DERIVACIONES DE HASSE-SCHMIDT, CUERPOS DE COEFICIENTES Y EXTENSIÓN DE ESCALARES EN CARACTERÍSTICA POSITIVA.

Memoria presentada por M. Magdalena Fernández Lebrón
para optar al grado de Doctor en Matemáticas
por la Universidad de Sevilla.

V^o B^o del Director	El doctorando
Fdo. Luis Narváez Macarro Catedrático de Algebra	M. Magdalena Fernández Lebrón

Sevilla, Diciembre 2001

UNIVERSIDAD DE SEVILLA

FACULTAD DE MATEMÁTICAS
DEPARTAMENTO DE ÁLGEBRA

A Joaquín,

Joaquinito,

Pablo y Ana

Agradecimientos

Deseo expresar mi más sincero agradecimiento a todos los que, de alguna forma, me han ayudado a lo largo de estos últimos años, a la realización de esta memoria.

En primer lugar, doy las gracias a Luis Narváez Macarro, director de la misma, por su valiosa guía, por poner a mi disposición sus conocimientos en el Álgebra de característica positiva, por su paciencia ante los retrasos y por las horas dedicadas a ayudarme y corregir los errores de aquél que empieza en algo. Sin su ayuda, no hubiese sido posible la realización del presente trabajo.

Mi agradecimiento, también, es para el profesor J. M. Giral de la Universidad de Barcelona por su valiosa y eficaz ayuda cuando se le solicitó, por su interés en el tema y por su amabilidad al aceptar colaborar con nosotros.

Agradezco también a Joaquín y a mi compañero Jesús Gago, por sus valiosos comentarios tras la lectura de la misma.

Quiero agradecer a mis padres el esfuerzo y trabajo que siempre han estado dispuestos a realizar para que pudiese realizar mis estudios y el apoyo que siempre me han dado.

A mi marido, Joaquín, agradezco su apoyo en todo momento, su ánimo en los momentos difíciles y su comprensión. En especial, su dedicación en el cuidado de nuestros hijos durante tantas tardes, para que yo pudiera terminar la presente memoria y a ellos por ser la mejor forma de desconexión.

También agradecer a las dos abuelas, la de Cádiz y la de Sevilla, por estar siempre dispuestas a cuidar de sus nietos cuando todo se nos complicaba.

Por último, aunque no menos, a los compañeros del departamento por su ayuda de diversa índole, y tambien a los miembros del tribunal por haber aceptado formar parte del tribunal de esta tesis.

Introducción

Una de las diferencias más notables entre el Álgebra de característica positiva y el Álgebra de característica cero radica en el comportamiento respecto de los métodos, operaciones y estructuras diferenciales.

Por ejemplo, si k es un cuerpo de característica cero y $R = k[[x_1, \ldots, x_n]]$ es el anillo de las series formales (o convergentes en el caso en que k sea el cuerpo de los números reales o complejos), k coincide con el conjunto de las series que son anuladas por las derivadas parciales con respecto a cada una de las variables x_i, o más generalmente

$$k = \{a \in R \mid \partial_i(a) = 0, i = 1, \ldots, n\},$$

donde las ∂_i son unas k-derivaciones de R para las que existen unas series $a_j \in R$ con $\partial_i(a_j) = \delta_{ij}$. Esto se debe a que dichas ∂_i forman una base del R-módulo de todas las k-derivaciones de R (veáse el teorema IV–A.2). En particular, el cuerpo de las "constantes" aparece como las soluciones de un sistema de ecuaciones lineales en derivadas parciales particularmente sencillo. De hecho, el teorema de estructura de Cohen nos permite enunciar el resultado anterior para un anillo local completo regular de característica cero R y $k \subset R$ un cuerpo de coeficientes, con independencia de las coordenadas locales (corolario IV–A.5).

Los resultados anteriores han de entenderse como una versión parcial y puramente algebraica del Lema de Poincaré.

En el caso en que k sea un cuerpo de característica $p > 0$, el resultado anterior no es cierto, pues todas las series de la forma

$$a(x_1, \ldots, x_n) = b(x_1^p, \ldots, x_n^p),$$

con $b \in R$, son anuladas por las derivadas parciales respecto de las x_i. Para recuperar un resultado análogo al que se tiene en característica cero, es necesario recurrir a un sistema de ecuaciones diferenciales lineales de orden superior y de infinitas ecuaciones, cuyo tratamiento se simplifica notablemente con la noción de *derivación de Hasse-Schmidt* [HS37] (ver también [NaK70], [Mat86], [Tra00]).

En esta memoria nos ocupamos de estudiar las derivaciones de Hasse-Schmidt, de algunas de sus relaciones con los anillos de operadores diferenciales lineales, y de su uso en la determinación de cuerpos de coeficientes de anillos locales regulares completos de característica positiva.

Una de las motivaciones de esta memoria se encuentra en la extensión al caso de un cuerpo base de característica positiva de los resultados del trabajo [Nar91].

ANTECEDENTES

Los antecedentes inmediatos de este trabajo son los siguientes:

- Los aspectos algebraicos del desarrollo de Taylor en característica arbitraria [MV69] y su relación con los anillos de operadores diferenciales en el sentido de [GD67], §16, 16.8.
- La noción de derivación de Hasse-Schmidt [HS37].

- Los resultados de Nomura-Matsumura sobre los módulos de derivaciones de un anillo noetheriano local regular respecto de un cuerpo de casi-coeficientes [Mat80], th. 99.
- El artículo [Nar91].

RESULTADOS ORIGINALES CONTENIDOS EN LA MEMORIA

- La generalización de los resultados de [Nar91] al caso de un cuerpo base k perfecto de característica $p > 0$, exige reemplazar la extensión de escalares $A \to A \otimes_k k(t)$, donde A es una k-álgebra (por ejemplo, $A = k[[x_1, \dots, x_n]]$) y t es trascendente sobre k, por la extensión

  $$A \to A \otimes_k k(t)_{\text{per}},$$

  donde $k(t)_{\text{per}} = \bigcup_{m \geq 0} k(t^{\frac{1}{p^m}})$ es el cierre perfecto de $k(t)$. Un primer resultado de esta memoria es la conservación de la noetherianidad por la citada extensión. Obsérvese que, como $k(t)_{\text{per}}$ no es una extensión finitamente generada de k, la conservación de la noetherianidad no es clara en principio para k-álgebras A que no sean finitamente generadas. En esta memoria caracterizamos cuando el anillo $A_{(\infty)} := A \otimes_k k(t)_{\text{per}}$ es noetheriano (teorema III–C.6), y como consecuencia probamos que $A_{(\infty)}$ es noetheriano si A es el anillo de series formales en n indeterminadas sobre k (corolario III–C.8).
- En relación con el resultado anterior, también probamos que el mayor subcuerpo perfecto de un cuerpo de funciones formales sobre k, i.e. el cuerpo de fracciones de un cociente de $k[[x_1, \dots, x_n]]$ por un ideal primo, es una extensión finita del cuerpo de constantes k, que coincide con k cuando el cociente es normal (teorema III–B.8). La prueba de este resultado ha sido obtenida en colaboración con el profesor J. M. Giral.

- Generalizamos el teorema 99 de [Mat80] al caso de las derivaciones de Hasse-Schmidt y de un anillo noetheriano local regular equicaracterístico de característica $p > 0$ (ver teorema IV–A.10), y lo aplicamos para determinar cuerpos de coeficientes del anillo completado (corolario IV–A.11).

- Las derivaciones de Hasse-Schmidt de una k-álgebra A no poseen estructura de A-módulo, ni siquiera tienen una estructura aditiva. Poseen sin embargo, una estructura de grupo no abeliano, de carácter no lineal, que remonta la estructura aditiva (lineal) de las derivaciones usuales. En esta memoria demostramos que es posible "generar"cualquier derivación de Hasse-Schmidt, mediante expresiones explícitas no lineales, a partir de unas fijas con la condición de que sus componentes de grado 1 formen un sistema de generadores de las k-derivaciones de A (teorema IV–A.6).

- En el curso de la prueba de los resultados anteriores necesitamos una versión del lema de normalización para el anillo de series de potencias formales $A = k[[\underline{X}]]$, con k cuerpo perfecto de característica $p > 0$, válida para el caso en que k sea finito. Las pruebas que hemos encontrado en la literatura (cf. [Abh64], (24.5)), se restringen al caso en que k sea infinito, para poder así utilizar cambios lineales genéricos de coordenadas. En esta memoria adaptamos la prueba de loc. cit. al caso general, mediante cambios de coordenadas no lineales (teorema II–A.6).

- Por último, generalizamos el resultado principal (teorema 2.3) de [Nar91] al caso de un cuerpo base k perfecto de característica $p > 0$ y del anillo $R = k[[X_1, \ldots, X_n]]$. Concretamente, dado cualquier ideal maximal $\mathfrak{m}$ del anillo $R_{(\infty)}$, determinamos mediante las derivaciones de Hasse-Schmidt de R y de manera uniforme, un cuerpo de coeficientes del anillo $\widehat{(R_{(\infty)})_{\mathfrak{m}}}$ (teorema

V–A.1).

DESARROLLOS POSTERIORES

De manera muy esquemática señalamos algunas cuestiones surgidas a lo largo de este trabajo que consideramos interesantes de analizar en un futuro:

- Tal como señalamos en uno de los resultados originales de esta memoria expuestos anteriormente, si A es una k-álgebra (conmutativa), el conjunto $HS_k(A)$, de las k-derivaciones de Hasse-Schmidt de A, está dotado de una operación $\circ$ de grupo, no conmutativo en general, de manera que existe un homomorfismo de grupos de $(HS_k(A), \circ)$ en el grupo aditivo (abeliano) de las k-derivaciones usuales de A. El teorema IV–A.6, sugiere la existencia de una acción de los elementos de A sobre $HS_k(A)$ que satisface identidades de tipo no lineal, y que de alguna forma levanta la estructura de A-módulo sobre las derivaciones usuales. Sería interesante conocer y describir la estructura resultante, y eventualmente relacionarla con los grupos formales.
- La motivación original del trabajo [Nar91], era el cálculo de una dimensión homológica de un anillo de operadores diferenciales tras una extensión de escalares del tipo $k \to k(t)$, en el caso de cuerpos de característica cero. Los resultados de esta memoria parecen poder aplicarse de manera completamente análoga al caso de la extensión $k \to k(t)_{\mathrm{per}}$, si k es un cuerpo de característica $p > 0$.
- En el mismo sentido que el punto anterior, los resultados de esta memoria establecen algunas bases algebraicas para el estudio de ecuaciones funcionales tipo Bernstein-Sato [Ber72],

en el caso de cuerpos base de característica $p > 0$. El modelo a seguir sería el trabajo [MNM91].

DESCRIPCIÓN DEL CONTENIDO DE LA MEMORIA

El capítulo 1 está dedicado, en primer lugar, a recordar algunos resultados generales para la conveniencia del lector y que serán usados a lo largo de la memoria. Así, recordamos la noción de *derivación de Hasse-Schmidt* de una k-álgebra ([HS37],[NaK70]), como noción puramente algebraica que generaliza la de *derivación* de un anillo conmutativo.

Hemos recopilado algunos resultados de los trabajos [Mat86], [Mat82], [Ish77], [NaK70], y en algunos casos que consideramos oportunos incluimos sus demostraciones. En particular destacamos la relación existente entre las derivaciones de Hasse-Schmidt y el desarrollo de Taylor (cf. [MV69]), cuya filosofía la podemos resumir gráficamente en que, a pesar de las apariencias, "no es necesario dividir por los factoriales".

Recordamos también el concepto de *operadores diferenciales lineales* sobre una k-álgebra A. La referencia básica utilizada es [GD67], en donde se presenta una definición recursiva, respecto del orden, de los operadores diferenciales lineales. Dicha definición nos muestra directamente su estructura algebraica: se trata de un anillo (para la suma y composición de operadores), filtrado (por el orden de los operadores), no conmutativo en general, cuyo graduado sí es conmutativo. A continuación examinamos la relación entre las *derivaciones de Hasse-Schmidt* y los operadores diferenciales lineales, así como el caso fundamental de los anillos de polinomios y de series formales. Por último, estudiamos las propiedades de extensión a los completados, a los anillos de polinomios y a los anillos de fracciones.

En el capítulo 2, ofrecemos una demostración del lema de normalización para el anillo de series de potencias formales $A = k[[\underline{X}]]$, con k cuerpo perfecto de característica $p > 0$, que es una adaptación de la que se encuentra en [Abh64], (23.7) y (24.5). La prueba de loc. cit. usa cambios de coordenadas lineales y necesita que el cuerpo k sea infinito. Nuestra adaptación (teorema II–A.6), es válida para un cuerpo de coeficientes perfecto (infinito o no), usando cambios de coordenadas no lineales como los del lema II–A.4.

En el capítulo 3, estudiamos la conservación de la noetherianidad mediante la extensión del cuerpo base $k \to k_{(\infty)} := k(t)_{per}$, donde k es un cuerpo perfecto y $k(t)_{per}$ es la clausura perfecta de $k(t)$. Nuestro principal resultado caracteriza cuándo el anillo

$$A_{(\infty)} := A \otimes_k k_{(\infty)} = A \otimes_k k_{per}(t)$$

es noetheriano, y como consecuencia probamos que el anillo $A_{(\infty)}$ es noetheriano cuando A es el anillo de series formales en n indeterminadas sobre k (corolario III–C.8).

Además, probamos que el mayor subcuerpo perfecto de un cuerpo de funciones formales sobre k, es una extensión finita del cuerpo de constantes k (teorema III–B.8) [1]. Una versión más débil del resultado anterior, que dicha extensión es algebraica (proposición III–B.6), es uno de los ingredientes de la prueba de la caracterización de la conservación de la noetherianidad que acabamos de mencionar.

En el capítulo 4, determinamos cuerpos de coeficientes del anillo completado de un anillo noetheriano, local, regular, equicaracterístico de característica positiva, mediante una generalización del teorema 99 de [Mat80] al caso de derivaciones de Hasse-Schmidt (teorema IV–A.10). Dicha generalización utiliza, como herramienta fundamental, el teorema IV–A.6, que nos permite generar derivaciones de Hasse-Schmidt a partir de unas fijas, siempre que sus componentes de grado uno formen un sistema de generadores de las k-derivaciones de

[1] Resultado demostrado en colaboración con el profesor J. M. Giral.

nuestro anillo. Este último resultado, sugiere un estudio en profundidad de estructuras algebraicas no lineales sobre las derivaciones de Hasse-Schmidt.

Por último, en el capítulo 5, generalizamos el teorema 2.3 del trabajo [Nar91] al caso del anillo $R = k[[X_1, \ldots, X_n]]$, siendo k un cuerpo perfecto de característica $p > 0$. Para ello consideramos la extensión de escalares

$$R \longrightarrow R \otimes_k k(t)_{\text{per}} = R_{(\infty)},$$

donde $k(t)_{\text{per}} = \bigcup_{m \geq 0} k(t^{\frac{1}{p^m}})$ es el cierre perfecto de $k(t)$ y t es trascendente sobre k. Por el capítulo 3, sabemos que $R_{(\infty)}$ es noetheriano. Si $\mathfrak{m} \subset R_{(\infty)}$ es un ideal maximal y K es su cuerpo residual, construimos un isomorfismo de Cohen explícito $K[[Y_1, \ldots, Y_n]] \simeq \widehat{(R_{(\infty)})_{\mathfrak{m}}}$ de manera que las extensiones de las k-derivaciones de Hasse-Schmidt de R a este último anillo correspondan a K-derivaciones del primero. Dicho de otra forma, encontramos un cuerpo de coeficientes del anillo local completo $\widehat{(R_{(\infty)})_{\mathfrak{m}}}$, donde se anulan las extensiones de Hasse-Schmidt de R. Es más, dicho cuerpo de coeficientes está formado justamente por aquellos elementos anulados por las citadas extensiones.

ÍNDICE GENERAL

CAPÍTULO I

Notación y Preliminares

En este capítulo recordaremos algunos resultados conocidos para la comodidad del lector, y desarrollaremos una exposición sistemática de los resultados que necesitaremos posteriormente.

Todos los anillos y álgebras considerados en esta memoria serán conmutativos y con elemento unidad. Usaremos las letras L, K, k para denotar cuerpos y $\mathbb{F}_p$ para el cuerpo finito de p elementos, siendo p cualquier número primo.

Si B es un anillo, notaremos por $\dim(B)$ a la dimensión de Krull de B y $\Omega(B)$ al conjunto de todos los ideales maximales de B. Si $\mathfrak{p} \in \operatorname{Spec}(B)$, notaremos por $\operatorname{ht}(\mathfrak{p})$ a la altura de $\mathfrak{p}$. Si B es un dominio de integridad, notaremos por $Qt(B)$ a su cuerpo cociente.

Recordemos que un anillo B se dice *equicodimensional* si todos los ideales maximales de B tienen la misma altura. Además, B se llama *biequidimensional* si todas las cadenas saturadas de ideales primos en B tienen la misma longitud.

I–A La $k(t)$–álgebra $A(t)$

En esta sección recordamos algunos resultados de [Nar91], acerca de la $k(t)$-álgebra $A(t)$, siendo k un cuerpo y A una k-álgebra de dimensión de Krull n.

Consideramos la extensión de cuerpos $k \subset k(t)$ en una indeterminada t, y denotamos por $A(t)$ a la $k(t)$-álgebra

$$A(t) := k(t) \otimes_k A.$$

Si S es el subconjunto multiplicativamente cerrado de $k[t]$ formado por los polinomios no nulos, entonces

$$A(t) = S^{-1}A[t].$$

Por tanto, tenemos una correspondencia uno a uno, mediante extensión-contracción, entre los ideales $\mathfrak{p} \in \mathrm{Spec}(A[t])$ tales que $\mathfrak{p} \bigcap k[t] = (0)$ y los ideales primos de $A(t)$. Más aún, si A es una k–álgebra noetheriana se tiene que

$$dim(A) \leq dim(A(t)) \leq dim(A[t]) = dim(A) + 1.$$

El siguiente lema se puede encontrar, por ejemplo, en [GD65], proposiciones 5.5.3 y 5.5.6:

Lema I–A.1 ■ Sea B un anillo noetheriano, P un ideal primo de $B[t]$ y $\mathfrak{p} = P \bigcap B$. Entonces se verifica una de las siguientes condiciones:

(a) $P = \mathfrak{p}[t]$, $\mathrm{ht}(P) = \mathrm{ht}(\mathfrak{p})$ y $B[t]/P \simeq (A/\mathfrak{p})[t]$.

(b) $P \supset \mathfrak{p}[t]$, $\mathrm{ht}(P) = \mathrm{ht}(\mathfrak{p})+1$ y $B[t]/P$ es una extensión algebraica de $B/\mathfrak{p}$ (generada por t módulo P).

Una condición suficiente para que $dim(A) = dim(A(t))$ es :

Proposición I–A.2 ■ *([Nar91], proposición 1.4)* Sea A una k-álgebra noetheriana y supongamos que, para todo ideal maximal $\mathfrak{m}$ de A, el cuerpo residual $A/\mathfrak{m}$ es algebraico sobre k. Entonces $dim(A(t)) = dim(A)$.

Teorema I–A.3 ■ *([Nar91], teorema 1.6)* Sea A una k-álgebra noetheriana, biequidimensional, universalmente catenaria de dimensión de Krull n, tal que para todo ideal maximal $\mathfrak{m}$ de A, el cuerpo residual $A/\mathfrak{m}$ es algebraico sobre k. Entonces $A(t)$ es equicodimensional de dimensión n.

Nota I–A.4 ■ Bajo las hipótesis del teorema I–A.3 se deduce además que $A(t)$ es biequidimensional y universalmente catenaria. Sin embargo los cuerpos residuales sobre los ideales maximales de $A(t)$ no son, en general, algebraicos sobre $k(t)$.

Nota I–A.5 ■ Como consecuencia del teorema I–A.3, tenemos dos posibilidades para un ideal maximal M de $A(t)$.

(i) El ideal $\mathfrak{p} = M \cap A$ es maximal y $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(M) = n$. Entonces M es el ideal extendido de $\mathfrak{p}$, y $A(t)/M = k(t) \otimes_k A/\mathfrak{p}$ es algebraico sobre $k(t)$.

(ii) $\mathrm{ht}(\mathfrak{p}) = n - 1$. En este caso, $A(t)/M$ no es necesariamente algebraico sobre $k(t)$, como se muestra en el siguiente ejemplo.

Ejemplo I–A.6 ■ Sea $A = k[[X]]$ el anillo de series formales en una variable, entonces A satisface las hipótesis del teorema I–A.3. Si

$$P = (Xt - 1) \cdot A[t],$$

entonces P es maximal y $P \cap k[t] = 0$. Por tanto, $M = S^{-1}P$ es un ideal maximal en $A(t)$ y el cuerpo residual $A(t)/M = A[t]/P$ coincide con el cuerpo de fracciones de A, que tiene grado de trascendencia infinito sobre k.

I–B Resultados generales

En primer lugar, recordamos algunos resultados bien conocidos sobre extensiones enteras de anillos.

Teorema I–B.1 ■ **(Teorema del ascenso)***(cf. [AM69], teorema* 5.11*)* Sean $A \subseteq B$ anillos, B es entero sobre A. Sea $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ una cadena de ideales primos de A, y $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ (con $m < n$) una cadena de ideales primos de B tales que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ con $1 \leq i \leq m$. Entonces la cadena $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ se puede extender a una cadena $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$ tal que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para $1 \leq i \leq n$.

Definición I–B.2 ■ Sea $\Phi : A \to B$ un homomorfismo de anillos. Diremos que Φ verifica el teorema del descenso si para todo $\mathfrak{p}_1, \mathfrak{p}_2$ ideales primos de A tales que $\mathfrak{p}_1 \subset \mathfrak{p}_2$, y para cada ideal primo de B, P_2, tal que $P_2 \cap A = \mathfrak{p}_2$; existe P_1 ideal primo de B, que se contrae en $\mathfrak{p}_1$ ($P_1 \cap A = \mathfrak{p}_1$), y tal que $P_1 \subset P_2$.

Teorema I–B.3 ■ *(cf. [Mat80], teorema 4)* Sea $\Phi : A \to B$ un homomorfismo plano de anillos. Entonces el teorema del descenso se verifica para Φ.

Dos resultados sobre extensiones de cuerpos que necesitaremos son los siguientes:

Teorema I–B.4 ■ *(cf. [ZS79],* §5, *teorema* 8*)* Si K es una extensión algebraica separable de k, entonces $kK^p = K$. Recíprocamente, si K es una extensión de k tal que $kK^p = K$ y si la extensión K/k es finita, entonces K es una extensión separable de k.

Teorema I–B.5 ■ *(cf. [Jou83], teorema* 3.11*)* Sea K una extensión de un cuerpo k. Son equivalentes:

1. El cuerpo k es algebraicamente cerrado en K y K es separable sobre k.
2. $K \otimes_k \overline{k}$ es un cuerpo.
3. Existe una extensión algebraicamente cerrada Ω de k tal que $K \otimes_k \Omega$ es íntegro.
4. Para toda extensión L de k, el anillo $K \otimes_k L$ es íntegro.
5. Para toda extensión finita k' de k, el anillo $K \otimes_k k'$ es un cuerpo.

Además, recordamos el teorema preparatorio de Weiertrass para series formales.

Definición I–B.6 ■ Sobre un cuerpo k cualquiera y en el anillo de series formales $k[[\underline{X}]] = k[[X_1, \ldots, X_n]]$ y con la misma notación de (I–D.10), dada $f \in k[[\underline{X}]]$, definimos *ord(f)* como el menor $|\alpha|$ para el cual f_α es distinto de cero. Por convenio a la serie nula le asignaremos el orden ∞.

Definición I–B.7 ■ Sea $f(\underline{X}) \in k[[\underline{X}]]$, se dice que f es X_i-distinguida si

$$f(0,\dots,0,X_i,0,\dots,0) \neq 0.$$

Teorema I–B.8 ■ **(Teorema preparatorio de Weiertrass)***(cf. [Che79], Corolario 6.3.6)* Si $g \in k[[t,\underline{X}]]$, g es t-distinguida y

$$ord_t(g) = ord(g(t,\underline{0})) = m \geq 0,$$

entonces existen unos únicos $u(t,\underline{X})$, $p(t,\underline{X}) \in k[[t,\underline{X}]]$ tales que

1. $g = u \cdot p$, $u(0,\underline{0}) \neq 0$ y u unidad.
2. $p(t,\underline{X}) = t^m + p_1(\underline{X})t^{m-1} + \cdots + p_m(\underline{X})$ y $p_i(\underline{0}) = 0$ para $i = 1,\dots,m$.

