) = (R_i[X_1,\dots,X_n]_{Q_i})_0 = S(R_i)$ (c.f. 3.1.). 3.1.

Si $\overline{Z}_i = \{\mathrm{Spec}S(R_i)_j : j = 1,\dots,n\}$ (con la notación de 3.1.) se tiene que 3.1.
$\overline{Z} = \Sigma\, \overline{Z}_i$ es un cubrimiento de $Y_{\overline{Z}}$; podemos suponer entonces que $\mathcal{V} \gg \overline{Z}$. Por tanto $S_{\mathcal{V}}$ es de la forma

$$S_{\mathcal{V}} = \prod_{i\in I} \prod_{1\leq j\leq n} \prod_{k\in K_j} (S(R_i)_j)\left[\frac{1}{f_k}\right] \qquad (3.5.)$$

con $f_k \in R_i[\frac{X_1}{X_j},\dots,\frac{X_n}{X_j}]$. Si $q_i(X_1,\dots,X_n) = \sum_{j=1}^{n} a_j x_j^2$, tenemos que

$(S(R_i)_j)[\frac{1}{f_k}]$ es un álgebra aumentada sobre $R_i[\frac{1}{a_j}, \frac{1}{f_k(0)}] = R_i[\frac{1}{f_k(0)}]$.
Luego c va a cero sobre cada $R_i[\frac{1}{f_k(0)}]$ $k \in K_j$ $1 \leq j \leq n$. Obtenemos así,
para cada i, un cubrimiento de U_i sobre el cual c es cero; por tanto c va a cero en $\check{H}^n(\mathcal{X},A,\mu_2)$. En virtud de (3.1.) lo anterior concluye la demostración de ii).

iii) Sean Z y Z^* como arriba, $c \in \check{H}^n(\mathcal{X},R_Z,\mu_2) = \check{H}^n(\mathcal{X},R_Z,\mu_2) \subset \prod_{i\in I} \check{H}^n(\mathcal{X},R_i,\mu_2)$
tal que existe $\mathcal{V} \gg Z^*$ con $c \in H^0(\mathcal{V},\check{H}^n(\mathcal{X},\cdot,\mu_2))$, es decir, si $\mathcal{V} = \{V_\ell, \ell \in L\}$
c pertenece al núcleo del morfismo de borde

$$\prod_{\ell\in L} \check{H}^n(\mathcal{X},V_\ell,\mu_2) \xrightarrow{\partial} \prod_{V_\ell\cap V_p\neq\emptyset} \check{H}^n(\mathcal{X},V_\ell\cap V_p,\mu_2)$$

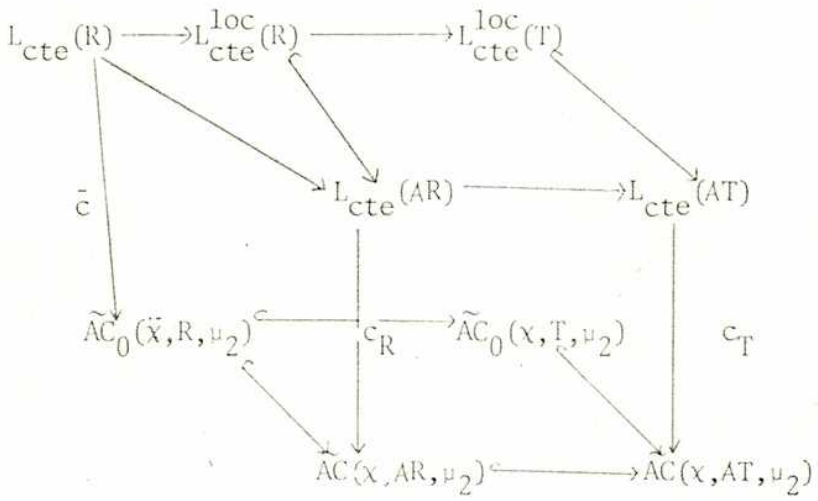
Como antes, podemos suponer que $\mathcal{V} \gg \overline{Z}$. En virtud de (3.5.) se tiene que
$Z \ll \mathcal{V}_* = \{\mathrm{Spec}\, R_i[\frac{1}{f_{k(0)}}]$; $i\in I$ $1\leq j\leq n$, $k \in K_j\}$ y $c \in H^0(\mathcal{V},\check{H}^n(\mathcal{X},\cdot,\mu_2))$ lo
que completa la demostración

Uniendo los resultados de la sección anterior con los de la proposición 2.4., se obtiene el

3.5. Teorema:

Sea R noetheriano, $2 \in UR$, S y A las R-álgebras definidas respectivamente en 1.0., c la aplicación natural en 3.1.