Por último, recordamos las nociones de cuerpo de coeficientes de un anillo local, el teorema de estructura de Cohen, la noción de anillo formalmente liso, formalmente étale, así como la de cuerpo de casi-coeficientes que utilizaremos en los capítulos IV y V.

Definición I–B.9 ■ *(cf. [Mat80],(28.A))* Sea $(R,\mathfrak{m})$ un anillo local, $K = R/\mathfrak{m}$ su cuerpo residual y k un subcuerpo de R. Decimos que k es un cuerpo de coeficientes de R si k se aplica isomórficamente sobre K mediante la aplicación natural $R \to R/\mathfrak{m}$.

Teorema I–B.10 ■ **(Teorema de estructura de Cohen)***(cf. [Mat80], (28.J), teorema 60)* Sea $(R,\mathfrak{m},K)$ un anillo local, separado y completo, que contiene a un cuerpo k. Entonces R contiene un cuerpo de coeficientes. Además, si K es separable sobre k, entonces R contiene un cuerpo de coeficientes que contiene a k.

Veáse también en [GD64], Chap. 0,Th.(19.8.8).

Definición I–B.11 ■ *(cf. [Mat80],* 28.*C)* Sean k, A anillos topológicos y $g : k \to A$ un homomorfismo continuo. Decimos que A es formalmente liso, o que A es una k-álgebra formalmente lisa, si se verifica la siguiente condición: Para cualquier anillo discreto C, para todo ideal N de C con $N^2 = (0)$ y para todo homomorfismo continuo $u : k \to C$ y $v : A \to C/N$ (viendo a C/N como un anillo discreto) tal que el diagrama

$$\begin{array}{ccc} A & \xrightarrow{v} & C/N \\ g\uparrow & & \uparrow q \\ k & \xrightarrow{u} & C \end{array}$$

(donde q es la aplicación natural) es conmutativo, existe un homomorfismo $v' : A \to C$ tal que $v = qv'$ y $u = v'g$.

$$\begin{array}{ccc} A & \xrightarrow{v} & C/N \\ g\uparrow & \searrow v' & \uparrow q \\ k & \xrightarrow{u} & C \end{array}$$

Si v' existe, entonces decimos que v puede levantarse a $A \to C$ sobre k, y v' se le llama un levantamiento de v sobre k.

Definición I–B.12 ■ *(cf. [Mat80], (38.E))* Bajo las mismas condiciones de la definición anterior, decimos que A es formalmente étale sobre k, si el levantamiento v' de v es único.

Nota I–B.13 ■ *(cf. [Mat80], (38.E))* Sea K/k una extensión de cuerpos. Si la característica de K es cero, entonces formalmente étale es lo mismo que algebraica separable.

Definición I–B.14 ■ *(cf. [Mat80], (38.F))* Sea $(R, \mathfrak{m}, K)$ un anillo local, (siendo $K = R/\mathfrak{m}$ su cuerpo residual) y k_0 un subcuerpo de R. Decimos que k_0 es un cuerpo de casicoeficientes de R si K/k_0 es formalmente étale.

I–C La extensión $K[t] \subset K[t^{\frac{1}{p}}]$

En esta sección analizamos el proceso de extensión–contracción de los ideales primos relativos a la extensión $K[t] \subset K[t^{\frac{1}{p}}]$, siendo K un cuerpo de característica $p > 0$. Una herramienta fundamental es el siguiente teorema:

Teorema I–C.1 ■ *(cf. [Gar86], teorema 10.8)* Sean K cuerpo de característica $p > 0$ y

$$g(X) = a_0 + a_1 X + \cdots + X^n$$

un polinomio mónico de $K[X]$. Entonces el polinomio

$$f(X) = g(X^p) = a_0 + a_1^p X^p + \cdots + X^{np}$$

es irreducible en $K[X]$ si y solo si g es irreducible en $K[X]$, y no todos sus coeficientes a_i son potencias p-ésimas de elementos de K.

Demostración. Si g factoriza como $g = g_1 g_2$ entonces f factoriza como

$$f(X) = g_1(X^p) g_2(X^p).$$

Por tanto si f es irreducible también lo es g. Supongamos ahora que cada a_i es una potencia p-ésima de un elemento de K, es decir $a_i = b_i^p$ para $b_i \in K$. Entonces f factoriza

$$f = b_0^p + b_1^p X^p + \cdots + b_n^p X^{np} = (b_0 + b_1 X + \cdots + b_n X^n)^p.$$

Por tanto si f es irreducible, no todos los a_i son potencias p-ésimas de elementos de K.

Recíprocamente, supongamos que f factoriza. Debemos probar que o g factoriza, o todos los a_i son potencias p-ésimas de elementos de K. Podemos escribir f como producto de factores irreducibles:

$$f = f_1^{n_1} \cdot \cdot \cdot f_r^{n_r}$$

donde los f_i son mónicos e irreducibles en $K[X]$, f_i y f_j son primos relativos para $i \neq j$ y $n_1 + \cdot \cdot \cdot + n_r > 1$. Consideramos dos casos:

- Supongamos primero $r > 1$. Entonces podemos escribir $f = h_1 h_2$ con h_1 y h_2 primos relativos (tomando $h_1 = f_1^{n_1}$). Y existen λ_1 y λ_2 en $K[X]$ tales que $\lambda_1 h_1 + \lambda_2 h_2 = 1$. Por lo tanto

  $$0 = Df = (Dh_1)h_2 + h_1(Dh_2).$$

  Eliminando h_2, tenemos que

  $$Dh_1 = \lambda_1 h_1(Dh_1) - \lambda_2 h_1(Dh_2)$$

  y entonces $h_1 \mid Dh_1$. Como el grado de Dh_1 es menor que el grado de h_1 se tiene que Dh_1 debe ser 0. De la misma manera $Dh_2 = 0$. Entonces podemos escribir

  $$h_1(X) = c_0 + c_1 X^p + \cdot \cdot \cdot + c_s X^s p = j_1(X^p)$$

  $$h_2(X) = d_0 + d_1 X^p + \cdot \cdot \cdot + d_t X^t p = j_2(X^p)$$

  y g factoriza como $g = j_1 j_2$.

- Supongamos ahora que $r = 1$. Entonces $f = f_1^n$ donde f_1 es irreducible y $n > 1$. De nuevo tenemos que considerar dos subcasos:

  Si $p \mid n$, podemos escribir $f = h^p$. Si $h = c_0 + c_1 X + \cdot \cdot \cdot + c_s X^s$, entonces

  $$f = h^p = c_0^p + c_1^p X^p + \cdot \cdot \cdot + c_s^p X^{sp}.$$

Así que todos los c_i son potencias p-ésimas.

Si p no divide a n,

$$0 = D_f = n(Df_1)f_1^{n-1}$$

y entonces $Df_1 = 0$. Así que podemos escribir

$$f_1(X) = d_0 + d_1 X^p + \cdots + d_t X^{tp} = g_1(X^p)$$

y $g = (g_1)^n$.

■

Del resultado anterior, deducimos el siguiente corolario, que nos describe el comportamiento de la extensión-contracción de ideales primos en la extensión $K[t] \subset K[t^{\frac{1}{p}}]$.

Corolario I–C.2 ■ Sea K cuerpo de característica $p > 0$. Sea P un ideal primo no nulo en $K[t^{\frac{1}{p}}]$ y sea $F(t) \in K[t]$ el polinomio mónico irreducible generador de la contracción $P^c = P \cap K[t]$. Entonces se verifican las siguientes condiciones

1. Si $F(t) = a_0^p + a_1^p t + \cdots + t^d \in K^p[t]$, entonces
$$P = (a_0 + a_1 t^{\frac{1}{p}} + \cdots + t^{\frac{d}{p}}).$$
2. $P = P^{ce}$ si y solo si no todos los coeficientes de $F(t)$ son potencias p-ésimas de elementos de K.

Demostración.

1. Veamos en primer lugar que si el polinomio
$$F(t) = a_0^p + a_1^p t + \cdots + t^d \in K[t]$$
es irreducible, entonces el polinomio
$$G(\tau) = a_0 + a_1 \tau + \cdots + \tau^d \in K[\tau] \; (\tau = t^{\frac{1}{p}}),$$

también lo es: Para ello consideremos el homomorfismo de anillos

$$\mu : K \longmapsto K$$

con $\mu(a) = a^p$ para todo $a \in K$,y consideremos

$$\tilde{\mu} : K[\tau] \longmapsto K[t]$$

definida por

$$\tilde{\mu}(\sum a_i \tau^i) = \sum \mu(a_i) t^i,$$

es fácil comprobar que

(a) $\tilde{\mu}$ es homomorfismo de anillos (puesto que μ lo es),

(b) $\tilde{\mu}(G) = F$, y

(c) $\tilde{\mu}$ aplica un elemento no unidad en un elemento no unidad, puesto que las unidades de $K[\tau]$ son las del cuerpo K.

Supongamos que G es reducible, entonces $F = \tilde{\mu}(G)$ también lo es (pues $\tilde{\mu}$ es homomorfismo de anillos). Es decir, si F es irreducible, G también lo es. Luego el ideal $(G(\tau))$ es primo en $K[t^{\frac{1}{p}}]$. Además, dado que

$$G(\tau)^p = F(t) \in P$$

y P es un ideal primo, se tiene que $G(\tau) \in P$ y por tanto,

$$(G(\tau)) \subset P;$$

y como

$$dim(K[t^{\frac{1}{p}}]) = dim(K[t]) = 1,$$

entonces se tiene que $(G(\tau)) = P$.

2. Supongamos ahora que

$$P^{ce} = (F) \cdot K[t^{\frac{1}{p}}] = (a_0 + a_1(t^{\frac{1}{p}})^p + \cdot \cdot \cdot + (t^{\frac{1}{p}})^{pd}) \cdot K[t^{\frac{1}{p}}],$$

pero ahora $F \in K[t^{\frac{1}{p}}]$. Sea $\tau = t^{\frac{1}{p}}$. La igualdad

$$P = P^{ce}$$

significa que

$$F(t) = F(\tau^p) \in K[\tau]$$

genera el ideal P. Lo que equivale a decir que $F(\tau^p)$ es irreducible en $K[\tau]$. Por el teorema I-C.1, equivale a decir que $F(\tau)$ es irreducible en $K[\tau]$ y no todos sus coeficientes son potencias p-ésimas de elementos de K.

∎

I–D Derivaciones de Hasse-Schmidt

En esta sección recordamos la noción de derivación de Hasse-Schmidt [HS37]. Se trata de un concepto puramente algebraico que generaliza al de derivación sobre un anillo conmutativo, en el caso de característica positiva. Hemos recopilado algunos resultados de [Mat86], [Mat82], [Ish77], [NaK70], dando las demostraciones de aquellos que nos parecen oportunos. En particular destacamos la relación existente entre las derivaciones de Hasse-Schmidt y el desarrollo de Taylor. Además, demostraremos que se pueden extender de manera única a la completación, por ser I–continuas para la topología I–ádica del anillo.

Sean $k \xrightarrow{f} A \xrightarrow{g} B$ homomorfismos de anillos. Sea t una indeterminada sobre B. Sean

$$B_m = B[t]/(t^{m+1}) \quad (m \geq 0) \text{ y } B_\infty = B[[t]].$$

Podemos considerar, de manera natural, a B_m $(m \leq \infty)$ como una k-álgebra.

Definición I–D.1 ■ En las condiciones anteriores, una sucesión

$$\underline{D} = (D_0, D_1, \ldots, D_m)$$

de aplicaciones k–lineales ($D_i : A \longrightarrow B$) se dice derivación de Hasse-Schmidt de longitud m de A en B (sobre k) si se verifica:

$$D_0 = g \quad \text{y} \quad D_i(xy) = \sum_{r+s=i} D_r(x) D_s(y) \qquad (1 \leq i \leq m,\ x, y \in A)$$

Una caracterización muy útil de las derivaciones de Hasse-Schmidt es la siguiente, que relaciona este concepto con los homomorfismos de A en B_m que coinciden con g módulo t.

Lema I–D.2 ■ En las condiciones anteriores, son equivalentes:

1. $\underline{D}$ es una derivación de Hasse-Schmidt de longitud m de A en B
2. La aplicación $E_t : A \longrightarrow B_m$ definida por
$$E_t(x) = \sum_{i=0}^{m} D_i(x) t^i$$
es un homomorfismo de k–álgebras que verifica
$$E_t(x) \equiv g(x) \pmod{t}.$$

Demostración. Probémoslo para $m < \infty$:

(1) $\Longrightarrow$ (2):

- Veamos que E_t es homomorfismo de k–álgebras: la k–linealidad se sigue trivialmente de la k–linealidad de las D_i. Se tiene que:

$$E_t(xy) = \sum_{i=0}^{m} D_i(xy)t^i = \sum_{i=0}^{m}\left(\sum_{r+s=i} D_r(x)D_s(y)\right) t^i,$$

por otro lado

$$\begin{aligned} E_t(x)E_t(y) &= \left(\sum_{r=0}^{m} D_r(x)t^r\right)\left(\sum_{s=0}^{m} D_s(y)t^s\right) = \\ &= \sum_{i=0}^{m}\left(\sum_{r+s=i} D_r(x)D_s(y)\right) t^i + \sum_{i=m+1}^{2m}\left(\sum_{r+s=i} D_r(x)D_s(y)\right) t^i \end{aligned} \quad ((\text{I–D.1}))$$

luego

$$E_t(xy) \equiv E_t(x)E_t(y) \pmod{t^{m+1}}.$$

- $E_t(x) \equiv g(x) \pmod{t}$:

$$\begin{aligned} E_t(x) - g(x) &= \sum_{i=0}^{m} D_i(x)t^i - g(x) \\ &= \sum_{i=1}^{m} D_i(x)t^i = t\left(\sum_{i=1}^{m} D_i(x)t^{i-1}\right). \end{aligned}$$

(2) $\Longrightarrow$ (1):

- $E_t(x+y) = E_t(x) + E_t(y)$, por tanto

$$\sum_{i=0}^{m} D_i(x+y)t^i = \sum_{i=0}^{m} D_i(x)t^i + \sum_{i=0}^{m} D_i(y)t^i,$$

de donde se sigue que

$$D_i(x+y) = D_i(x) + D_i(y).$$

Análogamente se prueba que

$$D_i(\lambda x) = \lambda D_i(x), \ (\lambda \in k, \ x \in A).$$

- De $E_t(x) \equiv g(x) \pmod{t}$ se sigue que

$$E_t(x) - g(x) = D_0(x) - g(x) + \sum_{i=1}^{m} D_i(x)t^i = 0 \pmod{t}$$

y por tanto $D_0 = g$.

- De $E_t(xy) = E_t(x)E_t(y)$ se sigue, utilizando (I–D.1), que

$$D_i(xy) = \sum_{r+s=i} D_r(x)D_s(y).$$

Con ésto se concluye la demostración del lema I–D.2 para $m < \infty$. En el caso $m = \infty$, la prueba es análoga. ∎

Notas I–D.3 ∎

1. Cuando $A = B$ y $g = 1_A$, entonces hablaremos simplemente de una k–derivación de A. A partir de ahora consideraremos este caso.
2. $D_i(1) = 0$, para todo $i > 0$:
   Para $i = 1$ trivial, pues D_1 es derivación. Supongamos cierto hasta $i - 1$, veamos para i:
   $$\begin{aligned} D_i(1) &= D_i(1 \cdot 1) = \sum_{r+s=i} D_r(1)D_s(1) = \\ &= 2D_i(1) + \sum_{\substack{r+s=i \\ r,s \leq i-1}} D_r(1)D_s(1) = \\ &= 2D_i(1) \end{aligned}$$
   por tanto $D_i(1) = 0$.
3. Si $\underline{D}$ es una k–derivación de Hasse-Schmidt de A entonces $D_1 \in Der_k(A)$, puesto que
   $$D_1(xy) = \sum_{r+s=1} D_r(x)D_s(y) = xD_1(y) + D_1(x)y, \ (x, y \in A).$$
   Además, D_i es cero sobre $f(k)$ para $i > 0$: ya que
   $$D_i(f(\lambda)) = D_i(\lambda \cdot 1) = \lambda D_i(1) = 0.$$

En general, diremos que $\underline{D}$ es trivial sobre $a \in A$, si $D_i(a) = 0$ para $i > 0$; esto quiere decir que $E_t(a)$ es una constante siendo E_t el endomorfismo correspondiente a $\underline{D}$, pues

$$E_t(a) = \sum_{i=0}^{m} D_i(a)t^i = D_0(a) = g(a).$$

Notaremos $HS_k(A, m)$ al conjunto de todas las k–derivaciones de Hasse-Schmidt de longitud m de A, y $HS_k(A) = HS_k(A, \infty)$. Si no hay confusión sobre el cuerpo k, escribiremos $HS(A, m)$ y $HS(A)$, respectivamente. Estos conjuntos no tienen estructura de módulo como $Der_k(A)$. Sin embargo, pueden ser dotados de estructura de grupo (generalmente no abeliano) de la siguiente manera:

Lema I–D.4 ■ El homomorfismo $E_t : A \longrightarrow A_m$ correspondiente a $\underline{D} \in HS_k(A, m)$ se puede extender a un automorfismo de A_m de la siguiente forma:

$$E_t\left(\sum_{\nu} a_\nu t^\nu\right) = \sum_{\nu} E_t(a_\nu)t^\nu$$

Demostración. La extensión de E_t así definida es trivialmente k–lineal. Veamos que es biyectiva:

- **Inyectividad:** Se tiene que si

$$\rho = a_r t^r + a_{r+1}t^{r+1} + \cdots \in A_m \qquad a_r \neq 0,$$

entonces

$$E_t(\rho) \equiv a_r t^r \pmod{t^{r+1}},$$

puesto que

$$\begin{aligned} E_t(\rho) - a_r t^r &= E_t(a_r)t^r + E_t(a_{r+1})t^{r+1} + \cdots - a_r t^r = \\ &= \left(\sum_{i=0}^{m} D_i(a_r)t^i\right) t^r - a_r t^r + E_t(a_{r+1})t^{r+1} + \cdots = \\ &= \left(\sum_{i=1}^{m} D_i(a_r)t^{r+i}\right) + E_t(a_{r+1})t^{r+1} + \cdots = \\ &= t^{r+1}\left(D_1(a_r) + E_t(a_{r+1}) + \ldots\right) \end{aligned}$$

y, por tanto, E_t así definida es inyectiva.

- **Sobreyectividad:** Dado $\rho = a_r t^r + a_{r+1} t^{r+1} + \cdots \in A_m$, se tiene que:

$$\begin{aligned} \rho - E_t(a_r t^r) &= a_r t^r + a_{r+1} t^{r+1} + \cdots - E_t(a_r) t^r = \\ &= a_r t^r + a_{r+1} t^{r+1} + \cdots - a_r t^r - D_1(a_r) t^{r+1} - \cdots = \\ &= b_{r+1} t^{r+1} + \ldots \end{aligned}$$

para unos ciertos $b_k \in A$, $k \geq r+1$.

$$\begin{aligned} \rho - E_t(a_r t^r + b_{r+1} t^{r+1}) &= \rho - E_t(a_r) t^r - E_t(b_{r+1}) t^{r+1} = \\ &= b_{r+1} t^{r+1} + b_{r+2} t^{r+2} + \cdots - \\ &\quad - b_{r+1} t^{r+1} - D_1(b_{r+1}) t^{r+2} - \cdots = \\ &= c_{r+2} t^{r+2} + \ldots \end{aligned}$$

para unos ciertos $c_l \in A$, $l \geq r+2$. Reiterando el proceso encontramos un elemento

$$a_r t^r + b_{r+1} t^{r+1} + c_{r+2} t^{r+2} + \cdots \in A_m - \{0\}, \text{ pues } a_r \neq 0.$$

Además verifica:

$$\rho - E_t(a_r t^r + b_{r+1} t^{r+1} + c_{r+2} t^{r+2} + \ldots) \in (t^{m+1}).$$

Con ésto se prueba que el homomorfismo E_t es sobreyectivo.

∎

Como consecuencia, un automorfismo E de la k–álgebra A_m que satisface $E(a) \equiv a \pmod t$ corresponde a una derivación de Hasse-Schmidt. Así podemos identificar $HS_k(A, m)$ con un subgrupo del grupo $Aut_k(A_m)$. Esto induce la siguiente estructura de grupo en $HS_k(A, m)$: Para $\underline{D} = (D_0, D_1, \ldots)$ y $\underline{D}' = (D'_0, D'_1, \ldots)$ sean

$$\underline{D} \cdot \underline{D}' = (D''_0, D''_1, \ldots)$$

y

$$\underline{D}^{-1} = (D^*_0, D^*_1, \ldots).$$

Entonces:

$$\begin{aligned}
E_t(E'_t(a)) &= E_t\left(a + D'_1(a)t + D'_2(a)t^2 + \dots\right) = \\
&= \left(a + D_1(a)t + D_2(a)t^2 + \dots\right) + \left(D'_1(a) + D_1(D'_1(a))t + \dots\right)t + \\
&+ \left(D'_2(a) + D_1(D'_2(a))t + \dots\right)t^2 + \cdots = \\
&= a + (D_1 + D'_1)(a)t + (D_2 + D_1D'_1 + D'_2)(a)t^2 + \dots
\end{aligned}$$

así que

$$D''_i = \sum_{p+q=i} D_p D'_q \text{ para todo } i.$$

Luego:

$$\underline{D} \cdot \underline{D}' = (1_A,\ D_1 + D'_1,\ D_2 + D_1D'_1 + D'_2,\ \dots,\ \sum_i D_i D'_{n-i},\ \dots).$$

Resolviendo $\sum_{p+q=i} D_p D^*_q = 0$ para $i > 0$ se obtienen los D^*_i, esto es:

$$\begin{aligned}
D^*_0 &= D_0 = 1_A \\
D^*_1 &= -D_1 \\
D^*_2 &= D_1^2 - D_2 \\
D^*_3 &= -D_1^3 + D_1D_2 + D_2D_1 - D_3 \\
&\vdots
\end{aligned}$$

Lema I–D.5 ■

$$D^*_n = \sum_{k=1}^{n} (-1)^k \left(\sum_{\substack{i_1+\cdots+i_k=n \\ i_j \geq 1}} D_{i_1} \cdots D_{i_k} \right) \quad \forall n \geq 1.$$

Demostración. Por inducción en n:

Para $n = 1$: $D^*_1 = (-1)^1 D_1 = -D_1$

Supongamos cierto hasta $n-1$, veamos si es cierto para n: D_n^* se obtiene de

$$\sum_{q=0}^{n} D_{n-q} D_q^* = 0;$$

luego

$$\begin{aligned}
D_n^* &= -\sum_{q=0}^{n-1} D_{n-q} D_q^* = \\
&= -D_n - \sum_{q=1}^{n-1} D_{n-q} D_q^* = [\text{hip. ind.}] = \\
&= -D_n - \sum_{q=1}^{n-1} D_{n-q} \sum_{k=1}^{q} (-1)^k \left(\sum_{\substack{i_1+\cdots+i_k=q \\ i_j \geq 1}} D_{i_1} \cdots D_{i_k} \right) = \\
&= -D_n + \sum_{q=1}^{n-1} \sum_{k=1}^{q} (-1)^{k+1} D_{n-q} \left(\sum_{\substack{i_1+\cdots+i_k=q \\ i_j \geq 1}} D_{i_1} \cdots D_{i_k} \right) = \\
&= -D_n + \sum_{q=1}^{n-1} \sum_{k=1}^{q} (-1)^{k+1} \left(\sum_{\substack{i_1+\cdots+i_k=q \\ i_j \geq 1}} D_{n-q} D_{i_1} \cdots D_{i_k} \right) = \\
&= -D_n + \sum_{q=1}^{n-1} \sum_{l=2}^{q+1} (-1)^l \left(\sum_{i_1+\cdots+i_l=n} D_{i_1} \cdots D_{i_l} \right) = \\
&= -D_n + \sum_{l=2}^{n} (-1)^l \left(\sum_{\substack{i_1+\cdots+i_l=n \\ i_j \geq 1}} D_{i_1} \cdots D_{i_l} \right) =
\end{aligned}$$

$$= \sum_{l=1}^{n}(-1)^l \left(\sum_{\substack{i_1+\cdots+i_l=n \\ i_j \geq 1}} D_{i_1} \cdots D_{i_l} \right).$$

Así que

$$D_n^* = \sum_{k=1}^{n}(-1)^k \left(\sum_{\substack{i_1+\cdots+i_k=n \\ i_j \geq 1}} D_{i_1} \cdots D_{i_k} \right).$$

■

Si A es un anillo de característica p, entonces una derivación ordinaria de A es cero sobre el subanillo A^p, pero las derivaciones de Hasse-Schmidt no necesariamente se anulan sobre A^p: Si la sucesión $\underline{D} = (D_0, D_1, D_2, \dots)$ es una derivación de Hasse-Schmidt de longitud $m \geq p$, entonces de la igualdad

$$E_t(a^p) = [E_t \text{ hom.}k\text{–álg.}] = E_t(a)^p = a^p + D_1(a)^p t^p + \cdots$$

obtenemos

$$D_p(a^p) = D_1(a)^p;$$

y en general,

$$D_{p^r}(a^{p^r}) = D_1(a)^{p^r}.$$

Definición I–D.6 ■ Diremos que $\underline{D} \in HS_k(A)$ es iterativa si satisface:

$$D_i \circ D_j = \binom{i+j}{i} D_{i+j} \quad \forall i, j.$$

Lema I–D.7 ■ La definición anterior es equivalente a exigir que el siguiente diagrama sea conmutativo:

$$\begin{array}{ccc} A[[t]] & \xrightarrow{E_u} & A[[t,u]] \\ E_t \uparrow & & \uparrow \\ A & \xrightarrow{E_{t+u}} & A[[t+u]] \end{array}$$

donde

$$E_t(a) = \sum_{\nu} t^{\nu} D_{\nu}(a),$$

$$E_u(\sum_{\nu} t^{\nu} a_{\nu}) = \sum_{\nu} t^{\nu} E_u(a_{\nu})$$

y la flecha vertical derecha es la inclusión.

Demostración. Efectivamente:

$$\begin{aligned} E_u(E_t(a)) &= E_u(\sum_{\nu} t^{\nu} D_{\nu}(a)) = \sum_{\nu} t^{\nu} E_u(D_{\nu}(a)) = \\ &= \sum_{\nu} t^{\nu} \sum_{\mu} u^{\mu} D_{\mu} D_{\nu}(a) = \end{aligned}$$

por otro lado

$$\begin{aligned} E_{t+u}(a) &= \sum_{\lambda} (t+u)^{\lambda} D_{\lambda}(a) = \\ &= \sum_{\lambda} (\sum_{\nu+\mu=\lambda} \binom{\nu+\mu}{\nu} t^{\nu} u^{\mu}) D_{\lambda}(a) = \\ &= \sum_{\nu} t^{\nu} \sum_{\mu} u^{\mu} \binom{\nu+\mu}{\nu} D_{\nu+\mu}(a). \end{aligned}$$

■

Definición I–D.8 ■ Diremos que las derivaciones de Hasse-Schmidt $\underline{D} = (D_0, D_1, D_2, \dots)$ y $\underline{D'} = (D'_0, D'_1, D'_2, \dots)$ conmutan si sus componentes D_i y D'_j conmutan para cada par (i,j).

Notas I–D.9 ■ Se verifican las siguientes propiedades:

1. Si las derivaciones de Hasse-Schmidt $\underline{D}$ y $\underline{D'}$ son iterativas y

conmutan, entonces su producto $\underline{D} \cdot \underline{D'}$ es de nuevo iterativa: puesto que

$$(E_u E'_u) \circ (E_t E'_t) = E_u E_t E'_u E'_t = E_{t+u} E'_{t+u}$$

donde todas las aplicaciones se ven como automorfismos de $A[[t, u]]$ que dejan t, u invariantes.

2. Si A contiene al cuerpo $\mathbb{Q}$, entonces una derivación de Hasse-Schmidt iterativa satisface

$$D_n = \frac{D_1^n}{n!}$$

y por lo tanto está determinada solamente por D_1. En efecto, por inducción en n:
Para $n = 1$: $D_1 = \frac{D_1^1}{1!} = D_1$
Supongamos cierto para $n - 1$, veamos si es cierto para n:

$$D_1^n = D_1 \circ D_1^{n-1}$$

entonces, aplicando hipótesis de inducción:

$$\begin{aligned} D_1^n &= D_1((n-1)!D_{n-1}) = (n-1)!D_1 \circ D_{n-1} = [\underline{D} \text{ es iterativa}] = \\ &= (n-1)! \begin{pmatrix} 1+n-1 \\ 1 \end{pmatrix} D_{1+n-1} = n!D_n \end{aligned}$$

luego $D_n = \dfrac{D_1^n}{n!}$.

3. Además, para $D \in Der_k(A)$ ($\mathbb{Q} \subset A$) se ve trivialmente que $(1, D, \frac{D^2}{2!}, \frac{D^3}{3!}, \ldots)$ es una derivación de Hasse-Schmidt iterativa.

4. Si A tiene característica p, entonces para una derivación de Hasse-Schmidt iterativa $\underline{D} = (D_0, D_1, D_2, \ldots)$, se tiene que

$$D_i = \frac{D_1^i}{i!} \quad \text{para } i < p$$

y $D_1^p = 0$ (ya que $D_1^p = p!D_p = 0$).

Por tanto, no podemos esperar extender cualquier derivación a una derivación de Hasse-Schmidt iterativa, incluso si A es cuerpo.

Notación I–D.10 ■ Utilizaremos la siguiente notación para manejar n–uplas: Sean $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$. Entonces

1. $|\alpha| = \alpha_1 + \cdots + \alpha_n$.
2. $\underline{X} = (X_1, \ldots, X_n)$.
3. Si $\underline{T} = (T_1, \ldots T_n)$ entonces $\underline{X} + \underline{T} = (X_1 + T_1, \ldots, X_n + T_n)$.
4. $\underline{X}^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$.
5. $\underline{1} = (1, \ldots, 1) \in \mathbb{N}^n$.
6. En $\mathbb{N}^n$ definiremos el siguiente orden (parcial):
$$\alpha \geq \beta \text{ significa } \alpha_1 \geq \beta_1, \ldots, \alpha_n \geq \beta_n,$$
7. $\alpha < \beta$ si $\alpha \leq \beta$ y $\alpha \neq \beta$
8. $\alpha! = \alpha_1! \cdots \alpha_n!$
9. $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \cdots \begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix} \quad \forall \alpha, \beta \in \mathbb{N}^n$.
10. Un elemento genérico de $k[[\underline{X}]]$ será de la forma
$$\sum_{\alpha \in \mathbb{N}^n} \lambda_\alpha \underline{X}^\alpha,$$
11. Un elemento genérico de $k[\underline{X}]$ será de la forma
$$\sum_{\alpha \in I} \lambda_\alpha \underline{X}^\alpha,$$
donde I es un subconjunto finito de $\mathbb{N}^n$.
12. $\left(\frac{\partial}{\partial \underline{X}}\right)^\alpha = \left(\frac{\partial}{\partial X_1}\right)^{\alpha_1} \cdots \left(\frac{\partial}{\partial X_n}\right)^{\alpha_n}$.

Proposición I–D.11 ■ **(Desarrollo de Taylor)** *(ver [MV69])* Sea $A = k[\underline{X}]$ ó $A = k[[\underline{X}]]$. Sean $\underline{T} = (T_1, \ldots, T_n)$ otra indeterminada y

$$f(\underline{X}) = \sum_{\alpha \in \mathbb{N}^n} \lambda_\alpha \underline{X}^\alpha \in A.$$

Definimos $\Delta^{(\alpha)}$ por:

$$f(\underline{X} + \underline{T}) = \sum_{\alpha \in \mathbb{N}^n} \Delta^{(\alpha)}(f(\underline{X}))\underline{T}^\alpha,$$

entonces se tiene que

1. $\Delta^{(\alpha)}$ son k-lineales e I–continuas.
2. $$\Delta^{(\alpha)}(\underline{X}^\beta) = \begin{cases} 0 & \text{si } \beta \ngeq \alpha \\ \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \underline{X}^{\beta-\alpha} & \text{si } \beta \geq \alpha \end{cases}$$
3. $\Delta^{(\alpha_1,\ldots,\alpha_n)} = \Delta^{(\alpha_1,0,\ldots,0)} \circ \Delta^{(0,\alpha_2,\ldots,0)} \circ \cdots \circ \Delta^{(0,\ldots,0,\alpha_n)}$ y además los $\Delta^{(0,\ldots,\alpha_j,\ldots,0)}$ conmutan para todo $j = 1, \ldots, n$.
4. $\Delta^{(0,\ldots,\overset{(j)}{1},\ldots,0)} = \frac{\partial}{\partial X_j}$.
5. $\alpha! \Delta^{(\alpha)} = (\frac{\partial}{\partial X_1})^{\alpha_1} \cdots (\frac{\partial}{\partial X_n})^{\alpha_n}$.
6. $\Delta^{(\alpha)} \circ \Delta^{(\beta)} = \begin{pmatrix} \alpha + \beta \\ \alpha \end{pmatrix} \Delta^{(\alpha+\beta)}$.
7. $\Delta^{(\alpha)}(f \cdot g) = \sum_{\beta+\sigma=\alpha} \Delta^{(\beta)}(f)\Delta^{(\sigma)}(g)$.
8. Para todo $j = 1, \ldots, n$ y $i \geq 0$ notaremos $\Delta^{(0,\ldots,\overset{(j)}{i},\ldots,0)} = \Delta^j_i$. Entonces

   $$\underline{\Delta}^j = (1_A, \Delta^j_1, \Delta^j_2, \ldots) \in HS_k(A)$$

   para $j = 1, \ldots, n$ y además son iterativas. Por último también se verifica que $i!\Delta^j_i = (\Delta^j_1)^i$, para todo $j = 1, \ldots, n$ y para todo $i \geq 0$.

Demostración.

1. Trivial tal como se han definido las $\Delta^{(\alpha)}$.

2.

$$\begin{aligned}
&(X_1+T_1)^{\beta_1}\cdots(X_n+T_n)^{\beta_n}=\\
&=\left(\sum_{j_1=0}^{\beta_1}\binom{\beta_1}{j_1}X_1^{\beta_1-j_1}T_1^{j_1}\right)\cdots\left(\sum_{j_n=0}^{\beta_n}\binom{\beta_n}{j_n}X_n^{\beta_n-j_n}T_n^{j_n}\right)=\\
&=\sum_{j_1=0}^{\beta_1}\cdots\sum_{j_n=0}^{\beta_n}\binom{\beta_1}{j_1}\cdots\binom{\beta_n}{j_n}X_1^{\beta_1-j_1}\cdots X_n^{\beta_n-j_n}T_1^{j_1}\cdots T_n^{j_n},
\end{aligned}$$

luego

$$\Delta^{(\alpha)}(\underline{X}^{\beta})=\begin{cases}0 & \text{si } \exists j\mid \alpha_j>\beta_j\\ \binom{\beta}{\alpha}\underline{X}^{\beta-\alpha} & \text{si } \alpha\le\beta\end{cases}$$

A partir de ahora, basta ver que las propiedades se verifican para los monomios, puesto que las aplicaciones $\Delta^{(\alpha)}$ son k-lineales e I-continuas.

3. Aplicando 2 se tiene trivialmente.

4.

$$\begin{aligned}
\Delta^{((0,\ldots,\overset{(j)}{1},\ldots,0))}(\underline{X}^{\beta}) &=\begin{cases}0 & \text{si } 1>\beta_j\\ \binom{\beta_j}{1}X_1^{\beta_1}\cdots X_j^{\beta_j-1}\cdots X_n^{\beta_n} & \text{si } 1\le\beta_j\end{cases}=\\
&=\frac{\partial}{\partial X_j}(\underline{X}^{\beta}).
\end{aligned}$$

5.

$$\alpha!\Delta^{(\alpha)}(\underline{X}^{\beta})=\alpha!\begin{cases}0 & \text{si } \exists j\mid \alpha_j>\beta_j\\ \binom{\beta}{\alpha}\underline{X}^{\beta-\alpha} & \text{si } \alpha\le\beta\end{cases}$$

y por otro lado

$$\left(\frac{\partial}{\partial X_1}\right)^{\alpha_1}\cdots\left(\frac{\partial}{\partial X_n}\right)^{\alpha_n}(\underline{X}^{\beta})=\begin{cases}0 & \text{si } \exists j\mid \alpha_j>\beta_j\\ \alpha!\binom{\beta}{\alpha}\underline{X}^{\beta-\alpha} & \text{si } \alpha\le\beta\end{cases}$$

6.

$$(\Delta^{(\alpha)} \circ \Delta^{(\beta)})(\underline{X}^{\sigma}) = \Delta^{(\alpha)}\left(\begin{cases} 0 & \text{si } \exists j \mid \beta_j > \sigma_j \\ \binom{\sigma}{\beta}\underline{X}^{\sigma-\beta} & \text{si } \beta \leq \sigma \end{cases}\right) =$$

$$= \begin{cases} 0 & \text{si } \exists j \mid \beta_j > \sigma_j \\ 0 & \text{si } \exists j \mid \alpha_j > \sigma_j - \beta_j \\ \binom{\sigma}{\beta}\binom{\sigma-\beta}{\alpha}\underline{X}^{\sigma-\beta-\alpha} & \text{si } \alpha \leq \sigma - \beta \end{cases} =$$

$$= \begin{cases} 0 & \text{si } \exists j \mid \alpha_j + \beta_j > \sigma_j \\ \binom{\sigma}{\beta}\binom{\sigma-\beta}{\alpha}\underline{X}^{\sigma-\beta-\alpha} & \text{si } \alpha + \beta \leq \sigma \end{cases}$$

por otro lado

$$\binom{\alpha+\beta}{\alpha}\Delta^{(\alpha+\beta)}(\underline{X}^{\sigma}) = \binom{\alpha+\beta}{\alpha}\begin{cases} 0 & \text{si } \exists j \mid \alpha_j + \beta_j > \sigma_j \\ \binom{\sigma}{\alpha+\beta}\underline{X}^{\sigma-\alpha-\beta} & \text{si } \alpha + \beta \leq \sigma \end{cases}$$

y se tiene que

$$\binom{\sigma}{\beta}\binom{\sigma-\beta}{\alpha} = \binom{\alpha+\beta}{\alpha}\binom{\sigma}{\alpha+\beta}.$$

7.

$$\Delta^{(\alpha)}(\underline{X}^{\rho} \cdot \underline{X}^{\mu}) = \Delta^{(\alpha)}(\underline{X}^{\rho+\mu}) = \begin{cases} 0 & \text{si } \exists j \mid \alpha_j > \rho_j + \mu_j \\ \binom{\rho+\mu}{\alpha}\underline{X}^{\sigma+\mu-\alpha} & \text{si } \alpha \leq \rho + \mu \end{cases}$$

por otro lado

$$\sum_{\beta+\sigma=\alpha} \Delta^{(\beta)}(\underline{X}^{\rho}) \cdot \Delta^{(\sigma)}(\underline{X}^{\mu}) =$$

$$= \sum_{\beta+\sigma=\alpha} \begin{cases} \binom{\rho}{\beta}\binom{\mu}{\sigma}\underline{X}^{\rho-\beta}\underline{X}^{\mu-\sigma} & \text{si } \beta \leq \rho \text{ y } \sigma \leq \mu \\ 0 & \text{en otro caso} \end{cases} =$$

$$= \sum_{\beta+\sigma=\alpha} \begin{cases} \binom{\rho}{\beta}\binom{\mu}{\sigma}\underline{X}^{\rho+\mu-\alpha} & \text{si } \beta + \sigma \leq \rho + \mu \\ 0 & \text{en otro caso} \end{cases}$$

para que sean iguales, necesitamos el siguiente

Aserto:

$$\sum_{\beta+\sigma=\alpha} \binom{\rho}{\beta}\binom{\mu}{\sigma} = \binom{\rho+\mu}{\alpha}.$$

Demostración del Aserto. Para el caso $n = 1$, se tiene que:

$$(1+X)^{\rho+\mu} = \sum_{k=0}^{\rho+\mu} \binom{\rho+\mu}{k} X^k$$

y como

$$(1+X)^{\rho+\mu} = (1+X)^{\rho}(1+X)^{\mu} = (\sum_{\beta=0}^{\rho} \binom{\rho}{\beta} X^{\beta})(\sum_{\sigma=0}^{\mu} \binom{\mu}{\sigma} X^{\sigma})$$

igualando los coeficientes de X^{α} en ambas expresiones se tiene lo pedido. Para $n > 1$, el resultado se sigue de:

$$\sum_{\substack{\beta_j+\sigma_j=\alpha_j \\ 1\le j\le n}} \binom{\rho_1}{\beta_1}\binom{\mu_1}{\sigma_1}\cdots\binom{\rho_n}{\beta_n}\binom{\mu_n}{\sigma_n} = \prod_{1\le j\le n} \sum_{\beta_j+\sigma_j=\alpha_j} \binom{\rho_j}{\beta_j}\binom{\mu_j}{\sigma_j}$$

luego aplicando el caso $n = 1$, se tiene lo pedido. ∎

8. Para todo $j = 1, \ldots, n$ y $i \geq 0$,se verifica

$$\Delta_i^j(X_k^l) = \begin{cases} 0 & \text{si } i > l \text{ o } k \neq j \\ \binom{l}{i} X_k^{l-i} & \text{si } k = j,\ i \leq l \end{cases}.$$

Además, por (4) sabemos que Δ_1^j es derivación, y por (7) se cumple la condición para el producto de dos elementos, luego $\underline{\Delta}^j \in HS_k(A)$ para $j = 1, \ldots, n$. Además, dichas derivaciones son iterativas, (por (6)). Veamos, por último, que

$$i!\Delta_i^j = (\Delta_1^j)^i, \quad \forall j = 1, \ldots, n; \ i \geq 0,$$

por inducción en i:

Para $i = 1$: $1!\Delta_1^j = (\Delta_1^j)^1$

Supongamos cierto para $i-1$, veamos si es cierto para i: Utilizando que

$$(\Delta_1^j)^i = \Delta_1^j \circ (\Delta_1^j)^{i-1}$$

se tiene, aplicando hipótesis de inducción, que

$$\begin{aligned}(\Delta_1^j)^i &= \Delta_1^j\left((i-1)!\Delta_{i-1}^j\right) = (i-1)!\Delta_1^j \circ \Delta_{i-1}^j = [\Delta_i^j \text{ iterativas}] = \\ &= (i-1)!\binom{i}{1}\Delta_i^j = i!\Delta_i^j.\end{aligned}$$

■

Nota I–D.12 ■ Una forma sencilla de obtener nuevas derivaciones de Hasse- Schmidt es la siguiente: Sea t' un elemento de $A[[t]]$ sin término constante y $\underline{D}$ una derivación de Hasse-Schmidt de A. El homomorfismo:

$$E_{t'} : A \longrightarrow A[[t]]$$

$$E_{t'}(a) = \sum_{n=0}^{\infty} t'^n D_n(a)$$

se puede extender de manera única a un automorfismo de $A[[t]]$ de manera análoga a I–D.4 es decir:

$$E_{t'}(\sum_{\nu} a_\nu t^\nu) = \sum_{\nu} E_{t'}(a_\nu)t^\nu.$$

Como $E_{t'}$ es un automorfismo de $A[[t]]$ que satisface $E_{t'}(a) \equiv a \pmod{t'}$, corresponde a una nueva derivación de Hasse-Schmidt $\underline{D}'$.

Ejemplo I–D.13 ■ Dados $\underline{D} = (1, D_1, D_2, \ldots)$ y $t' = xt$, entonces $E_{t'} : A \longrightarrow A[[t]]$ definida por:

$$E_{t'}(a) = \sum_{n=0}^{\infty} t'^n D_n(a) = \sum_{n=0}^{\infty} (xt)^n D_n(a) = \sum_{n=0}^{\infty} t^n x^n D_n(a)$$

Entonces $\underline{D}' = (1, xD_1, x^2D_2, \ldots)$ con $x \in A$ es una derivación de Hasse-Schmidt.

Proposición I–D.14 ■ Si $\underline{D} = (D_0, D_1, \ldots) \in HS_k(A)$, entonces para todo i, las D_i son I–continuas, para todo I ideal de A.

Demostración. Probaremos que

$$D_i(I^n) \subset I^{n-i} \quad \forall i,\ \forall n \geq i$$

por inducción en i:

Para $i = 0$, $D_0 = 1_A$, luego es trivial.

Supongamos cierto para todo $j < i$, veamos si es cierto para i: Hacemos ahora inducción en $n \geq i$:

Para $n = i$: $D_i(I^i) \subseteq I^0 = (1) = A$.

Supongamos cierto hasta $n-1$, veámoslo para n: Por ser los D_i endomorfismos aditivos, basta probarlo para $\lambda a_1 \cdots a_n \in I^n$, $(\lambda \in A, a_i \in I)$.

$$\begin{aligned} D_i(\lambda a_1 \cdots a_n) &= \sum_{l+k=i} D_l(\lambda a_1 \cdots a_{n-1}) D_k(a_n) = \\ &= D_i(\lambda a_1 \cdots a_n) \cdot a_n + \lambda a_1 \cdots a_{n-1} D_i(a_n) + \\ &+ \sum_{\substack{l+k=i \\ 1 \leq k,l \leq i-1}} D_l(\lambda a_1 \cdots a_{n-1}) D_k(a_n) \in I^{n-i} \end{aligned}$$

puesto que:

- como $n > i$, $n-1 \geq i$ y aplicando hipótesis de inducción en n, se tiene que
$$D_i(\lambda a_1 \cdots a_{n-1}) \in I^{n-1-i};$$
además $a_n \in I$, por lo tanto $D_i(\lambda a_1 \cdots a_{n-1}) a_n \in I^{n-i}$.
- $\lambda a_1 \cdots a_{n-1} \in I^{n-1}$ y $D_i(a_n) \in A$, por tanto se tiene que
$$\lambda a_1 \cdots a_{n-1} D_i(a_n) \in I^{n-1} \subseteq I^{n-i}.$$
- Por último, como $n-1 \geq i > l$, aplicando hipótesis de inducción en i tenemos
$$D_l(\lambda a_1 \cdots a_{n-1}) \in I^{n-1-l};$$

además $D_k(a_n) \in A$, por lo tanto

$$\sum_{\substack{l+k=i \\ 1\leq k,l\leq i-1}} D_l(\lambda a_1 \cdot \cdot \cdot a_{n-1})D_k(a_n) \in I^{n-1-l} = I^{n-(l+1)} \subseteq I^{n-i}$$

(pues $l + 1 \leq i$).

Por tanto, D_i es I-continua. ■

Proposición I–D.15 ■ Si $\underline{D} = (D_0, D_1, \dots) \in HS_k(A)$, entonces existe un única extensión $\hat{\underline{D}} \in HS_k(\hat{A})$, (siendo $\hat{A}$ el completado de A para la topología I–ádica).

Demostración. Si $\underline{D} = (D_0, D_1, \dots) \in HS_k(A)$, por la proposición anterior sabemos que D_i son I–continuas para todo i. Luego existe una única extensión

$$\hat{\underline{D}} = (\hat{D}_0, \hat{D}_1, \dots),$$

donde $\hat{D}_i : \hat{A} \longrightarrow \hat{A}$ son las extensiones al completado de las funciones I–continuas D_i, de la siguiente manera: Si $a \in \hat{A}$, existe (a_n) de Cauchy en A con límite a. Entonces definimos

$$\hat{D}_i(a) = \lim D_i(a_n).$$

Veamos que $\hat{\underline{D}} \in HS_k(\hat{A})$: Sea $a \cdot b \in \hat{A}$, entonces existe $(a_n) \in A$ tal que $(a_n) \to a$ y existe $(b_n) \in A$ tal que $b_n \to b$; luego

$$a_n \cdot b_n \to a \cdot b.$$

Por tanto

$$\hat{D}_i(a \cdot b) = \lim D_i(a_n \cdot b_n) = \lim \sum_{j+k=i} D_j(a_n)D_k(b_n) = \sum_{j+k=i} \hat{D}_j(a)\hat{D}_k(b).$$

■

I–E Derivaciones integrables

En esta sección recordamos la noción de derivación integrable y vemos que en el caso de la característica positiva, no toda derivación lo es.