Se tiene un diagrama conmutativo



Donde $\bar{c}$ viene dada por 3.4. iii).

Demostración:

Es inmediata a partir de 2.4., 1.3. y 3.4. ■

En virtud de este teorema podemos dar una nueva definición de clases características.

3.6. Definición 2.4.'

La clase característica total de un elemento de $L_{cte}(R)$ es su imagen por $\bar{c}$ en

$\widetilde{AC}_0(\chi,R,\mu_2) = \prod_{n\geq 0} H^0(\chi,H^n(\chi,R,\mu_2))$. La <u>i-ésima clase característica</u> es la coordenada i-ésima de la clase total.

<u>Observación 3.7.</u>

Como vimos en 2.8., la aplicación natural $Q(R) \to L^{loc}_{cte}(R)$ no es inyectiva, y por tanto $\bar{c}$ no distingue entre formas cuadráticas localmente isomorfas. Sin embargo, dado $(P,q) \in Q(R)$ si $T = T(P,q)$ podemos asociar a (P,q) un elemento $d(P,q)$ en $\widetilde{AC}(\chi,T,\mu_2)$ por la flecha natural. En virtud de la conmutatividad del diagrama

$$\begin{array}{ccc} \widetilde{AC}(\chi,R,\mu_2) & \longrightarrow & \widetilde{AC}_0(\chi,R,\mu_2) \\ \downarrow & & \downarrow \\ \widetilde{AC}(\chi,T,\mu_2) & \longrightarrow & \widetilde{AC}_0(\chi,T,\mu_2) \end{array}$$

Tenemos que $d(P,q) \in \widetilde{AC}(\chi,T,\mu_2)$ se aplica sobre $\bar{c}(P,q)$ en $\widetilde{AC}_0(\chi,T,\mu_2)$; es decir que, en algún sentido, $d(P,q)$ es más fino que $c(P,q)$. Es posible que este hecho permita definir una teoría de invariantes más fina que la antes expuesta. Quizás sea necesaria una construcción similar a la de AR, reemplazando la topología de SpecR por la topología de Grothendieck generada por las álgebras del tipo $S(P,q)$ para $(P,q) \in Q(R)$.

<u>Observación 3.8.</u>

Si $2 \notin UR$ la construcción de $S(P,q)$ puede hacerse cambiando el espacio proyectivo por la Grassmaniana $G_2(P,q)$. Por otro lado las propiedades de $A(R)$ siguen valiendo en ese caso, reemplazando μ_2 por I_p. Vemos así que el problema de definir clases características se reduce al caso en que R es local.

APENDICE: CASO ORDENADO

En la presente sección se utilizan las definiciones y resultados básicos del trabajo de Marshall y Walters [M-W].

Proposición:
Sea R conmutativo, con unidad, $Z \in UR$, y $X=\mathrm{Spec}R$ localmente conexo (1). Sean (P,q) un R-módulo cuadrático, $\mathrm{rk}P = n$, $A = AR$(§1) y $S = S(P,q)$ (§2), k un número entero positivo par. Se verifican

i) A tiene muchas unidades.

ii) Si R admite un preorden de nivel k, A admite un preorden de nivel k. Más aún, si F_k es el funtor que asigna a cada anillo su espacio de órdenes de nivel k, se tiene $F_k(A) = \varprojlim_{U \in C(X)} F_k(R_U)$.

iii) Si R admite un preorden de nivel k, S admite un preorden de nivel k.

Demostración:
Sea f un polinomio en $A[X_1,\ldots,X_n]$, y para todo primo $P \in M = \mathrm{Spec}A$, $x_p \in A^n$ tal que $a_p f(x_p) \notin P$. El conjunto $\theta = \{a_p : P \in M_p\}$ genera entonces el ideal (1); luego existen $a_{p_i} \in \theta$, $b_{p_i} \in A$ $1 \leq i \leq r$ con $1 = \Sigma a_{p_i} . b_{p_i}$. Sea $U \in C(X)$ tal que $f \in R_U[X_1,\ldots,X_n]$, $x_{p_i} \in R_U^n$, $a_{p_i}, b_{p_i} \in R_U$. Como los a_{p_i} generan el ideal (1), se tiene que $\bigcup \{X_{U a_{p_i}} : 1 \leq i \leq r\}$ es un cubrimiento de $X_U =$

---

(1) La hipótesis de conexidad local no es necesaria para iii).