Definición I–E.1 ■ Sea k un anillo, A una k–álgebra y $D \in Der_k(A)$. Diremos que D es integrable sobre k, si existe una extensión $\underline{D} \in HS_k(A)$ con $\underline{D} = (D_0, D, D_2, \ldots)$. Diremos que $\underline{D}$ es una integral de D.

Sea $Ider_k(A) = \{D \in Der_k(A) \mid D \text{ es integrable sobre } k\}$.

Lema I–E.2 ■ $Ider_k(A) \subset Der_k(A)$ es un A–submódulo.

Demostración.

1. Veamos que es subgrupo (aditivo) de $Der_k(A)$.

   - Sean $\underline{D}, \underline{D}'$ unas integrales de $D, D' \in Ider_k(A)$. Entonces sabemos que

     $$\underline{D} \circ \underline{D}' = (1,\ D + D',\ \ldots) \in HS_k(A),$$

     por lo tanto $D + D' \in Der_k(A)$ es además integrable.

   - Sea $\underline{D}$ una integral de $D \in Ider_k(A)$. Entonces sabemos que

     $$\underline{D}^{-1} = (1,\ -D,\ \ldots) \in HS_k(A),$$

     por lo tanto $-D \in Der_k(A)$ es además integrable. Luego $-D \in Ider_k(A)$ es el elemento inverso de D.

2. $Ider_k(A)$ es cerrado respecto a la multiplicación por elementos de A: Sean $D \in Ider_k(A)$ y $a \in A$. Sea $\underline{D}$ una integral de D, o sea,

$$\underline{D} = (1,\ D,\ D_2,\ \ldots).$$

Por el ejemplo I–D.13, sabemos que la sucesión

$$(1,\ aD,\ a^2D_2,\ \ldots)$$

es una derivación de Hasse-Schmidt. Luego aD es integrable sobre k.

■

Si A contiene al conjunto de los números racionales, $\mathbb{Q}$, es fácil ver que todas las derivaciones son integrables. Tambien es cierto si $A|k$ es 0–lisa, o si A es un cuerpo de cualquier característica (ver corolario del teorema 6 de [Mat82], y [Mol79]). Pero, en general, existen derivaciones no integrables:

Ejemplo I–E.3 ■ Sea k anillo de característica p y $A = \dfrac{k[X]}{(X^p)}$. Sean $x = \overline{X}$, y $D \in Der_k(A)$ tal que $D(x) = 1$ (D es la inducida por $\frac{\partial}{\partial X}$ de $k[X]$). Si D fuese integrable tendríamos:

$$0 = E_t(x^p) = E_t(x)^p = (x + t + \cdots)^p = t^p + \cdots$$

lo que es una contradicción. Por lo tanto D no es integrable;

$$Ider_k(A) \subsetneq Der_k(A).$$

Ejemplo I–E.4 ■ Sea k anillo de característica 2 y $A = \dfrac{k[X]}{(X^2)}$. Sean $x = \overline{X}$ y $D \in Der_k(A)$ la inducida por $\dfrac{\partial}{\partial X}$ de $k[X]$ (luego $D(x) = 1$). Supongamos que D es integrable, es decir, existe $(1_A, D, D_2, \dots) \in HS(A)$. Entonces

$$\begin{aligned} 0 &= D_2(x^2) = xD_2(x) + D_1(x)D_1(x) + D_2(x)x = \\ &= 2xD_2(x) + (D_1(x))^2 = 1. \end{aligned}$$

Luego no puede existir una derivación de Hasse-Schmidt que tenga a D en la primera componente.

Nota I–E.5 ■ Si E_t y E'_t corresponden a $\underline{D}$ y $\underline{D}'$ respectivamente, y si tomamos $s = t^n$ para algún $n > 1$, entonces $E_t \circ E'_s$ corresponde a una derivación de Hasse-Schmidt de la forma $(1, D_1, \dots, D_{n-1}, D_n + D'_1, \dots)$. En efecto:

$$\begin{aligned} E_t \circ E'_s(a) &= E_t(\sum_{i=0}^{\infty} s^i D'_i(a)) = \\ &= \sum_{i=0}^{\infty} t^{ni} E_t(D'_i(a)) = \\ &= \sum_{i=0}^{\infty} t^{ni} \sum_{j=0}^{\infty} t^j D_j \circ D'_i(a) = \\ &= a + D_1(a)t + \cdots + D_{n-1}(a)t^{n-1} + (D_n(a) + D'_1(a))t^n + \cdots \end{aligned}$$

Por tanto, una derivación integrable tiene muchas integrales.

I–F Operadores diferenciales lineales

En esta sección introducimos la noción de operador diferencial lineal sobre una k-álgebra. La referencia básica utilizada es [GD67], donde se presenta una definición recursiva, respecto del orden, de los operadores diferenciales lineales.

Definición I–F.1 ■ *(Véase [GD67],* §16, 16.8*)*. Sea A una k–álgebra. Para cada $i \geq 0$, definimos inductivamente el subconjunto $\mathcal{D}^{(i)}_{A/k} \subseteq End_k(A)$ como sigue:

$$\mathcal{D}^{(0)}_{A/k} := A \subseteq End_k(A)$$

$$\mathcal{D}_{A/k}^{(i+1)} := \{\varphi \in End_k(A) \mid [\varphi, a] \in \mathcal{D}_{A/k}^{(i)}, \quad \forall a \in A\}$$

Lema I-F.2 ■ $\left(\mathcal{D}_{A/k}^{(i)}\right)_{i\geq 0}$ es una sucesión creciente de (A, A)-bimódulos de $End_k(A)$ que satisfacen:

1. $\mathcal{D}_{A/k}^{(1)} = A \oplus Der_k(A)$.
2. $\mathcal{D}_{A/k}^{(i)} \circ \mathcal{D}_{A/k}^{(j)} \subset \mathcal{D}_{A/k}^{(i+j)}$.
3. Si $P \in \mathcal{D}_{A/k}^{(i)}$, $Q \in \mathcal{D}_{A/k}^{(j)}$, entonces $[P, Q] \in \mathcal{D}_{A/k}^{(i+j-1)}$.

Demostración. Veamos primero que para todo $i \geq 0$

$$\mathcal{D}_{A/k}^{(i)} \subseteq \mathcal{D}_{A/k}^{(i+1)}$$

por inducción en i:

Para $i = 0$: Sea $\lambda_a \in \mathcal{D}_{A/k}^{(0)}$ (es decir, $\lambda_a(x) = ax$ para todo $x \in A$). Veamos que $\lambda_a \in \mathcal{D}_{A/k}^{(1)}$:

$$[\lambda_a, b](c) = \lambda_a(bc) - b\lambda_a(c) = abc - bac = 0 \quad \forall c \in A$$

entonces

$$[\lambda_a, b] \in \mathcal{D}_{A/k}^{(0)},$$

luego

$$\lambda_a \in \mathcal{D}_{A/k}^{(1)}.$$

Supongamos la propiedad cierta para $i - 1$, y veamos si es cierta para i: Sea $\varphi \in \mathcal{D}_{A/k}^{(i)}$, entonces

$$[\varphi, a] \in \mathcal{D}_{A/k}^{(i-1)} \subseteq \mathcal{D}_{A/k}^{(i)} \quad \forall a \in A \text{ (aplicando hipótesis de inducción).}$$

por tanto $\varphi \in \mathcal{D}_{A/k}^{(i+1)}$.

1. $\mathcal{D}_{A/k}^{(1)} = A \oplus Der_k(A)$: Sea $P \in \mathcal{D}_{A/k}^{(1)}$, entonces

$$[P, a] = c \in A \quad \forall a \in A;$$

luego

$$[P, a](x) = cx \ \forall x \in A.$$

Por tanto

$$\forall a \in A \quad \exists c \in A \mid P(ax) - aP(x) = cx \quad \forall x \in A. \qquad \text{((I–F.1))}$$

Como $P \in \mathcal{D}^{(1)}_{A/k}$, entonces $P(1) \in A$. Veamos que $P - P(1)$ es una derivación:

$$(P - P(1))(ab) = P(ab) - P(1)ab = aP(b) + cb - P(1)ab$$

(por (I–F.1)) y

$$(P - P(1))(a)b + a(P - P(1))(b) = P(a)b - P(1)ab + aP(b) - P(1)ab.$$

Además se verifica que

$$P(a)b - P(1)ab = cb,$$

pues por (I–F.1) para $x = 1$ tenemos:

$$P(a) - aP(1) = c$$

por tanto

$$P(a)b - aP(1)b = cb, \ \ b \in A.$$

Luego

$$P - P(1) = \delta \quad \text{siendo } \delta \in Der_k(A),$$

o sea $P = a + \delta$ con $a \in A$, $\delta \in Der_k(A)$. Veamos que esta descomposición es única: Supongamos que existen $a' \in A$, $\delta' \in Der_k(A)$ tales que $P = a' + \delta'$, entonces:

$$P(1) = (a + \delta)(1) = a + 0 = a$$

y por otro lado

$$P(1) = (a' + \delta')(1) = a' + 0 = a',$$

por tanto $a = a'$. Luego $P = a + \delta = a + \delta'$ y entonces $\delta = \delta'$.

2. $\mathcal{D}^{(i)}_{A/k} \circ \mathcal{D}^{(j)}_{A/k} \subset \mathcal{D}^{(i+j)}_{A/k}$: Hacemos inducción sobre i: Para $i = 0$, se tiene que

$$\mathcal{D}^{(0)}_{A/k} \circ \mathcal{D}^{(j)}_{A/k} = A \circ \mathcal{D}^{(j)}_{A/k} \subset \mathcal{D}^{(0+j)}_{A/k}.$$

Supongamos cierto para $i - 1$, veamos si es cierto para i: Lo hacemos por inducción sobre j:
Para $j = 0$: $\mathcal{D}^{(i)}_{A/k} \circ \mathcal{D}^{(0)}_{A/k} = \mathcal{D}^{(i)}_{A/k} \circ A \subset \mathcal{D}^{(i+0)}_{A/k}$.
Supongamos cierto para $j - 1$, veamos si es cierto para j: Sea $P \in \mathcal{D}^{(i)}_{A/k}$, entonces

$$[P, a] \in \mathcal{D}^{(i-1)}_{A/k} \quad \forall a \in A,$$

además

$$[P, a](b) = P(ab) - aP(b) \quad \forall b \in A.$$

Análogamente, para $Q \in \mathcal{D}^{(j)}_{A/k}$ se tiene que

$$[Q, a] \in \mathcal{D}^{(j-1)}_{A/k} \quad \forall a \in A,$$

y

$$[Q, a](b) = Q(ab) - aQ(b) \quad \forall b \in A.$$

Entonces, dado $b \in A$:

$$\begin{aligned}
[P \circ Q, a](b) &= P \circ Q(ab) - aP \circ Q(b) = \\
&= P([Q, a](b) + aQ(b)) - aP(Q(b)) = \\
&= P([Q, a](b)) + P(aQ(b)) - aP(Q(b)) = \\
&= (P \circ [Q, a])(b) + [P, a](Q(b)) + aP(Q(b)) - aP(Q(b)) = \\
&= (P \circ [Q, a] + [P, a] \circ Q)(b).
\end{aligned}$$

Luego para todo $a \in A$

$$[P \circ Q, a] = P \circ [Q, a] + [P, a] \circ Q \in \mathcal{D}^{(i+j-1)}_{A/k}$$

puesto que $P \in \mathcal{D}^{(i)}_{A/k}$, $[Q, a] \in \mathcal{D}^{(j-1)}_{A/k}$, y aplicando hipótesis de inducción sobre j, se tiene que

$$P \circ [Q, a] \in \mathcal{D}^{(i+j-1)}_{A/k}.$$

Análogamente, se prueba por inducción sobre i, que

$$[P, a] \circ Q \in \mathcal{D}_{A/k}^{(i+j-1)};$$

por tanto para todo $a \in A$

$$[P \circ Q, a] \in \mathcal{D}_{A/k}^{(i+j-1)} \implies P \circ Q \in \mathcal{D}_{A/k}^{(i+j)}.$$

3. Si $P \in \mathcal{D}_{A/k}^{(i)}$, $Q \in \mathcal{D}_{A/k}^{(j)}$, entonces $[P, Q] \in \mathcal{D}_{A/k}^{(i+j-1)}$: Hacemos inducción sobre i:

   Para $i = 0$: Sea $P \in \mathcal{D}_{A/k}^{(0)} = A$, es decir, $P = \lambda_d$ con $d \in A$ y $Q \in \mathcal{D}_{A/k}^{(j)}$. Entonces para todo $a \in A$, se tiene que

   $$[Q, a] \in \mathcal{D}_{A/k}^{(j-1)}.$$

   Luego para todo $a, b \in A$

   $$[[Q, a], b] \in \mathcal{D}_{A/k}^{(j-2)}. \qquad \text{((I–F.2))}$$

   Veamos ahora que para todo $a \in A$

   $$[[P, Q], a] = -[[Q, a], P]:$$

   Sea $c \in A$. Se verifica que

   $$\begin{aligned} [[P, Q], a](c) &= [P, Q](ac) - a[P, Q](c) = \\ &= P(Q(ac)) - Q(P(ac)) - aP(Q(c) + aQ(P(c)) = \\ &= dQ(ac) - Q(dac) - adQ(c) + aQ(dc) = \\ &= d[Q, a](c) - [Q, a](dc) = \\ &= -[[Q, a], d](c), \end{aligned}$$

   luego usando (I–F.2),

   $$[[P, Q], a] \in \mathcal{D}_{A/k}^{(j-2)} \quad \forall a \in A$$

   y por tanto

   $$[P, Q] \in \mathcal{D}_{A/k}^{(j-1)} = \mathcal{D}_{A/k}^{(0+j-i)}.$$

   Supongamos cierto para $i-1$, veamos si es cierto para i: Lo hacemos por inducción sobre j:

Para $j = 0$: Sea $P \in \mathcal{D}^{(i)}_{A/k}$, entonces para todo $a, b \in A$

$$[[P, a], b] \in \mathcal{D}^{(i-2)}_{A/k} \qquad ((\text{I–F.3}))$$

y sea $Q \in \mathcal{D}^{(0)}_{A/k}$, es decir, $Q = \lambda_c$ con $c \in A$. Análogamente al caso anterior, se prueba que para todo $a \in A$

$$[[P, Q], a] = [[P, a], Q] \in \mathcal{D}^{(i-2)}_{A/k},$$

por (I–F.3), y por tanto

$$[P, Q] \in \mathcal{D}^{(i-1+0)}_{A/k}.$$

Supongamos el resultado cierto para $j-1$, y veámoslo para j: Sean $P \in \mathcal{D}^{(i)}_{A/k}$, $Q \in \mathcal{D}^{(j)}_{A/k}$. Entonces, para todo $a \in A$ se verifica que

$$[P, a] \in \mathcal{D}^{(i-1)}_{A/k}, \text{ y } [Q, a] \in \mathcal{D}^{(j-1)}_{A/k}.$$

Veamos que para todo $a \in A$

$$[[P, Q], a] = [[P, a], Q] + [P, [Q, a]] :$$

$$\begin{aligned}
[[P, Q], a]\,(b) &= [P, Q](ab) - a[P, Q](b) = \\
&= P(Q(ab)) - Q(P(ab)) - aP(Q(b)) + aQ(P(b)) = \\
&= P([Q, a](b)) + P(aQ(b)) - Q(P(ab)) - aP(Q(b)) + \\
&\quad + aQ(P(b)) = \\
&= P([Q, a](b)) + P(aQ(b)) - Q(P(ab)) - aP(Q(b)) + \\
&\quad + Q(aP(b)) - [Q, a](P(b)) = \\
&= [[P, a], Q]\,(b) + [P, [Q, a]]\,(b) \quad \forall b \in A,
\end{aligned}$$

puesto que

$$\begin{aligned}
[[P, a], Q]\,(b) &= [P, a](Q(b)) - Q([P, a](b)) = \\
&= P(aQ(b)) - aP(Q(b)) - Q(P(ab)) + Q(aP(b)).
\end{aligned}$$

Luego $\forall a \in A$ se tiene que

$$[[P, Q], a] \in \mathcal{D}^{(i+j-2)}_{A/k} :$$

ya que como $Q \in \mathcal{D}^{(j)}_{A/k}$ y $[P,a] \in \mathcal{D}^{(i-1)}_{A/k}$, aplicando hipótesis de inducción sobre i, se tiene que

$$[[P,a],Q] \in \mathcal{D}^{(i+j-2)}_{A/k}.$$

Análogamente se prueba, por inducción sobre j, que

$$[P,[Q,a]] \in \mathcal{D}^{(i+j-2)}_{A/k}.$$

Por tanto, se concluye que $[P,Q] \in \mathcal{D}^{(i+j-1)}_{A/k}$ (siendo $P \in \mathcal{D}^{(i)}_{A/k}$ y $Q \in \mathcal{D}^{(j)}_{A/k}$).

■

Proposición I–F.3 ■ Si $P \in \mathcal{D}_{A/k}$, entonces P es I–continua para la topología I–ádica para todo ideal $I \subseteq A$.

Demostración. Sea $P \in \mathcal{D}_{A/k}$. Entonces existe j tal que $P \in \mathcal{D}^{(j)}_{A/k}$. Si se cumple

$$P(I^{r+j}) \subset I^r \quad \forall r,$$

entonces P es I–continua para la topología I–ádica. Veámoslo por inducción sobre j:

Para $j = 0$: $P \in \mathcal{D}^{(0)}_{A/k} = A$, entonces $A \cdot I^r \subset I^r \quad \forall r$.

Supongamos cierto para j, veamos si es cierto para $j+1$: Sea $P \in \mathcal{D}^{(j+1)}_{A/k}$, veamos que para todo r

$$P(I^{r+j+1}) \subset I^r$$

y lo hacemos por inducción en r:

Para $r = 0$: $P(I^{j+1}) \subset I^0 = A$.

Supongamos cierto para $r-1$, veámoslo para r: Sea

$$a \in I^{r+j+1} = I \cdot I^{r+j},$$

entonces

$$a = \sum a_i b_i \text{ con } a_i \in I, b_i \in I^{r+j}.$$

Pero como P es k–lineal, podemos suponer $a = xy$ con $x \in I$, $y \in I^{r+j}$, entonces

$$P(a) = P(xy) = [P, x](y) + xP(y) \in I^r.$$

Y como $y \in I^{r+j}$, entonces $[P, x] \in \mathcal{D}^{(j)}_{A/k}$; aplicando hipótesis de inducción sobre j se tiene que

$$[P, x](y) \in I^r.$$

Además, como $P \in \mathcal{D}^{(j+1)}_{A/k}$, $y \in I^{r-1+j+1}$, aplicamos ahora hipótesis de inducción sobre r, y entonces $P(y) \in I^{r-1}$. Por último, como $x \in I$ se verifica que

$$xP(y) \in I^r.$$

Luego el operador P es I–continuo, para la topología I–ádica. ■

El siguiente resultado demuestra que toda derivación de Hasse-Schmidt es una sucesión de operadores diferenciales lineales.

Proposición I–F.4 ■ Si $\underline{D} = (D_0, D_1, D_2, \dots) \in HS_k(A)$, entonces $D_i \in \mathcal{D}^{(i)}_{A/k}$ $\forall i$.

Demostración. Por inducción sobre i:

Para $i = 0$: $D_0 = 1_A \in \mathcal{D}^{(0)}_{A/k}$.

Supongamos cierto para i, veamos si es cierto para $i+1$: Probaremos que $[D_{i+1}, a] \in \mathcal{D}^{(i)}_{A/k}$ para todo $a \in A$:

$$\begin{aligned}
[D_{i+1}, a](b) &= D_{i+1}(ab) - aD_{i+1}(b) = \\
&= \sum_{j+k=i+1} D_j(a)D_k(b) - aD_{i+1}(b) = \\
&= \left(\sum_{\substack{j+k=i+1 \\ k\neq i+1}} D_j(a)D_k \right)(b) \quad \text{con } b \in A.
\end{aligned}$$

Luego para todo $a \in A$

$$[D_{i+1}, a] = \sum_{\substack{j+k=i+1 \\ k\neq i+1}} D_j(a)D_k \in \mathcal{D}^{(i)}_{A/k},$$

puesto que aplicando hipótesis de inducción

$$D_k \in \mathcal{D}^{(k)}_{A/k} \subseteq \mathcal{D}^{(i)}_{A/k},$$

para $k = 0, \ldots, i$. Por lo tanto

$$D_{i+1} \in \mathcal{D}^{i+1}_{A/k}.$$

■

I–G Operadores diferenciales en el anillo de polinomios y en el anillo de series

En esta sección relacionamos los operadores diferenciales y las aplicaciones definidas a partir del desarrollo de Taylor en los casos del anillo de polinomios y del anillo de series (ver la proposición I–D.11).

■ Caso de una variable

Consideremos el conjunto $\{\Delta^{(\alpha)}\}_{\alpha\in\mathbb{N}}$, donde las $\Delta^{(\alpha)} = \Delta^1_\alpha$ definidas en la proposición I–D.11.

Lema I–G.1 ■ $\Delta^{(\alpha)} \in \mathcal{D}^{(\alpha)}_{A/k}$ para todo $\alpha \in \mathbb{N}$.

Demostración. Haremos inducción sobre α.

Para $\alpha = 0$: $\Delta^{(0)} = \Delta^1_0 = 1_A \in \mathcal{D}^{(0)}_{A/k}$.

Para $\alpha = 1$: por 4 de la proposición I–D.11, se tiene que

$$\Delta^{(1)} = \Delta_1^1 = \frac{\partial}{\partial X} \in Der_k(A) \subset \mathcal{D}^{(1)}_{A/k}.$$

Supongamos cierto para $\alpha - 1$, y veamos si es cierto para α: Basta probar que $[\Delta^{(\alpha)}, f] \in \mathcal{D}^{(\alpha-1)}_{A/k}$ para todo $f \in A$. Para todo $g \in A$, por 7 de la proposición I–D.11, se tiene que

$$[\Delta^{(\alpha)}, f](g) = \Delta^{(\alpha)}(f \cdot g) - f\Delta^{(\alpha)}(g) = \sum_{\beta+\sigma=\alpha} \Delta^{(\beta)}(f)\Delta^{(\sigma)}(g) - f\Delta^{(\alpha)}(g) = \sum_{\sigma=0}^{\alpha-1} \Delta^{(\alpha-\sigma)}(f)\Delta^{(\sigma)}(g).$$

Luego para todo $f \in A$, se tiene que

$$[\Delta^{(\alpha)}, f] = \sum_{\sigma=0}^{\alpha-1} \Delta^{(\alpha-\sigma)}(f)\Delta^{(\sigma)} \in \mathcal{D}^{(\alpha-1)}_{A/k},$$

aplicando la hipótesis de inducción y que $\Delta^{(\alpha-\sigma)}(f) \in A$ para todo $\sigma = 0, 1, \ldots, \alpha - 1$. ∎

Sea $P \in \mathcal{D}^{(n)}_{A/k}$, supongamos $P = \sum_{\alpha=0}^{n} a_\alpha \Delta^{(\alpha)}$, entonces los elementos a_α se pueden determinar de la siguiente manera:

$$P(1) = \sum_{\alpha=0}^{n} a_\alpha \Delta^{(\alpha)}(1) = a_0,$$

$$P(X) = \sum_{\alpha=0}^{n} a_\alpha \Delta^{(\alpha)}(X) = a_0\Delta^{(0)}(X) + a_1\Delta^{(1)}(X) = a_0 X + a_1,$$

luego

$$a_1 = P(X) - P(1)X.$$

$$P(X^2) = a_0\Delta^{(0)}(X^2) + a_1\Delta^{(1)}(X^2) + a_2\Delta^{(2)}(X^2) = a_0X^2 + 2a_1X + a_2$$

y por tanto

$$a_2 = P(X^2) - 2P(X)X + P(1)X^2.$$

En general, probaremos que

$$a_j = \sum_{i=0}^{j} (-1)^{j-1} \binom{j}{i} P(X^i)X^{j-i} \qquad j = 1, \ldots, n$$

Proposición I–G.2 ■ Si $P \in \mathcal{D}^{(n)}_{A/k}$, entonces

$$P = \sum_{\alpha=0}^{n} \left(\sum_{i=0}^{\alpha} (-1)^{\alpha-i} \binom{\alpha}{i} P(X^i) X^{\alpha-i} \right) \Delta^{(\alpha)}$$

Demostración. Probemos primero el siguiente

Aserto I: Sean $P, Q \in \mathcal{D}^{(n)}_{A/k}$ tales que $P(X^k) = Q(X^k)$ para todo $k = 0, \dots, n$. Entonces $P = Q$.

Demostración del Aserto I. Veámoslo en primer lugar en el caso $A = k[X]$. Podemos reducirnos a probar que si $R \in \mathcal{D}^{(n)}_{A/k}$ tal que $R(X^k) = 0$ para todo $k = 0, \dots, n$. Entonces $R = 0$ (ya que tomando $R = P - Q$ tendríamos el aserto).

Haremos inducción en n:

Para $n = 0$: Sea $R \in \mathcal{D}^{(0)}_{A/k} = A$ tal que $R(X^0) = R(1) = 0$ entonces trivialmente se tiene que $R = 0$.

Supongamos cierto para $n - 1$, veamos si es cierto para n: Sea $R \in \mathcal{D}^{(n)}_{A/k}$ tal que $R(X^k) = 0$ para todo $k = 0, \dots, n$. Es suficiente probar que

$$R(X^{n+l}) = 0$$

para todo $l \geq 1$. Veámoslo por inducción en l:

Para $l = 1$: $R(X^{n+1}) = R(X \cdot X^n) = [R, X](X^n) + XR(X^n) = 0$ puesto que:

- $R(X^n) = 0$
- $[R, X] \in \mathcal{D}^{(n-1)}_{A/k}$ y además para todo $k = 0, \dots, n-1$, se verifica que

$$[R, X](X^k) = R(X \cdot X^k) - XR(X^k) = 0.$$

Entonces podemos aplicar hipótesis de inducción en n y se tiene que $[R, X] = 0$

Supongamos cierto para $l-1$, veamos si es cierto para l:

$$R(X^{n+l}) = R(X \cdot X^{n+l-1}) = [R, X](X^{n+l-1}) + XR(X^{n+l-1}) = 0,$$

puesto que:

- $R(X^{n+l-1}) = 0$ por hipótesis de inducción en l.
- Análogamente al caso anterior, $[R, X] = 0$.

En segundo lugar, como los dos operadores $P, Q \in \mathcal{D}^{(n)}_{A/k}$ son continuos en $k[[X]]$, hemos probado que coinciden en $k[X]$, y $k[X]$ es denso en $k[[X]]$, luego los dos operadores coinciden en $k[[X]]$. ∎

Volvamos a la prueba de la proposición I–G.2. Como el segundo miembro de la igualdad pertenece a $\mathcal{D}^{(n)}_{A/k}$, (por el lema I–G.1); aplicando el aserto I, es suficiente probar que los dos operadores coinciden sobre las potencias X^k para todo $k = 0, \dots, n$. Ahora bien, para todo $0 \leq k \leq n$ se tiene que:

$$\begin{aligned}
&\sum_{\alpha=0}^{n}\left(\sum_{i=0}^{\alpha}(-1)^{\alpha-i}\binom{\alpha}{i}P(X^i)X^{\alpha-i}\right)\Delta^{(\alpha)}(X^k) = \\
&= \sum_{\alpha=0}^{k}\left(\sum_{i=0}^{\alpha}(-1)^{\alpha-i}\binom{\alpha}{i}P(X^i)X^{\alpha-i}\right)\binom{k}{\alpha}X^{k-\alpha} = \\
&= \sum_{\alpha=0}^{k}\left(\sum_{i=0}^{\alpha}(-1)^{\alpha-i}\binom{\alpha}{i}\binom{k}{\alpha}P(X^i)X^{k-i}\right) = \\
&= \sum_{i=0}^{k}\left(\sum_{\alpha=i}^{k}(-1)^{\alpha-i}\binom{\alpha}{i}\binom{k}{\alpha}\right)P(X^i)X^{k-i} = \\
&= \sum_{i=0}^{k-1}\left(\sum_{\alpha=i}^{k}(-1)^{\alpha-i}\binom{\alpha}{i}\binom{k}{\alpha}\right)P(X^i)X^{k-i} + P(X^k) = \\
&= P(X^k).
\end{aligned}$$

La última igualdad es cierta debido al siguiente:

Aserto II:

$$\sum_{\alpha=i}^{k}(-1)^{\alpha-i}\binom{\alpha}{i}\binom{k}{\alpha}=0$$

Demostración del Aserto II. Consideremos la función

$$f(x)=(x-1)^k=\sum_{\alpha=0}^{k}\binom{k}{\alpha}x^{\alpha}(-1)^{k-\alpha}$$

entonces $f^{i)}(x)=k(k-1)\cdot\cdot\cdot(k-i+1)(x-1)^{k-i}$ si $i\leq k-1$.

Por otro lado

$$f^{i)}(x)=\sum_{\alpha=i}^{k}\binom{k}{\alpha}(-1)^{k-\alpha}\alpha\cdot\cdot\cdot(\alpha-i+1)x^{\alpha-i},$$

entonces

$$\sum_{\alpha=i}^{k}(-1)^{k-\alpha}\alpha\cdot\cdot\cdot(\alpha-i+1)=f^{i)}(1)=0.$$

Basta tener en cuenta que, si llamamos S a la suma pedida, se tiene que:

$$\begin{aligned} S &= \frac{1}{(-1)^i i!}\sum_{\alpha=i}^{k}(-1)^{\alpha}\alpha\cdot\cdot\cdot(\alpha-i+1)\binom{k}{\alpha}= \\ &= \frac{(-1)^k}{(-1)^i i!}f^{i)}(1)=0. \end{aligned}$$

■

La prueba de este aserto concluye, pues, la demostración de la proposición I–G.2. ■

Como consecuencia de los dos resultados anteriores, hemos obtenido una A-base de $\mathcal{D}^{(n)}_{A/k}$:

Corolario I–G.3 ■ $\mathcal{D}^{(n)}_{A/k}=\left\{\sum_{\alpha=0}^{n}a_\alpha\Delta^{(\alpha)}\mid a_\alpha\in A\right\}$ y $\{\Delta^{(\alpha)}\}_{0\leq\alpha\leq n}$ es una A–base de $\mathcal{D}^{(n)}_{A/k}$.

Demostración.

"$\subseteq$" se tiene por la proposición I–G.2.

"$\supseteq$" se tiene por el lema I–G.1. ∎

Nota I–G.4 ∎ Si k es de característica 0, entonces

$$k = \{a \in A \mid \frac{\partial}{\partial X}(a) = 0\},$$

sin embargo, no es cierto en el caso de característica positiva, como vemos en el siguiente ejemplo:

Sea k un cuerpo de característica positiva. Entonces

$$\{a \in A \mid \frac{\partial}{\partial X}(a) = 0\} = \{\lambda_0 + \lambda_p X^p + \lambda_{2p} X^{2p} + \cdots\} = k[X^p] \neq k.$$

Nota I–G.5 ∎ En cualquier característica, lo que sí se verifica es:

$$\{a \in A \mid \Delta^{(\alpha)}(a) = 0 \ \forall \alpha \in \mathbb{N}\} = k.$$

En efecto: Supongamos que existe $p(X) \in k[X] \setminus k$ tal que para todo $\alpha \in \mathbb{N}$,

$$\Delta^{(\alpha)}(p(X)) = 0$$

Supongamos que $p(X) = \sum_{i \leq n} \lambda_i X^i$, entonces

$$\Delta^{(n)}(p(X)) = \sum_{i \geq n} \lambda_i \binom{i}{n} X^{i-n} = \lambda_n \binom{n}{n} = \lambda_n = 0,$$

y es una contradicción.

Como aplicación del corolario I–G.3, veamos cómo se puede expresar una derivación de Hasse-Schmidt $\underline{D} = (D_0, D_1, D_2, \ldots)$ en función de los operadores diferenciales $\Delta^{(\alpha)}$.

Proposición I-G.6 ■ Si $\underline{D} = (D_0, D_1, D_2, \dots) \in HS_k(A)$, entonces para todo $n \in \mathbb{N}$ se tiene que

$$D_n = \sum_{\alpha=0}^{n} \left\{ \sum_{i=0}^{\alpha} (-1)^{\alpha-i} \binom{\alpha}{i} \left(\sum_{j_1+\cdots+j_i=n} D_{j_1}(X) \cdots D_{j_i}(X) \right) X^{\alpha-i} \right\} \Delta^{(\alpha)}.$$

Demostración. Por la proposición I-F.4, $D_n \in \mathcal{D}^{(n)}_{A/k}$. Por tanto, aplicando la proposición I-G.2

$$D_n = \sum_{\alpha=0}^{n} \left(\sum_{i=0}^{\alpha} (-1)^{\alpha-i} \binom{\alpha}{i} D_n(X^i) X^{\alpha-i} \right) \Delta^{(\alpha)}. \qquad \text{((I-G.1))}$$

Se verifica que:

Aserto:

$$D_n(X^0) = D_n(1) = 0 \quad \forall n \geq 1,$$

$$D_n(X^i) = \sum_{j_1+\cdots+j_i=n} D_{j_1}(X) \cdots D_{j_i}(X) \quad \forall n, \ \forall 1 \leq i \leq n. \qquad \text{((I-G.2))}$$

Demostración del Aserto.

$$\begin{aligned} D_n(X^i) &= D_n(X^{i-1} \cdot X) = \\ &= \sum_{k_1+j_1=n} D_{k_1}(X^{i-1}) D_{j_1}(X) = \\ &= \sum_{k_1+j_1=n} \left(\sum_{k_2+j_2=k_1} D_{k_2}(X^{i-2}) D_{j_2}(X) \right) D_{j_1}(X) = \\ &= \sum_{k_2+j_2+j_1=n} D_{k_2}(X^{i-2}) D_{j_2}(X) D_{j_1}(X) = \\ &= \cdots\cdots\cdots = \\ &= \sum_{j_1+\cdots+j_i=n} D_{j_1}(X) \cdots D_{j_i}(X). \end{aligned}$$

■

Por tanto, sustituyendo (I-G.2) en (I-G.1) se deduce la igualdad requerida. ■

Caso de varias variables

En el caso de más de una variable, consideremos el conjunto $\{\Delta^{(\alpha)}\}_{\alpha\in\mathbb{N}^n}$ definido en la proposición I–D.11. Estimaremos el orden de $\Delta^{(\alpha)}$ como operador diferencial.

Lema I–G.7 ■ $\Delta^{(\alpha)} \in \mathcal{D}^{(|\alpha|)}_{A/k}$ para todo $\alpha \in \mathbb{N}^n$.

Demostración. Similar a la demostración del lema I–G.1. Haremos inducción sobre $|\alpha|$.

Para $|\alpha| = 0$: $\Delta^{(\alpha)} = 1_A \in \mathcal{D}^{(0)}_{A/k}$.

Para $|\alpha| = 1$: como $\alpha \in \mathbb{N}^n$, se tiene que $\alpha = (0,\ldots,\overset{(j)}{1},\ldots,0)$ para algún $j = 1,\ldots,n$. Además, por 4 de la proposición I–D.11, se tiene que

$$\Delta^{(0,\ldots,\overset{(j)}{1},\ldots,0)} = \frac{\partial}{\partial X_j} \in Der_k(A) \subset \mathcal{D}^{(1)}_{A/k}.$$

Supongamos cierto para todo $\gamma \in \mathbb{N}^n$ con $|\gamma| = 0, 1,\ldots, |\alpha|-1$, y veamos si es cierto para $|\gamma| = |\alpha|$: Basta probar que $[\Delta^{(\gamma)}, f] \in \mathcal{D}^{(|\alpha|-1)}_{A/k}$ para todo $f \in A$. Para todo $g \in A$, por 7 de la proposición I–D.11, se tiene que

$$\begin{aligned}[\Delta^{(\gamma)}, f](g) &= \Delta^{(\gamma)}(f \cdot g) - f\Delta^{(\gamma)}(g) = \sum_{\beta+\sigma=\gamma} \Delta^{(\beta)}(f)\Delta^{(\sigma)}(g) - f\Delta^{(\gamma)}(g) = \\ &= \sum_{\substack{\beta+\sigma=\gamma \\ |\beta|>0}} \Delta^{\beta}(f)\Delta^{\sigma}(g).\end{aligned}$$

Luego para todo $f \in A$, se tiene que

$$[\Delta^{(\gamma)}, f] = \sum_{\substack{\beta+\sigma=\gamma \\ |\beta|>0}} \Delta^{(\beta)}(f)\Delta^{(\sigma)} \in \mathcal{D}^{(|\alpha|-1)}_{A/k},$$

aplicando hipótesis de inducción (ya que como $|\beta| > 0$, entonces σ es tal que $|\sigma| < |\gamma| = |\alpha|$) y que $\Delta^{(\beta)}(f) \in A$. ■

Teorema I–G.8 ■ Sea $P \in \mathcal{D}^{(m)}_{A/k}$. Entonces

$$P = \sum_{\substack{\alpha \in \mathbb{N}^n \\ 0 \le |\alpha| \le m}} \left(\sum_{\beta \le \alpha} \binom{\alpha}{\beta} (-1)^{|\alpha-\beta|} P(\underline{X}^{\beta}) \underline{X}^{\alpha-\beta} \right) \Delta^{(\alpha)}$$

Demostración. Probemos en primer lugar el siguiente

Aserto I: Sean $P, Q \in \mathcal{D}^{(m)}_{A/k}$ tales que $P(\underline{X}^k) = Q(\underline{X}^k)$ para todo $k \in \mathbb{N}^n$ con $|k| = m$. Entonces $P = Q$.

Demostración del Aserto I. Veámoslo en primer lugar, en el caso $A = k[X_1, \dots, X_n]$. Basta probar que dado $R \in \mathcal{D}^{(m)}_{A/k}$ tal que $R(\underline{X}^k) = 0$ para todo $k \in \mathbb{N}^n$ con $0 \le |k| \le m$, entonces $R = 0$ (ya que tomando $R = P - Q$ tendríamos el aserto). Probémoslo por inducción en el orden m:

Para $m = 0$: Sea $R \in \mathcal{D}^{(0)}_{A/k} = A$ tal que $R(\underline{X}^0) = R(1) = 0$, y por tanto $R = 0$.

Supongamos cierto para todo $j \le m-1$, veamos si es cierto para m: Sea $R \in \mathcal{D}^{(m)}_{A/k}$ tal que $R(\underline{X}^k) = 0$ para todo $k \in \mathbb{N}^n$ con $|k| = m$. Es suficiente demostrar que

$$R(\underline{X}^{k+l}) = 0 \quad \forall l \in \mathbb{N}^n \text{ con } |l| \ge 1.$$

Veámoslo por inducción en $|l|$:

Para $|l| = 1$, l es de la forma $l = (0, \dots, \overset{(j)}{1}, \dots, 0)$, y se tiene que

$$R(\underline{X}^{k+l}) = R(\underline{X}^k \cdot \underline{X}^l) = [R, \underline{X}^l](\underline{X}^k) + \underline{X}^l R(\underline{X}^k) = 0$$

ya que

- $R(\underline{X}^k) = 0$
- $[R, \underline{X}^l] \in \mathcal{D}^{(m-1)}_{A/k}$ y además verifica que

$$[R, \underline{X}^l](\underline{X}^k) = R(\underline{X}^l \cdot \underline{X}^k) - \underline{X}^l R(\underline{X}^k) = 0, \ \forall k \in \mathbb{N}^n \text{ con } 0 \le |k| \le m-1$$

(pues $|l+k| \leq |l|+|k| \leq 1+m-1 = m$, luego $R(\underline{X}^{l+k}) = 0$). Entonces podemos aplicar hipótesis de inducción en m y se tiene que: $[R, \underline{X}^l] = 0$.

Supongamos cierto para $|l| - 1$, veamos si es cierto para $|l|$: Si $a \in \mathbb{N}^n$ con $|a| = 1$, entonces

$$R(\underline{X}^{k+l}) = R(\underline{X}^a \cdot \underline{X}^{k+l-a}) = [R, \underline{X}^a](\underline{X}^{k+l-a}) + \underline{X}^a R(\underline{X}^{k+l-a}) = 0,$$

ya que

- $R(\underline{X}^{k+l-a}) = 0$, aplicando hipótesis de inducción en $|l|$, puesto que

$$|l-a| = ||l| - |a|| = ||l| - 1| = |l| - 1.$$

- $[R, \underline{X}^a] \in \mathcal{D}^{(m-1)}_{A/k}$, y análogamente al caso $|l| = 1$, se tiene que

$$[R, \underline{X}^a](\underline{X}^k) = 0 \ \forall k \in \mathbb{N}^n \text{ con } 0 \leq |k| \leq m-1.$$

  Luego, aplicando la hipótesis de inducción en m, se tiene que $[R, \underline{X}^a] = 0$.

En segundo lugar, también es cierto en $A = k[[X_1, \ldots, X_n]]$, por verificarse en $k[X_1, \ldots, X_n]$ subconjunto denso en $k[[X_1, \ldots, X_n]]$, y por la continuidad. ∎

Volvamos a la prueba del teorema I–G.8. Como por el lema I–G.7, cada

$$\Delta^{(\alpha)} \in \mathcal{D}^{(|\alpha|)}_{A/k} \quad (0 \leq |\alpha| \leq m),$$

se tiene que el segundo miembro de la igualdad pertenece a $\mathcal{D}^{(m)}_{A/k}$. Por tanto, para probar la igualdad, y teniendo en cuenta el aserto I, basta probar que ambos operadores coinciden sobre las potencias $\underline{X}^k$ para todo $k \in \mathbb{N}^n$ con $0 \leq |k| \leq m$. Veámoslo:

$$\sum_{\substack{\alpha\in\mathbb{N}^n \\ 0\leq|\alpha|\leq m}} \left(\sum_{\beta\leq\alpha} \binom{\alpha}{\beta} (-1)^{|\alpha-\beta|} P(\underline{X}^{\beta})\underline{X}^{\alpha-\beta}\right) \Delta^{(\alpha)}(\underline{X}^{k}) =$$

$$= \sum_{\substack{\alpha\in\mathbb{N}^n \\ 0\leq|\alpha|\leq m}} \left(\sum_{\beta\leq\alpha} \binom{\alpha}{\beta} (-1)^{|\alpha-\beta|} P(\underline{X}^{\beta})\underline{X}^{\alpha-\beta}\right) \sum_{k\geq\alpha} \binom{k}{\alpha} \underline{X}^{k-\alpha} =$$

$$= \sum_{\substack{\alpha\leq k \\ 0\leq|\alpha|\leq m}} \left(\sum_{\beta\leq\alpha} (-1)^{|\alpha-\beta|} \binom{\alpha}{\beta}\binom{k}{\alpha} P(\underline{X}^{\beta})\underline{X}^{k-\beta}\right) =$$

$$= \sum_{\beta\leq k} \left(\sum_{\beta\leq\alpha\leq k} (-1)^{|\alpha-\beta|} \binom{\alpha}{\beta}\binom{k}{\alpha}\right) P(\underline{X}^{\beta})\underline{X}^{k-\beta} =$$

$$= \sum_{\beta< k} \left(\sum_{\beta\leq\alpha\leq k} (-1)^{|\alpha-\beta|} \binom{\alpha}{\beta}\binom{k}{\alpha}\right) P(\underline{X}^{\beta})\underline{X}^{k-\beta} + P(\underline{X}^{k}) =$$
$$= P(\underline{X}^{k}).$$

La última igualdad es cierta debido a la siguiente propiedad:

Aserto II: Para todo $\beta < k$, se verifica que

$$\sum_{\beta\leq\alpha\leq k} (-1)^{|\alpha-\beta|} \binom{\alpha}{\beta}\binom{k}{\alpha} = 0.$$

Demostración del Aserto II.

$$\sum_{\substack{\beta_1\leq\alpha_1\leq k_1 \\ \cdots \\ \beta_n\leq\alpha_n\leq k_n}} \prod_{i=1}^{n} (-1)^{\alpha_i-\beta_i} \binom{\alpha_i}{\beta_i}\binom{k_i}{\alpha_i} = \prod_{i=1}^{n} \sum_{\beta_i\leq\alpha_i\leq k_i} (-1)^{\alpha_i-\beta_i} \binom{\alpha_i}{\beta_i}\binom{k_i}{\alpha_i} = 0,$$

puesto que por el aserto II de la proposición I–G.2, todos los sumatorios son cero. ∎

Con ésto se concluye la prueba del teorema I–G.8. ∎

Los resultados anteriores nos describen la estructura de $\mathcal{D}^{(m)}_{A/k}$ repecto de los operadores $\Delta^{(\alpha)}$, $|\alpha| \leq m$.

Corolario I–G.9 ∎ $\mathcal{D}^{(m)}_{A/k} = \bigoplus_{|\alpha|\leq m} A \cdot \Delta^{(\alpha)}$

Demostración.

"$\subseteq$" se tiene por el teorema I–G.8.

"$\supseteq$" es consecuencia del lema I–G.7. ∎

Nota I–G.10 ∎ Se tiene que

$$k = \left\{a \in A \mid \Delta^{(\alpha)}(a) = 0 \;\; \forall \alpha \in \mathbb{N}^n\right\}.$$

Puesto que

"$\subset$" Trivial.

"$\supseteq$" Sea $a \in A$, $a = \sum_{\beta \in I} \lambda_\beta X^\beta$ siendo I subconjunto finito de $\mathbb{N}^n$. Sea γ un elemento maximal respecto del orden parcial "$\leq$ " de $\mathbb{N}^n$ definido en I–D.10, entonces

$$\Delta^\gamma(a) = \lambda_\gamma.$$

En efecto,

$$\Delta^\gamma\left(\sum_{\beta\in I} \lambda_\beta \underline{X}^\beta\right) = \sum_{\beta\in I} \lambda_\beta \Delta^\gamma(\underline{X}^\beta)$$

- si $\beta \neq \gamma$, como γ es un elemento maximal respecto de "$\leq$" se tiene que, $\beta < \gamma$, o no son comparables, y por tanto $\exists i \mid \beta_i > \gamma_i$ y $\exists j \mid \beta_j < \gamma_j$. Por tanto, en ambos casos se verifica que

$$\Delta^\gamma(\underline{X}^\beta) = 0,$$

y entonces $\lambda_\gamma = 0$.

- Si $\beta = \gamma$, tivialmente $\Delta^\gamma(a) = \lambda_\gamma$.

Repitiendo el razonamiento con el elemento $\sum_{\beta \in I - \{\gamma\}} \lambda_\beta \underline{X}^\beta$, se concluye que $a \in k$.

I–H Homomorfismos entre anillos del tipo $\mathcal{D}_{A/k}$

En esta sección describiremos los homomorfismos naturales de anillos filtrados entre $\mathcal{D}_{A/k}$ y $\mathcal{D}_{A[t]/k[t]}$, $\mathcal{D}_{S^{-1}A/k}$, $\mathcal{D}_{S^{-1}A/S^{-1}k}$.

Proposición I–H.1 ■ Para toda $\varphi \in \mathcal{D}^{(l)}_{A/k}$, existe una única $\tilde{\varphi} \in \mathcal{D}^{(l)}_{A[t]/k[t]}$ que extiende a la anterior y además la aplicación

$$\begin{array}{ccc} \mathcal{D}_{A/k} & \longrightarrow & \mathcal{D}_{A[t]/k[t]} \\ \varphi & \longmapsto & \tilde{\varphi} \end{array}$$

es un homomorfismo de anillos filtrados, inyectivo.

Demostración. Dado $\varphi \in \mathcal{D}_{A/k}$, definimos $\tilde{\varphi}$ de la siguiente manera: para todo $\sum_{n \le m} a_n t^n \in A[t]$,

$$\tilde{\varphi}(\sum_{n \le m} a_n t^n) = \sum_{n \le m} \varphi(a_n) t^n.$$

Así definida, la aplicación es, trivialmente, un homomorfismo de anillos inyectivo y tal que $\tilde{\varphi}|_A = \varphi$. Veamos que está bien definida como homomorfismo de anillos filtrados, es decir, si $\varphi \in \mathcal{D}^{(i)}_{A/k}$, entonces

$$\tilde{\varphi} \in \mathcal{D}^{(i)}_{A[t]/k[t]}$$

para todo i. Lo demostraremos por inducción en el orden i:

Para $i = 0$: Sea $\lambda_b \in \mathcal{D}^{(0)}_{A/k} = A$ con $\lambda_b(x) = b \cdot x$ para todo $x \in A$. Entonces

$$\tilde{\lambda}_b(\sum_{n \le m} a_n t^n) = \sum_{n \le m} \lambda_b(a_n) t^n = b \sum_{n \le m} a_n t^n,$$

luego $\tilde{\lambda}_b = \lambda_b \in A[t]$ y por tanto $\tilde{\lambda}_b \in \mathcal{D}^{(0)}_{A[t]/k[t]}$.