= Spec $R_{\mathcal{U}}$. Sea $\mathcal{V}' \in C(X)$, $\mathcal{V}' \gg \mathcal{V}$, entonces $\mathcal{V}' \gg \mathcal{U}$ y a_{p_i} es inversible en $R_{\mathcal{V}'}$ $(\forall i)$, lo que concluye la demostración.

ii) En virtud de [M-W] (1.1.) la primera parte consiste en probar que si $-1 \notin \Sigma R^k \Rightarrow -1 \notin \Sigma A^k$. En efecto si $a_1,\ldots,a_r \in A$ son tales que

$-1 = \sum_{i=1}^{r} a_i$, podemos tomar $\mathcal{U} \in C(X)$ con $a_i \in R_{\mathcal{U}}$. En particular,

$-1 \in \sum_{i=1}^{r} R_p^k \quad \forall\, p \in X$, luego $-1 \in \sum_{i=1}^{r} (R/P)^k \quad \forall\, p \in X$. Entonces el preorden

$T = \Sigma R^k$ no admite ningún primo compatible, lo que es absurdo en virtud de [M-W] th.1.6.

Veamos ahora la segunda parte de la afirmación. En virtud de la funtorialidad de F_k([M-W] (1.9.)iii)), se tiene una aplicación $F_k(A) \to \varprojlim_{\mathcal{U} \in C(X)} F_k(R_{\mathcal{U}}) = \Pi$. Recíprocamente, un elemento $T \in \Pi$ es un par $(\overline{T},\overline{P})$ donde $\overline{P}$ es una sucesión coherente de primos $\overline{P} = \{P_{\mathcal{U}}\}_{\mathcal{U} \in C(X)}$ con $P_{\mathcal{U}} \in X_{\mathcal{U}}$ y $\overline{T} = \{T_{\mathcal{U}}\}_{\mathcal{U} \in C(X)}$ es una sucesión coherente con $\overline{T}_{\mathcal{U}}$ orden en el cuerpo de fracciones del dominio $R_{\mathcal{U}}/P_{\mathcal{U}}$. Por tanto $\overline{P}$ determina unívocamente un elemento de Spec $A = \varprojlim_{\mathcal{U} \in C(X)} X_{\mathcal{U}}$. Si denotamos por K y $K_{\mathcal{U}}$ a los respectivos cuerpos de fracciones de $A/\overline{P}$ y $R_{\mathcal{U}}/P_{\mathcal{U}}$ se tiene que $\overline{T}$ determina unívocamente un orden en $K = \varprojlim_{\mathcal{U} \in C(X)} K_{\mathcal{U}}$.

iii) Sea $\mathcal{U}$ un cubrimiento de X, $\mathcal{U} = \{U_i : i \in I\}$ tal que $(\forall i \in I)$ (P,q) admite una base ortogonal sobre U_i. Si $Y = \mathrm{Spec} S$ sea $\overline{U}_i$ la preimagen de U_i en Y, $(i \in I)$ entonces $S^{(i)} = \Gamma(U_i, O_Y) \cong ((R[X_1,\ldots,X_n])_q)_0$.

Sea i fijo y supongamos $-1 = \sum_{l=1}^{r} \frac{f_l^k}{Q_l^{sk}} \quad S^{(i)}$; como Q no es divisor de cero en $R[X_1,\ldots,X_n]$, se obtiene una ecuación del tipo:

$$-Q^{sk} = \sum_{l=1}^{r} g_l^k \qquad R[X_1,\ldots,X_n] \ .$$

Ahora bien, $Q = \sum_{j=1}^{n} a_j X_j^2$; especializando $e_j = (0,\ldots,\overset{j}{1},0\ldots0)$ $1 \leq j \leq n$, se obtiene ecuaciones

$$R_i = \Gamma(U_i,O_X) \quad - (a_j^s)^k = \sum_{l=1}^{r} b_{jl}^k \qquad (1 \leq j \leq n).$$

Como $a_j \in UR_i$, se sigue que $-1 \in \Sigma R_i^k$. Usando ahora el principio local-global ([M-W](1.6)) y el hecho de que U es un cubrimiento de X, se llega a que $-1 \in \Sigma R^k$. ∎

Observación:

Los ítems i) y ii) de la proposición anterior sugieren la posibilidad de utilizar nuestros métodos para la teoría de signaturas de nivel k, lo mismo que la parte iii) en el caso $k = 2$.

BIBLIOGRAFIA

Am S.A. Amitsur. Simple Algebras and Cohomology Groups of Arbitrary Fields. TAMS 90 (1959) 73-112.

Ara J.Kr. Arason. Wittring und Galois Cohomologie bei Charakteristik 2, J. Reine und Angerwundte Math. 307-308 (1979) 247-256.

Art M. Artin. Grothendieck Topologies. Harvard U. Notes (1962).

Ba H. Bass. Lectures on Topics in Algebraic K-Theory. T.I.F.R., Bombay, 1972.

Bae R. Baeza: Quadratic forms over semilocal rings. L.N.M. 655, Springer, 1978.

C-H-R S.U. Chase, D.K. Harrison and A. Rosenberg. Galois Theory and Cohomology of commutative rings. Memoirs A.M.S. 52 (1965).

De A. Delzant. Définition des clases de Stiefel-Whitney d'une module quadratique sur un corps de caractéristique différente de 2. C.R. Acad. Sci. Paris 255 (1962), 1366-1368.

DeMe-In F.De Meyer y E. Ingraham. Separable Algebras over commutative rings. 1971. L.N.M. 181, Springer Verlag.

G A. Grothendieck. Theorie des Classes de Chern. Bull. Soc. Math. France 86, 1958, p. 137 a 154.

H E.Hornix, Stiefel-Whitney invariants of quadratic forms over local rings. J. of Algebra. 26 (1973), 258-279.

K K. Kato. Symmetric bilinear forms, quadratic forms and Milnor's K-theory in characteristic 2, Invent. Math. 66, 1982, 493-510.

Lab O. Laborde. Classes de Stiefel-Whitney en cohomologie étale. Colloque sur les formes quadratiques. (Montpellier-1975). Mem. Soc. Math. France 48 (1976) 47-51.

McL S. Mac Lane. Homology. Grindlehren der matematischen Wissenschaften, 114.1967

Ma A.R. Magid. The separable Galois theory of commutative rings. Dekker, NY, 1974.

M-W M. Marshall and L. Walter. Signatures of higher level on rings with many units. (Preliminary version). July, 1988. Preprint. Univ. of Satskatchewian, Canadá

M-R A. Micali, Ph. Revoy. Modules quadratiques. Bull. Soc. Math. France 63, (1979) 144 p.

M-V-1 A. Micali, O.E. Villamayor. Sur les Algebres de Clifford. Annales Scientifiques de l'Ecole Normale Supérieure. 4e. serie, t.1, fasc. 2, 1968.

M-V-2 A. Micali, O.E. Villamayor. Sur les Algebres de Clifford. Journal de Crelle 242 (1970), 61-90.

M-V-3 A. Micali, O.E. Villamayor. Algebres de Clifford et Groupe de Brauer. Ann. Sc. Ec. Normale Sup. 4 (1971), 285-310.

Mil J. Milnor. Algebraic K-theory and Quadratic Forms. Inventiones Math. 9 (1970) 318-344.

Se J.P. Serre. Applications algébriques de la cohomologie des Groupes II. Theorie des algébres simples. Exposé 7. Seminaire H. Cartan. 3e année 1950/51. E.N.S.

Sch W. Scharlau. Quadratischen Formen und Galois Cohomologie. Inventiones Math. 4 (1967), 161-171.

V O.E. Villamayor. Separable Algebras and Galois Extensions. Osaka J. Math. 4(1967), 161-171.

V-Z-1 O.E. Villamayor and D. Zelinsky. Galois Theory for Rings with finitely many idempotents. Nagoya Math. J. 27 (July, 1966).

V-Z-2 O.E. Villamayor and D. Zelinsky. Galois Theory with infinitely many idempotents. Nagoya Math. J. 35 (July, 1969).

V-Z-3 O.E. Villamayor and D. Zelinsky. Brauer Groups and Amitsur Cohomology for general commutative ring extensions. Journal of Pure and Applied Algebra. 10(1977) 19-55.