Supongamos el resultado cierto para i, y demostremos que también es cierto para $i+1$:

Sea $\varphi \in \mathcal{D}^{(i+1)}_{A/k}$. Deseamos probar que $\tilde{\varphi} \in \mathcal{D}^{(i+1)}_{A[t]/k[t]}$, que equivale a comprobar que

$$[\tilde{\varphi}, b(t)] \in \mathcal{D}^{(i)}_{A[t]/k[t]},$$

para todo $b(t) = \sum_{l\le n} b_l t^l \in A[t]$. En efecto: Para todo $\sum_{k\le m} c_k t^k \in A[t]$,

$$\begin{aligned}
[\tilde{\varphi}, \sum_{l\le n} b_l t^l](\sum_{k\le m} c_k t^k) &= \tilde{\varphi}\left(\left(\sum_{l\le n} b_l t^l\right)\left(\sum_{k\le m} c_k t^k\right)\right) - \left(\sum_{l\le n} b_l t^l\right)\tilde{\varphi}\left(\sum_{k\le m} c_k t^k\right) = \\
&= \tilde{\varphi}\left(\sum_{l+k=0}^{n+m} b_l c_k t^{l+k}\right) - \left(\sum_{l\le n} b_l t^l\right)\left(\sum_{k\le m} \varphi(c_k) t^k\right) = \\
&= \sum_{l+k=0}^{n+m} \varphi(b_l c_k) t^{l+k} - \sum_{l+k=0}^{n+m} b_l \varphi(c_k) t^{l+k} = \\
&= \sum_{l+k=0}^{n+m} [\varphi, b_l](c_k) t^{l+k} = \\
&= \sum_{l\le n} t^l \widetilde{[\varphi, b_l]}\left(\sum_{k\le m} c_k t^k\right).
\end{aligned}$$

Luego

$$[\tilde{\varphi}, \sum_{l\le n} b_l t^l] = \sum_{l\le n} \widetilde{[\varphi, b_l]} t^l \in \mathcal{D}^{(i)}_{A[t]/k[t]},$$

para todo $b(t) \in A[t]$ (puesto que como $\varphi \in \mathcal{D}^{(i+1)}_{A/k}$, $[\varphi, b_l] \in \mathcal{D}^{(i)}_{A/k}$ y aplicando la hipótesis de inducción, sabemos que $\widetilde{[\varphi, b_l]} \in \mathcal{D}^{(i)}_{A[t]/k[t]}$). Por tanto

$$\tilde{\varphi} \in \mathcal{D}^{(i+1)}_{A[t]/k[t]}.$$

La prueba de la unicidad de la extensión obtenida, es trivial. ∎

Estudiemos ahora la extensión natural $\mathcal{D}^{(l)}_{A/k} \longrightarrow \mathcal{D}^{(l)}_{S^{-1}A/k}$. En la siguiente proposición, se dá una descripción de la única tal extensión $\varphi \longrightarrow \tilde{\varphi}$.

Proposición I–H.2 ■ Sea S subconjunto de A multiplicativamente cerrado. Para toda $\varphi \in \mathcal{D}^{(l)}_{A/k}$, existe una única $\tilde{\varphi} \in \mathcal{D}_{S^{-1}A/k}$ tal que extiende a la anterior, es decir, para todo $a \in A$,

$$\tilde{\varphi}\left(\frac{a}{1}\right) = \frac{\varphi(a)}{1}.$$

Además, $\tilde{\varphi} \in \mathcal{D}^{(l)}_{S^{-1}A/k}$ y dado $\frac{a}{s} \in S^{-1}A$,

$$\tilde{\varphi}\left(\frac{a}{s}\right) = \frac{\varphi(a)}{s} - \frac{1}{s}\widetilde{[\varphi, s]}\left(\frac{a}{s}\right).$$

Demostración. Haremos inducción en l:

Para $l = 0$: Sea $\varphi \in \mathcal{D}^{(0)}_{A/k}$. Entonces $\varphi \equiv a$ con $a \in A$, es decir, φ es el homomorfismo

$$\varphi(x) = ax \quad \forall x \in A.$$

Definimos la extensión $\tilde{\varphi} \in \mathcal{D}^{(0)}_{S^{-1}A/k}$ como

$$\tilde{\varphi}\left(\frac{x}{s}\right) = \frac{a}{1} \cdot \frac{x}{s}$$

que trivialmente está bien definida, y como se tiene que

$$\tilde{\varphi}\left(\frac{1}{1}\right) = \frac{\varphi(1)}{1} = \frac{a}{1},$$

$\tilde{\varphi}$ es claramente única. Además, se observa que para todo $a \in A$,

$$\tilde{\varphi}\left(\frac{a}{1}\right) = \frac{\varphi(a)}{1}.$$

Supongamos cierto para toda $l \leq m - 1$, veamos si es cierto para m: En particular esto implica que

1. Si $\varphi,\ \psi \in \mathcal{D}^{(l)}_{A/k}$, entonces $\widetilde{\varphi + \psi} = \tilde{\varphi} + \tilde{\psi}$.

2. Si $\varphi \in \mathcal{D}^{(l)}_{A/k}$, $b \in A = \mathcal{D}^{(0)}_{A/k}$, entonces $\widetilde{\varphi \cdot b} = \tilde{\varphi} \cdot \tilde{b}$ (siendo $\tilde{b} = \frac{b}{1}$).

Veamos que $\tilde{\varphi}$ satisface las condiciones exigidas en el enunciado:

- Dada $\varphi \in \mathcal{D}^{(m)}_{A/k}$ y dado $\frac{a}{s} \in S^{-1}A$

$$\tilde{\varphi}\left(\frac{a}{s}\right) = \frac{\varphi(a)}{s} - \frac{1}{s}\widetilde{[\varphi, s]}\left(\frac{a}{s}\right),$$

está bien definida y

$$\tilde{\varphi}\left(\frac{a}{1}\right) = \frac{\varphi(a)}{1},$$

para todo $a \in A$. Dado $t \in S$, veamos en primer lugar que

$$\tilde{\varphi}\left(\frac{a}{s}\right) = \tilde{\varphi}\left(\frac{ta}{ts}\right).$$

$$\tilde{\varphi}(\frac{ta}{ts}) = \frac{\varphi(ta)}{ts} - \frac{1}{ts}\widetilde{[\varphi, ts]}(\frac{ta}{ts})$$

(como $[\varphi, ts] = [\varphi s, t] + t[\varphi, s]$ y $[\varphi, ts] \in \mathcal{D}^{(m-1)}_{A/k}$, se deduce que

$$\widetilde{[\varphi, ts]} = \widetilde{[\varphi s, t]} + t\widetilde{[\varphi, s]}),$$

aplicando la hipótesis de inducción. Luego

$$\begin{aligned}\tilde{\varphi}\left(\frac{ta}{ts}\right) &= \frac{\varphi(ta)}{ts} - \frac{1}{ts}\widetilde{[\varphi s, t]}\left(\frac{ta}{ts}\right) - \frac{t}{ts}\widetilde{[\varphi, s]}\left(\frac{a}{s}\right) = \\ &= \frac{\varphi(ta)}{ts} - \frac{1}{ts}(\widetilde{[\varphi, t]} \circ \tilde{s})\left(\frac{a}{s}\right) - \frac{1}{s}\widetilde{[\varphi, s]}\left(\frac{a}{s}\right) = \\ &= \frac{\varphi(ta)}{ts} - \frac{1}{ts}\widetilde{[\varphi, t]}\left(\frac{a}{1}\right) - \frac{1}{s}\widetilde{[\varphi, s]}\left(\frac{a}{s}\right),\end{aligned}$$

y por otro lado tenemos

$$\tilde{\varphi}\left(\frac{a}{s}\right) = \frac{\varphi(a)}{s} - \frac{1}{s}\widetilde{[\varphi, s]}\left(\frac{a}{s}\right).$$

Por tanto, basta probar que

$$\frac{\varphi(a)}{s} = \frac{\varphi(ta)}{ts} - \frac{1}{ts}\widetilde{[\varphi, t]}\left(\frac{a}{1}\right),$$

pero

$$\widetilde{[\varphi, t]} = (\widetilde{\varphi \circ t - t \circ \varphi}) = \widetilde{\varphi \circ t} - \widetilde{t \circ \varphi} = [\tilde{\varphi}, \tilde{t}],$$

así que

$$\widetilde{[\varphi, t]}\left(\frac{a}{1}\right) = [\tilde{\varphi}, \tilde{t}]\left(\frac{a}{1}\right) = \frac{\varphi(ta) - t\varphi(a)}{1}.$$

Dados $\frac{a}{s}, \frac{a'}{s'} \in S^{-1}A$ tales que $\frac{a}{s} = \frac{a'}{s'}$, falta probar que

$$\tilde{\varphi}\left(\frac{a}{s}\right) = \tilde{\varphi}\left(\frac{a'}{s'}\right).$$

Aplicando el razonamiento anterior, se deduce tal igualdad, puesto que como

$$\frac{a}{s} = \frac{a'}{s'},$$

entonces existe $t \in A$ tal que $t(as' - a's) = 0$, es decir,

$$tas' - ta's = 0.$$

Luego

$$\frac{a}{s} = \frac{ts'a}{ts's} = \frac{ta's}{ts's} = \frac{a'}{s'}.$$

Trivialmente se tiene que

$$\tilde{\varphi}\left(\frac{a}{1}\right) = \frac{\varphi(a)}{1}$$

para todo $a \in A$.

- $\tilde{\varphi}$ es lineal.
- Veamos que $\tilde{\varphi} \in \mathcal{D}^{(m)}_{S^{-1}A/k}$: Dado $\frac{a}{s} \in S^{-1}A$,

$$\left[\tilde{\varphi}, \frac{a}{s}\right] = \left[\tilde{\varphi}, \frac{a}{1}\right] + \frac{a}{1}\left[\tilde{\varphi}, \frac{1}{s}\right]$$

puesto que

$$\begin{aligned}\left[\tilde{\varphi}, \frac{a}{s}\right] &= \tilde{\varphi}\frac{a}{s} - \frac{a}{s}\tilde{\varphi} = \\ &= \tilde{\varphi}\frac{a}{1}\frac{1}{s} - \frac{a}{1}\tilde{\varphi}\frac{1}{s} + \frac{a}{1}\tilde{\varphi}\frac{1}{s} - \frac{a}{1}\frac{1}{s}\tilde{\varphi} = \\ &= \left[\tilde{\varphi}, \frac{a}{1}\right]\frac{1}{s} + \frac{a}{1}\left[\tilde{\varphi}, \frac{1}{s}\right].\end{aligned}$$

Veamos que $\left[\tilde{\varphi}, \frac{a}{1}\right]$ y $\left[\tilde{\varphi}, \frac{1}{s}\right]$ pertenecen a $\mathcal{D}^{(m-1)}_{S^{-1}A/k}$, para lo cual necesitaremos los siguientes asertos:

Aserto I: En las condiciones anteriores,

$$\left[\tilde{\varphi}, \frac{a}{1}\right] = \widetilde{[\varphi, a]} \quad \forall a \in A.$$

Demostración del Aserto I. Dado $\frac{x}{t} \in S^{-1}A$,

$$\begin{aligned}\left[\tilde{\varphi}, \frac{a}{1}\right]\left(\frac{x}{t}\right) &= \tilde{\varphi}\left(\frac{ax}{t}\right) - \frac{a}{1}\tilde{\varphi}\left(\frac{x}{t}\right) = \\ &= \frac{\varphi(ax)}{t} - \frac{1}{t}\widetilde{[\varphi, t]}\left(\frac{ax}{t}\right) - \frac{a}{1}\frac{\varphi(x)}{t} + \frac{a}{1}\frac{1}{t}\widetilde{[\varphi, t]}\left(\frac{x}{t}\right)\end{aligned}$$

y por otro lado

$$\begin{aligned}\widetilde{[\varphi, a]}\left(\frac{x}{t}\right) &= \frac{[\varphi, a](x)}{t} - \frac{1}{t}[\widetilde{[\varphi, a], t]}\left(\frac{x}{t}\right) = \\ &= \frac{\varphi(ax) - a\varphi(x)}{t} - \frac{1}{t}[\widetilde{[\varphi, t], a]}\left(\frac{x}{t}\right) = [\text{hip. ind. y } 2] = \\ &= \frac{\varphi(ax) - a\varphi(x)}{t} - \frac{1}{t}\left[\widetilde{[\varphi, t]}, \frac{a}{1}\right]\left(\frac{x}{t}\right) = \\ &= \frac{\varphi(ax) - a\varphi(x)}{t} - \frac{1}{t}\left(\widetilde{[\varphi, t]}\left(\frac{ax}{t}\right) - \frac{a}{1}\widetilde{[\varphi, t]}\left(\frac{x}{t}\right)\right).\end{aligned}$$

■

Aserto II: En las mismas condiciones anteriores,

$$\left[\tilde{\varphi}, \frac{1}{s}\right] = -\frac{1}{s} \circ \left[\tilde{\varphi}, \frac{s}{1}\right] \circ \frac{1}{s}$$

Demostración del Aserto II. Dado $\frac{x}{t} \in S^{-1}A$,

$$\left[\tilde{\varphi}, \frac{1}{s}\right]\left(\frac{x}{t}\right) = \tilde{\varphi}\left(\frac{x}{st}\right) - \frac{1}{s}\tilde{\varphi}\left(\frac{x}{t}\right),$$

y por otro lado

$$\begin{aligned}\left[-\frac{1}{s}\circ\left[\tilde{\varphi},\frac{s}{1}\right]\circ\frac{1}{s}\right]\left(\frac{x}{t}\right) &= \left(-\frac{1}{s}\circ\left[\tilde{\varphi},\frac{s}{1}\right]\right)\left(\frac{x}{st}\right)=\\ &=-\frac{1}{s}\left(\tilde{\varphi}\left(\frac{x}{t}\right)-\frac{s}{1}\tilde{\varphi}\left(\frac{x}{st}\right)\right)=\\ &=-\frac{1}{s}\tilde{\varphi}\left(\frac{x}{t}\right)+\tilde{\varphi}\left(\frac{x}{st}\right).\end{aligned}$$

∎

Volvamos a la prueba de la proposición I–H.2. Aplicando el aserto I tenemos

$$\left[\tilde{\varphi},\frac{a}{1}\right]=\widetilde{[\varphi,a]},$$

como $\varphi\in\mathcal{D}^{(m)}_{A/k}$ entonces $[\varphi,a]\in\mathcal{D}^{(m-1)}_{A/k}$ y aplicando hipótesis de inducción

$$\left[\tilde{\varphi},\frac{a}{1}\right]=\widetilde{[\varphi,a]}\in\mathcal{D}^{(m-1)}_{S^{-1}A/k}.$$

Aplicando el aserto II tenemos

$$\left[\tilde{\varphi},\frac{1}{s}\right]=-\frac{1}{s}\circ\left[\tilde{\varphi},\frac{s}{1}\right]\circ\frac{1}{s},$$

además por el aserto I y aplicando hipótesis de inducción

$$\left[\tilde{\varphi},\frac{s}{1}\right]=\widetilde{[\varphi,s]}\in\mathcal{D}^{(m-1)}_{S^{-1}A/k}$$

y $\frac{1}{s}\in\mathcal{D}^{(0)}_{S^{-1}A/k}$. Luego se tiene que

$$\left[\tilde{\varphi},\frac{1}{s}\right]\in\mathcal{D}^{(m-1)}_{S^{-1}A/k}.$$

- Unicidad: Sea $\psi\in\mathcal{D}^{(m)}_{S^{-1}A/k}$ tal que $\psi|_A=\varphi$. Veamos que $\psi=\tilde{\varphi}$. Dado $\frac{a}{s}\in S^{-1}A$

$$\begin{aligned}\psi\left(\frac{a}{s}\right) &=\left[\psi,\frac{1}{s}\right]\left(\frac{a}{1}\right)+\frac{1}{s}\psi\left(\frac{a}{1}\right)=\\ &=\left(-\frac{1}{s}\circ\left[\psi,\frac{s}{1}\right]\circ\frac{1}{s}\right)\left(\frac{a}{1}\right)+\frac{1}{s}\frac{\varphi(a)}{1}.\end{aligned}$$

Pero como $\left[\psi, \frac{s}{1}\right]$ extiende a $[\varphi, s]$, se tiene que $\left[\psi, \frac{s}{1}\right] = \widetilde{[\varphi, s]}$.
Por tanto

$$\begin{aligned}\psi\left(\frac{a}{s}\right) &= \left(-\frac{1}{s} \circ \widetilde{[\varphi, s]} \circ \frac{1}{s}\right)\left(\frac{a}{1}\right) + \frac{\varphi(a)}{s} = \\ &= -\frac{1}{s}\widetilde{[\varphi, s]}\left(\frac{a}{s}\right) + \frac{\varphi(a)}{s} = \\ &= \tilde{\varphi}\left(\frac{a}{s}\right).\end{aligned}$$

Luego hemos probado el resultado. ■

Proposición I–H.3 ■ Sea S un subconjunto de A multiplicativamente cerrado. Consideremos la aplicación $\psi : \mathcal{D}_{A/k} \longrightarrow \mathcal{D}_{S^{-1}A/k}$ encontrada en la proposición I–H.2 y la aplicación natural $\mathcal{D}_{A/k} \longrightarrow S^{-1}\mathcal{D}_{A/k}$. Entonces existe un único homomorfismo de anillos filtrados entre $S^{-1}\mathcal{D}_{A/k}$ y $\mathcal{D}_{S^{-1}A/k}$, que hace conmutativo el diagrama

$$\begin{tikzcd} \mathcal{D}_{A/k} \arrow[r, "\Psi"] \arrow[d] & \mathcal{D}_{S^{-1}A/k} \\ S^{-1}\mathcal{D}_{A/k} \arrow[ur] & \end{tikzcd}$$

Demostración. Basta aplicar la propiedad universal del anillo $S^{-1}\mathcal{D}_{A/k}$ (Veáse por ejemplo, [Gab81]).

Proposición I–H.4 ■ Sean $S \subset A$, $T \subset k$ subconjuntos multiplicativamente cerrados tales que $T \subset S$. Entonces existe un homomorfismo entre los anillos filtrados

$$\begin{array}{ccc} \mathcal{D}_{A/k} & \longrightarrow & \mathcal{D}_{S^{-1}A/T^{-1}k} \\ \varphi & \longmapsto & \tilde{\varphi} \end{array}$$

Además, este homomorfismo es tal que, para toda $\varphi \in \mathcal{D}_{A/k}$, $\tilde{\varphi}|_A = \varphi$.

Demostración. Sea $\tilde{\varphi}$ la extensión de φ definida en la proposición I–H.2, que sabemos que es k–lineal ($\tilde{\varphi} \in \mathcal{D}_{S^{-1}A/k}$). Bastará probar que

$\tilde{\varphi}$ es $S^{-1}k$–lineal. Sea $\frac{1}{s} \in S^{-1}k$, $\frac{a}{t} \in T^{-1}A$ y supongamos que $\tilde{\varphi}$ es k-derivación, se tiene

$$\begin{aligned}\tilde{\varphi}\left(\frac{1}{s}\cdot\frac{a}{t}\right) &= \tilde{\varphi}\left(\frac{a}{\rho(s)t}\right) = \\ &= \frac{\varphi(a)\rho(s)t - a\varphi(\rho(s)t)}{\rho(s)^2t^2} = \\ &= \frac{\varphi(a)\rho(s)t - a\rho(s)\varphi(t)}{\rho(s)^2t^2} = \\ &= \frac{\varphi(a)t - a\varphi(t)}{\rho(s)t^2} = \\ &= \frac{1}{s}\tilde{\varphi}\left(\frac{a}{t}\right).\end{aligned}$$

Luego $\tilde{\varphi}$ es $S^{-1}k$-derivación. Trivialmente se tiene en los demás casos. ∎

Proposición I–H.5 ∎ Sea $I \subseteq A$ ideal y $\hat{A}$ el completado del anillo A. Dado $P \in \mathcal{D}_{A/k}$, existe un único $\hat{P} \in \mathcal{D}_{\hat{A}/k}$ tal que $\hat{P}|_A = P$ y además la aplicación

$$\begin{array}{ccc}\mathcal{D}_{A/k} & \longrightarrow & \mathcal{D}_{\hat{A}/k} \\ P & \longmapsto & \hat{P}\end{array}$$

es un homomorfismo de anillos filtrados.

Demostración. Si $P \in \mathcal{D}_{A/k}$, por la proposición I–F.3 sabemos que es I–continua, luego existe una única extensión $\hat{P}$ de manera que dados $a_n \in A$ con $lim_n a_n = a \in \hat{A}$, $\hat{P}(a) = lim_n P(a_n)$. Utilizaremos los siguientes asertos:

Aserto I: Sea $\{\varphi_n\}_{n\geq 0} \subseteq \mathcal{D}^{(m)}_{\hat{A}/k}$ y supongamos que para todo $a \in \hat{A}$ existe $lim_n\varphi_n(a) = \varphi(a)$. Entonces $\varphi \in \mathcal{D}^{(m)}_{\hat{A}/k}$.

Demostración del Aserto I. Por inducción en m:

Para $m = 0$: Sean $\varphi_n \in \mathcal{D}^{(0)}_{\hat{A}/k}$ entonces $\varphi_n = a_n$ con $a_n \in \hat{A}$, es decir,

$$\varphi_n(x) = a_n x \quad \forall x \in \hat{A}, \ \forall n \geq 0.$$

Como existe $lim_n a_n = a$, entonces existe $lim_n\varphi_n(x) = ax$ para todo $x \in \hat{A}$. Luego $\varphi = a \in \hat{A} = \mathcal{D}^{(0)}_{\hat{A}/k}$.

Supongamos cierto para m, veamos si es cierto para $m+1$: Sea $\varphi_n \in \mathcal{D}^{(m+1)}_{\hat{A}/k}$ tales que para todo $a \in \hat{A}$ existe $lim_n \varphi_n(a) = \varphi(a)$. Entonces se tiene que dado $x \in \hat{A}$, $[\varphi_n, x] \in \mathcal{D}^{(m)}_{\hat{A}/k}$ y además

$$lim_n[\varphi_n, x] = lim_n \varphi_n x - x\varphi_n = \varphi x - x\varphi = [\varphi, x].$$

Aplicando la hipótesis de inducción, $[\varphi, x] \in \mathcal{D}^{(m)}_{\hat{A}/k}$ con $x \in \hat{A}$. Por tanto, $\varphi \in \mathcal{D}^{(m+1)}_{\hat{A}/k}$. ∎

Aserto II: Sea $P \in \mathcal{D}_{A/k}$ y $\hat{P}$ su extensión. Sea $(a_n)_n$ una sucesión en A tal que $lim_n a_n = a \in \hat{A}$. Entonces para todo $b \in \hat{A}$ existe

$$lim_n \widehat{[P, a_n]}(b) = [\hat{P}, a](b).$$

Demostración del Aserto II. Dado $b \in \hat{A}$, existen $b_j \in A$ tales que $lim_j b_j = b$.

$$\begin{aligned}
\widehat{[P, a_n]}(b) &= lim_j \widehat{[P, a_n]}(b_j) = \\
&= lim_j [P, a_n](b_j) = \\
&= lim_j (P(a_n b_j) - a_n P(b_j)) = \\
&= lim_j (\hat{P}(a_n b_j) - a_n \hat{P}(b_j)) = \\
&= \hat{P}(a_n b) - a_n \hat{P}(b),
\end{aligned}$$

luego existe $lim_n \widehat{[P, a_n]}(b) = \hat{P}(ab) - a\hat{P}(b) = [\hat{P}, a](b)$. ∎

Veamos que si $P \in \mathcal{D}^{(l)}_{A/k}$, entonces $\hat{P} \in \mathcal{D}^{(l)}_{\hat{A}/k}$, por inducción en el orden l:

Para $l = 0$: Sea $P \in \mathcal{D}^{(0)}_{A/k}$ entonces $P = a$ con $a \in A$, es decir,

$$P(x) = ax \quad \forall x \in A.$$

Entonces $\hat{P} = a \in A \subseteq \hat{A} = \mathcal{D}^{(0)}_{\hat{A}/k}$.

Supongamos cierto para l, veamos si es cierto para $l+1$: Sea $P \in \mathcal{D}^{(l+1)}_{A/k}$. Basta probar que para todo $a \in \hat{A}$, $[\hat{P}, a] \in \mathcal{D}^{(l)}_{\hat{A}/k}$. Como $a \in \hat{A}$, $a = lim_n a_n$

con $a_n \in A$. Entonces, por el aserto II,

$$[\hat{P}, a] = lim_n \widehat{[P, a_n]}.$$

Como por hipótesis de inducción $[P, a_n] \in \mathcal{D}^{(l)}_{A/k}$; se tiene que $\widehat{[P, a_n]} \in \mathcal{D}^{(l)}_{\hat{A}/k}$. Aplicando el aserto I, $[\hat{P}, a] \in \mathcal{D}^{(l)}_{\hat{A}/k}$, es decir, $\hat{P} \in \mathcal{D}^{(l+1)}_{\hat{A}/k}$. ∎

CAPÍTULO II

El Lema de Normalización para el anillo de series de potencias

En este capítulo presentamos una demostración del lema de normalización para el anillo de series formales $A = k[[\underline{X}]]$, con k cuerpo perfecto de característica $p > 0$, que es una adaptación de la que se encuentra en [Abh64] (23.7 y 24.5). Dicha prueba usa cambios de coordenadas lineales y necesita que el cuerpo k sea infinito. Nuestra adaptación es para un cuerpo de coeficientes perfecto (infinito o no), usando cambios de coordenadas no lineales, (veáse la proposición II–A.4).

II–A El Lema de Normalización para el anillo de series de potencias

Lema II–A.1 ■ Sea B cuerpo de característica $p > 0$, y consideremos la extensión $B \subset G = B[\alpha_1, \dots, \alpha_n]$ con $\alpha_i^p \in B$ para $i = 1, \dots, n$, siendo el grado de la extensión $[G : B] = p^e$. Entonces existen $\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(e)}$ tales que

$$G = B[\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(e)}].$$

Demostración. Veamos que el resultado es cierto para $e = 1$: sea

$$B \subset B[\alpha_1] \subset B[\alpha_1, \dots, \alpha_n] = G$$

siendo $[G : B] = p$, entonces tenemos dos posibilidades para $[B[\alpha_1] : B]$:

- $[B[\alpha_1] : B] = 1$, en cuyo caso $\alpha_1 \in B$;
- $[B[\alpha_1] : B] = p$ y entonces $G = B[\alpha_1]$.

Supongamos cierto para $e - 1$ y ahora $[G : B] = p^e$. Sea $B' = B[\alpha_{i_0}]$ con $\alpha_{i_0} \notin B$ y por tanto $[B' : B] = p$, entonces

$$B \subset B' \subset B[\alpha_1, \dots, \alpha_n] = B'[\alpha_1, \dots, \hat{\alpha}_{i_0}, \dots, \alpha_n],$$

luego

$$[B'[\alpha_1, \dots, \widehat{\alpha_{i_0}}, \dots, \alpha_n] : B'] = p^{e-1}.$$

Aplicando la hipótesis de inducción, existen $\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(e-1)}$ tales que

$$G = B'[\alpha_1, \dots, \widehat{\alpha_{i_0}}, \dots, \alpha_n] = B'[\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(e-1)}] = B[\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(e-1)}, \alpha_{i_0}].$$

■

El siguiente lema, de carácter combinatorio, será necesario para obtener determinadas series distinguidas.

Lema II–A.2 ■ Dado $\sigma = (\sigma_1, \dots, \sigma_{n-1}) \in (\mathbb{N}^*)^{n-1}$, sea $L_\sigma : \mathbb{N}^n \to \mathbb{N}$ definida por $L_\sigma(\alpha) = \sigma_1\alpha_1 + \cdots + \sigma_{n-1}\alpha_{n-1} + \alpha_n$ para todo $\alpha \in \mathbb{N}^n$. Para cada subconjunto finito $F \subset \mathbb{N}^n$, existe una constante $C \geq 1$ tal que si $\sigma_1 \geq \sigma_2 C$, $\sigma_2 \geq \sigma_3 C, \dots, \sigma_{n-2} \geq \sigma_{n-1} C$ y $\sigma_{n-1} \geq C$, entonces $L_\sigma|_F$ es inyectiva.

Demostración. Supongamos $\sharp F = r$. El resultado es cierto para $n = 1$ y cualquier F. Además, también es cierto para todo $n \geq 1$ y para todo F tal que $r = 1$. Supongamos cierto el resultado para $n-1$, y sea ahora $F \subset \mathbb{N}^n$. Consideramos los subconjuntos finitos

$$F_i = \{(\gamma_2, \dots, \gamma_n) \in \mathbb{N}^{n-1} \mid (i, \gamma_2, \dots, \gamma_n) \in F\}$$

con $i \in I \subset \mathbb{N}$ siendo I subconjunto finito. Por tanto aplicando hipótesis de inducción a F_i, existirá para cada i, constantes $C^i \geq 1$ tales que si

$$\sigma_2 \geq C^i\sigma_3, \dots, \sigma_{n-2} \geq C^i\sigma_{n-1} \quad \text{y} \quad \sigma_{n-1} \geq C^i;$$

entonces

$$L_{(\sigma_2,\dots,\sigma_{n-1})} : \mathbb{N}^{n-1} \to \mathbb{N}$$

es inyectiva en F_i. Luego tomando $C \geq max\{C_i\}$ tal que si

$$\sigma_2 \geq C\sigma_3, \dots, \sigma_{n-2} \geq C\sigma_{n-1} \text{ y } \sigma_{n-1} \geq C,$$

$L_{(\sigma_2,\dots,\sigma_{n-1})} : \mathbb{N}^{n-1} \to \mathbb{N}$ es inyectiva sobre cada F_i con $i \in I$. Sea

$$R = max\{|\gamma_i| \mid \gamma \in F,\ 1 \leq i \leq n\}$$

y tomemos dos elementos distintos γ, $\delta \in F$ de manera que $\gamma_1 = i$, $\delta_1 = j$, $\gamma' = (\gamma_2, \dots, \gamma_n) \in F_i$, $\delta' = (\delta_2, \dots, \delta_n) \in F_j$, de este modo

$$L_\sigma(\gamma) - L_\sigma(\delta) = \sigma_1(i-j) + (L_{\delta'}(\gamma') - L_{\sigma'}(\delta'))$$

(siendo $\sigma' = (\sigma_2, \dots, \sigma_{n-1})$). Entonces se verifica:

- Si $i = j$, entonces $\gamma' \neq \delta'$ con $\gamma', \delta' \in F_i$. Luego

  $$L_{\sigma'}(\gamma') \neq L_{\sigma'}(\delta'),$$

  y por tanto $L_\sigma(\gamma) \neq L_\sigma(\delta)$.

- Si $i > j$, entonces si llamamos $x = \sigma_1(i-j) \geq \sigma_1$ y

$$|\mu| = |L_{\sigma'}(\gamma') - L_{\sigma'}(\delta')| \leq |L_{\sigma'}(\gamma')| + |L_{\sigma'}(\delta')| \leq 2n\sigma_2 R,$$

(puesto que $\sigma_3 \leq C\sigma_3 \leq \sigma_2$, $\sigma_4 \leq C\sigma_4 \leq \sigma_3 \leq \sigma_2, \ldots, 1 \leq \cdots \leq \sigma_2$). Por tanto si $x > |\mu|$ entonces $x + \mu = L_\sigma(\gamma) - L_\sigma(\delta) \neq 0$. Basta pues, que $\sigma_1 > \sigma_2 R2n$.

Luego tomando $C = max\{R2n+1,\ C^i\}$, se tiene el resultado. ∎

Lema II–A.3 ∎ Sea $f(\underline{X}) \in k[[X_1, \ldots, X_n]]$ una serie de potencias no nula y no unidad. Entonces para $\sigma_1 >> \sigma_2 >> \cdots >> \sigma_{n-1} >> 0$ (suficientementes grandes), la serie $f(y_1 + y_n^{\sigma_1}, \ldots, y_{n-1} + y_n^{\sigma_{n-1}}, y_n)$ es y_n-distinguida.

Demostración. Dada

$$f(\underline{X}) = \sum_{\alpha \in \mathbb{N}^n} f_\alpha \underline{X}^\alpha \in k[[\underline{X}]]$$

no nula y no unidad, consideremos su diagrama de Newton

$$\mathcal{N}(f) = \{\alpha \in \mathbb{N}^n \mid f_\alpha \neq 0\} \neq \varnothing,$$

y $\underline{0} \notin \mathcal{N}(f)$. Sea

$$E = \mathcal{N}(f) + \mathbb{N}^n,$$

que es un ideal de $\mathbb{N}^n$ y por tanto está finitamente generado (por el teorema de la base de Hilbert), luego existe $F \subset E$ finito y minimal con la propiedad

$$\mathcal{N}(f) \subset E = \bigcup_{\alpha \in F} (\alpha + \mathbb{N}^n).$$

Dado $\sigma = (\sigma_1, \ldots, \sigma_{n-1}) \in (\mathbb{N}^*)^{n-1}$ y

$$L_\sigma(\alpha) = \sigma_1\alpha_1 + \cdots + \sigma_{n-1}\alpha_{n-1} + \alpha_n$$

para todo $\alpha \in \mathbb{N}^n$, aplicamos el lema II-A.2, y para F subconjunto finito de $\mathbb{N}^n$ podemos conseguir $\sigma_1 >> \sigma_2 >> \cdots >> \sigma_{n-1} >> 0$ tales que $L_\sigma|_F$ es inyectiva, y por tanto se tiene el resultado. ∎

Proposición II–A.4 ■ Sea $\mathfrak{p}$ un ideal propio de A de altura $n-e$ siendo $e = dim\frac{A}{\mathfrak{p}}$. Entonces existe un cambio de variables del tipo

$$\begin{cases} y_1 &= X_1 + F_1(X_2^p, \ldots, X_n^p) \\ y_2 &= X_2 + F_2(X_3^p, \ldots, X_n^p) \\ \vdots & \\ y_{n-1} &= X_{n-1} + F_{n-1}(X_n^p) \\ y_n &= X_n \end{cases}$$

con $F_i \in \mathbb{Z}/\mathbb{Z}_p[X_{i+1}^p, \ldots, X_n^p]$ para $i = 1, \ldots, n-1$, tal que la extensión

$$k[[y_1, \ldots, y_e]] \hookrightarrow \frac{A}{\mathfrak{p}}$$

es una extensión finita y $\mathfrak{p} \cap k[[y_1, \ldots, y_e]] = \{0\}$.

Demostración. Veamos que el resultado es cierto para $n = 1$: tenemos $\mathfrak{p}$ ideal propio de $A = k[[X_1]]$ de altura 1. Entonces $\mathfrak{p} = (X_1^m)$ y

$$k \subsetneq \frac{k[[X_1]]}{\mathfrak{p}} = k[\overline{X}_1]$$

con $\overline{X}_1^m = 0$. Luego es una extensión entera, finitamente generada y por tanto finita.

Supongamos cierto el resultado para $n-1$, y sea ahora $\mathfrak{p}$ ideal propio de $A = k[[X_1, \ldots, X_n]]$, $f(X_1, \ldots, X_n) \in \mathfrak{p}$ una serie no nula y no unidad. Mediante el cambio:

$$\begin{cases} y_j = X_j - X_n^{\sigma_j},\ j = 1, \ldots, n-1 \text{ con } \sigma_j = \dot{p} \text{ (suficientemente grandes)} \\ y_n = X_n \end{cases}$$

obtenemos que la serie

$$g(y_1, \ldots, y_{n-1}, X_n) = f(y_1 + X_n^{\sigma_1}, \ldots, y_{n-1} + X_n^{\sigma_{n-1}}, X_n)$$

es X_n-distinguida, por el lema II–A.3. Por el teorema preparatorio de Weierstrass (I–B.8), $g(y_1, \ldots, y_{n-1}, X_n)$ se puede escribir como

$$g(y_1, \ldots, y_{n-1}, X_n) = u \cdot H$$

con u unidad,

$$H = X_n^q + a_{q-1}(y_1, \dots, y_{n-1})X_n^{q-1} + \cdots + a_0(y_1, \dots, y_{n-1}),$$

$$q = ord_{X_n}(f(X_n^{\sigma_1}, \dots, X_n^{\sigma_{n-1}}, X_n))$$

y $a_i(\underline{0}) = 0$.

Por consiguiente $H \in \mathfrak{p}$ y además

$$\frac{k[[y_1, \dots, y_{n-1}]]}{\mathfrak{p}^c} \subseteq \frac{k[[\underline{X}]]}{\mathfrak{p}} = k[[y_1, \dots, y_{n-1}]][X_n]$$

es finita, luego

$$ht(\mathfrak{p}^c) = ht(\mathfrak{p}) - 1.$$

Aplicando la hipótesis de inducción a $\mathfrak{p}^c$ y $k[[y_1, \dots, y_{n-1}]]$, se tiene el resultado.

Por último, aplicando (23.3)+(23.1) de [Abh64], se verifica que $\mathfrak{p}$ es regular relativo a $R = k[[y_1, \dots, y_e]]$ y entonces $\mathfrak{p} \cap k[[y_1, \dots, y_e]] = \{0\}$. ■

Proposición II–A.5 ■ Sean $A = k[[X_1, \dots, X_n]]$, $\mathfrak{p}$ un ideal primo de A, $e = dim \frac{A}{\mathfrak{p}}$ y

$$\varphi : A \to \overline{A} = \frac{A}{\mathfrak{p}}$$

el epimorfismo natural. Para todo $a \in A$ denotamos por $\overline{a}$ a $\varphi(a)$ y $\mathcal{L} = Qt\left(\frac{A}{\mathfrak{p}}\right)$. Entonces se tiene que

$$\mathcal{L} = \mathcal{L}^p[\overline{X}_1, \dots, \overline{X}_n], \ [\mathcal{L} : \mathcal{L}^p] = p^e,$$

y que un sistema generador de la extensión $\mathcal{L}^p \subset \mathcal{L}$ es el conjunto

$$\{\overline{X}_1^{\sigma_1} \cdots \overline{X}_n^{\sigma_n} \ : \ 0 \le \sigma_i < p, \ i = 1, \dots, n\}.$$

Además, después de una reordenación de $\overline{X}_1, \ldots, \overline{X}_n$, podemos tomar

$$\mathcal{L} = \mathcal{L}^p[\overline{X}_1, \ldots, \overline{X}_e]$$

y

$$\{\overline{X}_1^{\alpha_1} \cdots \overline{X}_e^{\alpha_e} \; : \; 0 \leq \alpha_i < p, \; i = 1, \ldots, e\}$$

como una base del espacio vectorial $\mathcal{L}$ sobre $\mathcal{L}^p$.

Demostración. Adaptaremos la demostración de (24.4) en [Abh64]: En primer lugar, por (24.1) de [Abh64], del hecho de ser k cuerpo perfecto se deduce que

$$A = A^p[X_1, \ldots, X_n]$$

y que A es un A^p-módulo libre de rango p^n, siendo el conjunto

$$\{X_1^{\sigma_1} \cdots X_n^{\sigma_n} \; : \; 0 \leq \sigma_1 < p, \ldots, 0 \leq \sigma_n < p\}$$

una base de A sobre A^p (puesto que $X_{i+1} \notin A^p[X_1, \ldots, X_i]$ y $X_{i+1}^p \in A^p[X_1, \ldots, X_i]$ para $i = 0, 1, \ldots, n-1$). Por tanto,

$$\overline{A} = \overline{A}^p[\overline{X}_1, \ldots, \overline{X}_n],$$

y entonces

$$\mathcal{L} = \mathcal{L}^p[\overline{X}_1, \ldots, \overline{X}_n].$$

Además por la proposición II–A.4, mediante un cambio de variables sobre $X_1, \ldots, X_n$, podemos conseguir que

$$R = k[[X_1, \ldots, X_e]] \subset \frac{A}{\mathfrak{p}}$$

sea una extensión finita (por comodidad seguiremos llamando X_i a las y_i de la proposición II–A.4). Luego si $\mathcal{R} = k((X_1, \ldots, X_e))$, tenemos que $\mathcal{R} \subset \mathcal{L}$ es una extensión algebraica finita.

Aplicando (24.1) de [Abh64] a $R = k[[X_1, \ldots, X_e]]$ y $\mathcal{R} = Qt(R)$ tenemos que

$$[\mathcal{R} : \mathcal{R}^p] = p^e.$$

Mediante el isomorfismo $F(h) = h^p$

$$\begin{array}{ccc} \mathcal{R} & \subset & \mathcal{L} \\ F\downarrow & & \downarrow F \\ \mathcal{R}^p & \subset & \mathcal{L}^p \end{array}$$

obtenemos $[\mathcal{L} : \mathcal{R}] = [\mathcal{L}^p : \mathcal{R}^p]$. Por consiguiente

$$[\mathcal{L} : \mathcal{R}][\mathcal{R} : \mathcal{R}^p] = [\mathcal{L} : \mathcal{R}^p] = [\mathcal{L} : \mathcal{L}^p][\mathcal{L}^p : \mathcal{R}^p]$$

y entonces

$$[\mathcal{L} : \mathcal{L}^p] = [\mathcal{R} : \mathcal{R}^p] = p^e.$$

Como sabemos que

$$\{X_1^{\sigma_1} \cdots X_n^{\sigma_n} : 0 \leq \sigma_1 < p, \ldots, 0 \leq \sigma_e < p\}$$

es una base de A sobre A^p, se tiene que un sistema generador de la extensión $\mathcal{L}^p \subset \mathcal{L}$ es el conjunto de monomios

$$\{\overline{X}_1^{\sigma_1} \cdots \overline{X}_n^{\sigma_n} : 0 \leq \sigma_i < p, \ i = 1, \ldots, n\}.$$

Aplicando ahora el lema II–A.1, después de una reordenación adecuada de $\overline{X}_1, \ldots, \overline{X}_n$, podemos tomar

$$\mathcal{L} = \mathcal{L}^p[\overline{X}_1, \ldots, \overline{X}_e]$$

y

$$\{\overline{X}_1^{\alpha_1} \cdots \overline{X}_e^{\alpha_e} : 0 \leq \alpha_i < p, \ i = 1, \ldots, e\},$$

como una base del espacio vectorial $\mathcal{L}$ sobre $\mathcal{L}^p$. ∎

Teorema II–A.6 ∎ **(Lema de Normalización para el anillo de series de potencias)** Sean $A = k[[X_1, \ldots, X_n]]$ y $\mathfrak{p}$ un ideal primo propio de A siendo $e = \dim(A/\mathfrak{p})$. Entonces existen $y_1, \ldots, y_n \in A$ nuevas variables tales que

1. $\mathfrak{p} \cap k[[y_1, \ldots, y_e]] = \{0\}$,

2. la extensión $k[[y_1,\ldots,y_e]] \hookrightarrow \dfrac{A}{\mathfrak{p}}$ es finita,

3. la extensión $\mathcal{R} \hookrightarrow \mathcal{L}$ es finita separable, siendo $\mathcal{L} = Qt\left(\dfrac{A}{\mathfrak{p}}\right)$ y $\mathcal{R} = Qt(k[[y_1,\ldots y_e]]) = k((y_1,\ldots,y_e))$.

Demostración. En primer lugar, si $\mathcal{L} = Qt\left(\dfrac{A}{\mathfrak{p}}\right)$, y

$$\varphi : A \to \overline{A} = \frac{A}{\mathfrak{p}}$$

es el epimorfismo natural, (para todo $a \in A$ denotamos por $\overline{a}$ a $\varphi(a)$), entonces por la proposición II–A.5 se tiene que

$$\mathcal{L} = \mathcal{L}^p[\overline{X}_1,\ldots,\overline{X}_n], \quad [\mathcal{L} : \mathcal{L}^p] = p^e,$$

y que un sistema generador de la extensión $\mathcal{L}^p \subset \mathcal{L}$ es el conjunto de monomios

$$\{\overline{X}_1^{\sigma_1} \cdots \overline{X}_n^{\sigma_n} \,:\, 0 \le \sigma_1 < p,\ldots,0 \le \sigma_n < p\}.$$

Además, después de una reordenación adecuada de $\{\overline{X}_1,\ldots,\overline{X}_n\}$, podemos tomar

$$\mathcal{L} = \mathcal{L}^p[\overline{X}_1,\ldots,\overline{X}_e]$$

y

$$\{\overline{X}_1^{\alpha_1} \cdots \overline{X}_e^{\alpha_e} \,:\, 0 \le \alpha_1 < p,\ldots,0 \le \alpha_e < p\}$$

como una base del espacio vectorial $\mathcal{L}$ sobre $\mathcal{L}^p$. Por comodidad, llamemos a los monomios

$$\overline{X}_1^{\alpha_1} \cdots \overline{X}_e^{\alpha_e} = f_\alpha(\overline{X}_1,\ldots,\overline{X}_e)$$

con $\alpha = 1,\ldots,p^e$.

Por la proposición II–A.4, sabemos que existe un cambio de variables del tipo:

$$\begin{cases} y_1 = & X_1 + F_1(X_2^p, \ldots, X_n^p) \\ y_2 = & X_2 + F_2(X_3^p, \ldots, X_n^p) \\ \vdots & \\ y_n = & X_n \end{cases}$$

con $F_i \in \mathbb{Z}/\mathbb{Z}_p[X_{i+1}^p, \ldots, X_n^p]$ para $i = 1, \ldots, n-1$, y tal que la extensión

$$k[[y_1, \ldots, y_e]] \hookrightarrow \frac{A}{\mathfrak{p}}$$

es una extensión finita y $\mathfrak{p} \cap k[[y_1, \ldots, y_e]] = \{0\}$ (luego se verifican (1) y (2)).

Por último, si $\mathcal{R} = Qt(R) = k((y_1, \ldots, y_e))$, entonces tenemos que $\mathcal{L} = Qt\left(\frac{A}{\mathfrak{p}}\right)$ es una extensión algebraica finita de $\mathcal{R}$ (puesto que $R \subset \frac{A}{\mathfrak{p}}$ es finita). Si demostramos que

$$\mathcal{L} = \mathcal{L}^p(\mathcal{R}),$$

tendríamos que $\mathcal{L}$ es separable sobre $\mathcal{R}$ (aplicando el teorema I–B.4). Ahora bien, sabemos que

$$\{f_\alpha(\overline{X}_1, \ldots, \overline{X}_e) : \ \alpha = 1, \ldots, p^e\}$$

es una base de $\mathcal{L}$ sobre $\mathcal{L}^p$ y la relación

$$\overline{y}_j = \overline{X}_j + F_j(\overline{X}_{j+1}^p, \ldots, \overline{X}_n^p) \text{ para } j = 1, \ldots, e;$$

luego

$$\{f_\alpha(\overline{y}_1 - F_1(\overline{X}_2^p, \ldots, \overline{X}_n^p)), \ldots, \overline{y}_e - F_e(\overline{X}_{e+1}^p, \ldots, \overline{X}_n^p)), \ \alpha = 1, \ldots, p^e\}$$

es una base de $\mathcal{L}$ sobre $\mathcal{L}^p$, con $\overline{y}_j \in \mathcal{R}$ y $F_j(\overline{X}_{j+1}^p, \ldots, \overline{X}_n^p) \in \mathcal{L}^p$ para $j = 1, \ldots, e$. Por tanto, $\mathcal{L} = \mathcal{L}^p(\mathcal{R})$ y se verifica el apartado (3).. ∎

CAPÍTULO III

La noetherianidad de $A_{(\infty)} = A \otimes_k k_{(\infty)}$

El objetivo fundamental de este capítulo es demostrar la noetherianidad del anillo $A_{(\infty)}$ que definiremos a continuación, con el que trabajaremos en el resto de la memoria.

III–A Caracterización de $A_{(\infty)}$

Sea k un cuerpo de característica $p > 0$. Para cada k-álgebra A, consideramos la $k(t)$–álgebra definida en la sección I–A,

$$A(t) := A \otimes_k k(t).$$

Consideraremos también la extensión de cuerpos $k \subset k_{(\infty)}$ siendo

$$k_{(\infty)} = \bigcup_{m \geq 1} k(t^{\frac{1}{p^m}}).$$

Nótese que si k es perfecto, $k_{(\infty)}$ coincide con la clausura perfecta de

$k(t)$, $k(t)_{per}$.

Para simplificar la notación, notaremos $t_m = t^{\frac{1}{p^m}}$. Definimos también

$$A_{(m)} := A(t_m) := A \otimes_k k(t_m) = A(t) \otimes_{k(t)} k(t_m),$$

$$A_{[m]} := A[t_m]$$

y

$$A_{(\infty)} := A \otimes_k k_{(\infty)} = \bigcup_{m\geq 0} A_{(m)},$$

$$A_{[\infty]} := \bigcup_{m\geq 0} A[t_m].$$

Se verifica que cada $A_{(m)}$ (resp. $A_{[m]}$) es un módulo libre sobre $A(t)$ (resp. sobre $A[t]$) de rango p^m (pues $(t_m)^{p^m} - t = 0$). Por tanto, tenemos las extensiones

$$\begin{array}{ccccccccccc}
A_{[0]} = A[t] & \subset & A[t_1] & \subset & A[t_2] & \subset & \cdots & A[t_m] & \subset & \cdots & \subset & A_{[\infty]} \\
\cap & & \cap & & \cap & & & \cap & & & & \cap \\
A_{(0)} = A(t) & \subset & A(t_1) & \subset & A(t_2) & \subset & \cdots & A(t_m) & \subset & \cdots & \subset & A_{(\infty)}
\end{array}$$

Notas III–A.1 ■

1. Las k–álgebras $A_{[m]}$ (respectivamente $A_{(m)}$) son isomorfas entre sí.
2. Si $S_m = k[t_m] - \{0\}$, entonces $A_{(m)} = S_m^{-1} A_{[m]}$.
3. Dado que $(S_m)^{p^m} \subset S_0$ (al ser k cuerpo de característica $p > 0$), y como $S_0 \subset S_m$, se verifica que $A_{(m)} = S_0^{-1} A_{[m]}$ para todo $m \geq 0$. Como consecuencia, $A_{(\infty)} = S_0^{-1} A_{[\infty]}$.
4. Si A es un dominio (integramente cerrado), entonces $A_{[m]}$ y $A_{(m)}$ son dominios (integramente cerrados) para todo $m \geq 0$, ó $m = \infty$.

5. Si A es una k–álgebra noetheriana, entonces los anillos $A_{[m]}$ son anillos noetherianos, para todo $m \geq 0$ (puesto que son isomorfos a $A[t]$). Los $A_{(m)}$ son también anillos noetherianos, puesto que $A_{(m)} = S_0^{-1} A_{[m]}$.
6. Si $I \subset A$ es un ideal, entonces $(A/I)_{(\infty)} = A_{(\infty)}/A_{(\infty)} I$.
7. Si $T \subset A$ es un subconjunto multiplicativamente cerrado, entonces se tiene que $(T^{-1}A)_{(\infty)} = T^{-1}A_{(\infty)}$.
8. Si $A = k[\underline{X}] = k[X_1, \ldots, X_n]$, entonces el anillo $A_{(\infty)} = k_{(\infty)}[\underline{X}]$, por tanto $A_{(\infty)}$ es noetheriano. Más aún, el anillo $A_{(\infty)}$ es noetheriano para toda k–álgebra A finitamente generada.

Sin embargo, si $A = k[\underline{X}]$, entonces el anillo $A_{[\infty]}$ no es noetheriano, como probamos en el siguiente lema:

Lema III–A.2 ∎ Si $A = k[\underline{X}]$, entonces $A_{[\infty]}$ no es noetheriano.

Demostración. Comprobemos que el ideal generado por las raíces p^m-ésimas

$$I = (\{t^{\frac{1}{p^m}} : m \geq 0\}),$$

no es finitamemte generado. Supongamos que sí, entonces existirá

$$\{t, t^{\frac{1}{p}}, t^{\frac{1}{p^2}}, \cdots, t^{\frac{1}{p^k}}\}$$

un sistema de generadores finito de I. Como $t^{\frac{1}{p^{k+1}}} \in I$, entonces existen

$$\alpha_0, \alpha_1, \cdots, \alpha_k \in A_{[\infty]}$$

tales que

$$t^{\frac{1}{p^{k+1}}} = \alpha_0 t + \alpha_1 t^{\frac{1}{p}} + \cdots + \alpha_k t^{\frac{1}{p^k}}.$$

Tomemos el exponente

$$k_0 = max\{k+1, max\{l \text{ tales que } t^{\frac{1}{p^l}} \text{aparece en algún } \alpha_i\}\}.$$

Elevando la igualdad anterior a p^{k_0} (siendo p la característica del cuerpo k) obtenemos

$$t^{p^{k_0-k-1}} = \alpha_0^{p^{k_0}} t^{p^{k_0}} + \alpha_1^{p^{k_0}} t^{p^{k_0-1}} + \cdots + \alpha_k^{p^{k_0}} t^{p^{k_0-k}},$$

donde los $\alpha_i^{p^{k_0}}$ son polinomios en $A[t]$. Luego t es algebraico sobre A, lo que es una contradicción. ∎

Proposición III–A.3 ∎ Sea A una k–álgebra cualquiera y $m \geq 1$. Las extensiones $A_{[m-1]} \subset A_{[m]}$ y $A_{(m-1)} \subset A_{(m)}$ verifican:

1. Son libres finitas, y por tanto, enteras y fielmente planas.
2. Las extensiónes correspondientes a sus cuerpos de fracciones son puramente inseparables.

Demostración. Veámoslo para la extensión $A_{(m-1)} \subset A_{(m)}$:

- Es libre finita de rango p, puesto que

  $$A_{(m)} = A \otimes_k k(t_m) = A_{(m-1)} \otimes_{k(t_{m-1})} k(t_m)$$

  y t_m satisface la ecuación $F = 0$, siendo F el polinomio mónico

  $$F = X^p - t_{m-1} \in A_{(m-1)}[X].$$

  Luego es entera y fielmente plana (puesto que libre implica fielmente plana).
- Sea $\mathbf{K} = Qt(A)$, entonces $Qt(A_{(m-1)}) = \mathbf{K}(t_{m-1})$ y $Qt(A_{(m)}) = \mathbf{K}(t_m)$. Se tiene que la extensión

  $$\mathbf{K}(t_{m-1}) \subset \mathbf{K}(t_m)$$

  es puramente inseparable, pues $(t_m)^p = t_{m-1} \in \mathbf{K}(t_{m-1})$.

Para la extensión $A_{[m-1]} \subset A_{[m]}$, la proposición se demuestra de manera análoga. ∎

Corolario III–A.4 ■ $A_{[\infty]}$ (resp. $A_{(\infty)}$) es entera y fielmente plana sobre cada $A_{[m]}$ (resp. $A_{(m)}$).

A partir de ahora, para cada ideal primo P de $A_{(\infty)}$, notaremos

$$P_{[\infty]} := P \cap A_{[\infty]}, \quad P_{[m]} := P \cap A_{[m]} \in \operatorname{Spec}(A_{[m]})$$

y

$$P_{(m)} := P \cap A_{(m)} \in \operatorname{Spec}(A_{(m)}).$$

De manera similar, si Q es un ideal primo de $A_{[\infty]}$,

$$Q_{[m]} := Q \cap A_{[m]} \in \operatorname{Spec}(A_{[m]}).$$

Se verifica que

- $P = \bigcup_{m\geq 0} P_{(m)}$, $P_{[\infty]} = \bigcup_{m\geq 0} P_{[m]}$, (resp. $Q = \bigcup_{m\geq 0} Q_{[m]}$).
- $P_{(n)} \cap A_{(m)} = P_{(m)}$ y $P_{[n]} \cap A_{[m]} = P_{[m]}$ para todo $n \geq m$ (resp. $Q_{[n]} \cap A_{[m]} = Q_{[m]}$ para todo $n \geq m$).

Lema III–A.5 ■ Sean $P' \subseteq P$ ideales primos de $A_{(\infty)}$ (resp. de $A_{[\infty]}$). Las siguientes condiciones son equivalentes:

(a) $P' \subsetneq P$

(b) Existe un $m \geq 0$ tal que $P'_{(m)} \subsetneq P_{(m)}$ (resp. $P'_{[m]} \subsetneq P_{[m]}$).

(c) Para todo $m \geq 0$, $P'_{(m)} \subsetneq P_{(m)}$ (resp. $P'_{[m]} \subsetneq P_{[m]}$).

Demostración. Trivial, por el corolario III–A.4 y por verificarse en las extensiones enteras. ■

Lema III–A.6 ■ Sea P un ideal primo de $A_{(\infty)}$ (resp. de $A_{[\infty]}$). Las siguientes condiciones son equivalentes:

(a) P es maximal.

(b) $P_{(m)}$ (resp. $P_{[m]}$) es maximal para algún $m \geq 0$.

(c) $P_{(m)}$ (resp. $P_{[m]}$) es maximal para todo $m \geq 0$.

Demostración. Es trivial por el corolario III–A.4 y por verificarse en extensiones enteras. ■

Corolario III–A.7 ■ Con la notación anterior, para cada ideal primo P de $A_{(\infty)}$ se verifica que

$$\mathrm{ht}(P) = \mathrm{ht}(P_{(m)}) = \mathrm{ht}(P_{[m]}) \quad \text{para todo} \quad m \geq 0.$$

Más aún, $\dim(A_{(\infty)}) = \dim(A_{(m)})$.

Demostración. Por el corolario III–A.4, $A_{(\infty)}$ es fielmente plana sobre cada $A_{(m)}$, luego es plana y entonces se verifica el "teorema del descenso". Por tanto

$$\mathrm{ht}(P \cap A_{(m)}) = \mathrm{ht}(P_{(m)}) \leq \mathrm{ht}(P).$$

Otra vez por el corolario III–A.4, $A_{(\infty)}$ es entera sobre cada $A_{(m)}$, y entonces

$$\mathrm{ht}(P) \leq \mathrm{ht}(P \cap A_{(m)}).$$

La igualdad $\mathrm{ht}(P_{(m)}) = \mathrm{ht}(P_{[m]})$ es cierta, dado que $A_{(m)}$ es una localización de $A_{[m]}$.

Por último, por ser $A_{(m)} \subset A_{(\infty)}$ entera, se verifica el "teorema del ascenso", luego

$$\dim(A_{(m)}) \leq \dim(A_{(\infty)}).$$

La otra desigualdad, se debe de nuevo a que la extensión es entera y a que dado $P \in \mathrm{Spec}(A_{(\infty)})$

$$\mathrm{ht}(P) \leq \mathrm{ht}(P^c) = \mathrm{ht}(P \cap A_{(m)}) = \mathrm{ht}(P_{(m)}).$$

■

Nota III–A.8 ■ El corolario III–A.7 también es cierto si reemplazamos $A_{(m)} \subset A_{(\infty)}$ por $A_{[m]} \subset A_{[\infty]}$.

Corolario III–A.9 ■ Con la notación anterior, para todo $Q \in \mathrm{Spec}(A_{(m)})$ existe un único $\tilde{Q} \in \mathrm{Spec}(A_{(m+1)})$ tal que $\tilde{Q}^c = Q$. Más aún, el ideal $\tilde{Q}$ viene dado por

$$\tilde{Q} = \{y \in A_{(m+1)} \mid y^p \in Q\}.$$

Demostración. La extensión $A_{(m)} \subset A_{(m+1)}$ verifica que $(A_{(m+1)})^p \subset A_{(m)}$. Además, sabemos que para cualquier ideal primo P de $A_{(m+1)}$, su contracción $P^c = P \cap A_{(m)}$ es un ideal primo de $A_{(m)}$.

Dado $Q \in \mathrm{Spec}(A_{(m)}$, sea

$$\tilde{Q} = \{y \in A_{(m+1)} \mid y^p \in Q\}.$$

Es fácil probar que:

- $\tilde{Q}$ es un ideal primo de $A_{(m+1)}$ (por ser Q ideal primo y por verificarse $(A_{(m+1)})^p \subset A_{(m)}$).
- $\widetilde{P^c} = P$ (por ser P ideal primo).
- $\tilde{Q}^c = Q$ (por ser Q ideal primo).

■

Corolario III–A.10 ■ Supongamos que A es noetheriano y que para todo ideal maximal $\mathfrak{m}$ de A, el cuerpo residual $A/\mathfrak{m}$ es algebraico sobre k. Entonces para todo $m \geq 0$, se verifica que:

1. $\dim(A_{[\infty]}) = \dim(A_{[m]}) = \dim(A[t]) = n + 1$.
2. $\dim(A_{(\infty)}) = \dim(A_{(m)}) = \dim(A(t)) = n$.

Demostración.

1. Cierto por la nota III–A.8 y la hipótesis de noetherianidad.
2. Es consecuencia del corolario III–A.7 y la proposición I–A.2.

■

Como consecuencia del análisis previo, obtenemos la altura de los ideales maximales de $A_{(\infty)}$ en el caso siguiente:

Corolario III–A.11 ■ Sea A una k–álgebra noetheriana, biequidimensional, universalmente catenaria de dimensión de Krull n, y tal que para todo ideal maximal $\mathfrak{m}$ de A, el cuerpo residual $A/\mathfrak{m}$ es algebraico sobre k. Entonces todo ideal maximal de $A_{(\infty)}$ tiene altura n.

Demostración. Consecuencia del teorema I–A.3, del lema III–A.6, y del corolario III–A.10. ■

III–B El mayor subcuerpo perfecto de un cuerpo de funciones formales

A lo largo de toda esta sección k será un cuerpo perfecto de característica $p > 0$, $A = k[[\underline{X}]] = k[[X_1, \ldots, X_n]]$ el anillo de series formales, $\mathfrak{p}$ un ideal primo de A, $R = \dfrac{A}{\mathfrak{p}}$ y $K = Qt(R)$. Para cualquier $\mathbb{F}_p$–álgebra B, notaremos por $B^\sharp = \bigcap_{e \geq 0} B^{p^e}$.

El objetivo de esta sección es demostrar que el mayor subcuerpo perfecto de K, $K^\sharp$, es una extensión algebraica del cuerpo de constantes, k. Este resultado se prueba en la proposición III–B.6 y será uno de los ingredientes de la prueba del corolario III–C.8.

Proposición III–B.1 ■ Bajo las condiciones anteriores, se tiene que $k = R^\sharp$.

Demostración. Sea $\mathfrak{m}$ el ideal maximal de R. Es suficiente probar que $R^\sharp \subseteq k$. Si $f \in R^\sharp$, entonces para todo $e > 0$ existe un $f_e \in R$ tal que $f = f_e^{p^e}$.

- Supongamos primero que f no es una unidad. Entonces f_e no es unidad para ningún $e > 0$, y por tanto $f_e \in \mathfrak{m}$ para todo $e > 0$. Es decir, $f \in \mathfrak{m}^{p^e}$ para todo $e > 0$, y usando el teorema de intersección de Krull,

$$f \in \bigcap_{e \geq 0} \mathfrak{m}^{p^e} = \bigcap_{k \geq 0} \mathfrak{m}^k = (0).$$

- Si f es unidad, entonces $f = f_0 + \tilde{f}$, con $f_0 \in k \subset R^\sharp$ y $\tilde{f} \in R^\sharp$ no es unidad. Por el caso anterior $\tilde{f} = 0$, luego $f \in k$.

■

Proposición III–B.2 ■ Bajo las condiciones anteriores, si $\mathfrak{p} = (0)$, es decir, $R = k[[\underline{X}]]$ y $K = k((X))$. Se verifica que $k = K^\sharp$.

Demostración. Sea $\mathfrak{m} = (X_1, \dots, X_n)$ el ideal maximal de R. Sean $g, h \in R$ primos entre sí. Si $g/h \in K^p$, entonces existen $a_1, b_1 \in R$ primos entre sí tales que

$$\frac{g}{h} = \left(\frac{a_1}{b_1}\right)^p = \frac{a_1^p}{b_1^p}.$$

Como ahora R es un dominio de factorización única, existirán $\lambda, \mu \in k$ (o sea unidades), tales que $g = \lambda a_1^p$, $h = \mu b_1^p$. Como k es perfecto, $\lambda = \delta^p$ y $\mu = \gamma^p$ con $\delta, \gamma \in k$. Luego

$$g = \delta^p a_1^p = (\delta a_1)^p \in R^p \text{ y } h = \gamma^p b_1^p = (\gamma b_1)^p \in R^p.$$

Por tanto si $g/h \in K^\sharp$, entonces $g, h \in R^\sharp = k$ (por III–B.1). Por consiguiente, $g/h \in k$ y tenemos que $K^\sharp \subset k$. La otra inclusión es trivial. ■

Con el fin de tratar el caso general, primero necesitamos los siguientes lemas:

Lema III–B.3 ■ Si L es una extensión algebraica separable de un cuerpo K de característica $p > 0$, entonces $L^\sharp$ es una extensión algebraica de $K^\sharp$.

Demostración. Si $x \in L^\sharp$, entonces $x = y_e^{p^e}$ con $y_e \in L$ para todo $e \geq 0$. Como y_e es separable sobre K, se tiene que

$$K(y_e) = K(y_e^{p^e}) = K(x).$$

Luego $y_e = x^{p^{-e}} \in K(x)$, y elevando a p^e, resulta que $x \in K^{p^e}(x^{p^e})$. Por tanto

$$[K^{p^e}(x) : K^{p^e}] = [K^{p^e}(x^{p^e}) : K^{p^e}],$$

y como

$$[K^{p^e}(x^{p^e}) : K^{p^e}] = [K(x) : K].$$

Entonces x tiene igual polinomio mínimo sobre K^{p^e} que sobre K para todo $e \geq 0$, y los coeficientes de dicho polinomio mínimo deben pertenecer a $K^\sharp$. Por lo tanto, x es algebraico sobre $K^\sharp$. ∎

Lema III–B.4 ∎ Toda extensión algebraica de un cuerpo perfecto es perfecto.

Demostración. Basta probarlo para las extensiones algebraicas finitas; así consideremos $k \subset L$ una extensión algebraica finita, con k perfecto. Entonces $k \subset L^p \subset L$, y se tiene que la sucesión decreciente de extensiones

$$k \subset \cdots \subset L^{p^3} \subset L^{p^2} \subset L^p \subset L$$

es estacionaria, puesto que $k \subset L$ es finita. Sea $r \geq 0$ tal que

$$L^{p^r} = L^{p^{r+1}} = \cdots .$$

Para todo $y \in L$, existe un $z \in L$ tal que $y^{p^r} = z^{p^{r+1}}$, y como k es perfecto, $(y - z^p)^{p^r} = 0$. Por tanto $y - z^p = 0$, es decir, L es perfecto. ∎

Lema III–B.5 ∎ Sea F un subanillo de un dominio de integridad G y sea H la clausura íntegra de F en G. Sean p, q polinomios mónicos en $G[X]$ tales que $pq \in H[X]$. Entonces $p, q \in H[X]$.

Demostración. Tomemos un cuerpo que contenga a G en el que los polinomios p, q se descompongan en factores lineales:

$$p = \prod(x - \alpha_i), \qquad q = \prod(x - \beta_j).$$

Cada α_i y cada β_j es una raíz de pq, por tanto son enteros sobre H. Luego los coeficientes de p y q son enteros sobre H, y como H es entero sobre F, son enteros sobre F, luego están en H. Por lo tanto $p, q \in H[X]$. ∎

Los siguientes resultados han sido obtenidos en colaboración con el profesor J. M. Giral.

Proposición III–B.6 ■ Sean k cuerpo perfecto de característica $p > 0$, $A = k[[\underline{X}]]$ el anillo de series formales, $\mathfrak{p} \subset A$ un ideal primo, $R = A/\mathfrak{p}$ y $K = Qt(R)$. Entonces $K^\sharp$ es una extensión algebraica de k.

Demostración. Supongamos $dim(A/\mathfrak{p}) = r \leq n$. Por el lema de normalización para anillos de series de potencias (II–A.6), sabemos que existe un nuevo sistema de coordenadas formales $Y_1, \ldots, Y_n \in A$ tales que

- $\mathfrak{p} \cap k[[Y_1, \ldots, Y_r]] = \{0\}$,
- $k[[Y_1, \ldots, Y_r]] \hookrightarrow \frac{A}{\mathfrak{p}}$ es una extensión finita,
- $k((Y_1, \ldots, Y_r)) \hookrightarrow K$ es una extensión finita separable.

Como K es finita separable sobre $k((Y_1, \ldots, Y_r))$, por el lema III–B.3, se sigue que $K^\sharp$ es algebraico sobre $(k((Y_1, \ldots, Y_r)))^\sharp$, que es igual a k, (por la proposición III–B.2). ■

Nota III–B.7 ■ En particular, si k es un cuerpo algebraicamente cerrado, se tiene que $K^\sharp = k$.

En el siguiente teorema damos una información más precisa de la proposición III–B.6.

Teorema III–B.8 ■ Bajo las hipótesis de la proposición III–B.6, se verifican:

1. Si R es íntegramente cerrado en K, entonces $K^\sharp = k$.
2. En el caso general, $K^\sharp$ es una extensión finita de k.

Demostración. Sea L la clausura algebraica de k en K. Por el lema III–B.4, L es perfecto. Luego $L^\sharp = L$ y por tanto $L \subset K^*$. La otra inclusión se tiene porque $K^\sharp$ es algebraico sobre k, por la proposición III–B.6, y L es la clausura algebraica de k en K, luego $K^\sharp \subset L$. Por tanto $L = K^\sharp$.

1. Necesitamos probar que k es algebraicamente cerrado en K, lo que equivale a demostrar que $k^0 \otimes_k K$ es un dominio íntegro, siendo k^0 una clausura algebraica de k en K (por I–B.5). Basta probar que $k' \otimes_k K$ es un dominio íntegro siendo k' una extensión finita de k, ya que toda extensión algebraica de un cuerpo es un límite inductivo de extensiones finitas y el límite inductivo conmuta con el producto tensorial.
   Ahora bien, puesto que k es perfecto se verifica el teorema del elemento primitivo, luego k' es de la forma $k[T]/(h)$ con h un polinomio mónico irreducible de $k[T]$. Entonces
   $$k' \otimes_k K = \frac{K[T]}{(K[T]h)}.$$
   Además, h es irreducible en $R[T]$: Supongamos lo contrario, es decir, $h = fg$ con $f, h \in R[T]$ que podemos suponer mónicos con grado mayor igual a 1. Reduciendo módulo el ideal maximal de R, obtenemos
   $$h = \overline{fg} \quad \text{en} \quad k[T],$$
   lo que se contradice con la irreducibilidad de h en $k[T]$.
   Pero si h es irreducible en $R[T]$, también es irreducible en $K[T]$: ya que en caso contrario, si h fuese reducible en $K[T]$, como R es íntegramente cerrado en K, por el lema III–B.5, lo sería también en $R[T]$ lo que es una contradicción. Por tanto $k' \otimes_k K$ es un dominio íntegro. De ahí se concluye que k es algebraicamente cerrado en K, y entonces $k = L = K^\sharp$.
2. Sea $\overline{R}$ la clausura íntegra de R en K. Sabemos que $\overline{R}$ es un R–módulo finitamente generado (por el teorema (23.I.5), Ch.

0 de [GD64]), y $\overline{R}$ es un anillo local completo (por el corolario (23.I.6), Ch. 0 de [GD64]), que es obviamente un dominio íntegro. Por tanto, aplicando el teorema de estructura de Cohen (I–B.10), deducimos que $\overline{R}$ es un dominio formal sobre una extensión finita k' de k. Por el caso 1 sabemos que $K^\sharp = k'$, y entonces $K^\sharp$ es una extensión finita de k.

■

III–C El anillo $A \otimes_k k(t)_{per}$ es noetheriano

A lo largo de esta sección, k será un cuerpo perfecto de característica positiva, y conservaremos las mismas notaciones de las secciones III–A y III–B.

Proposición III–C.1 ■ Sea K una extensión de k y supongamos que $K^\sharp$ es algebraico sobre k. Para todo ideal primo $\mathcal{P} \in \operatorname{Spec}(K_{[\infty]})$ tal que $\mathcal{P} \cap k[t] = 0$, existe un $m_0 \geq 0$ tal que $\mathcal{P}_{[m]}$ es el ideal extendido de $\mathcal{P}_{[m_0]}$ para todo $m \geq m_0$.

Demostración. La extensión $k[t] \subset K^\sharp[t]$ es entera y como $\mathcal{P} \cap k[t] = 0$, entonces $\mathcal{P} \cap K^\sharp[t] = 0$.

Podemos suponer $\mathcal{P} \neq (0)$. Aplicamos la nota III–A.8 al caso $A = K$, y tenemos que

$$\operatorname{ht}(\mathcal{P}_{[i]}) = \operatorname{ht}(\mathcal{P}) = 1 \quad \text{para todo } i \geq 0.$$

Como K es cuerpo, $K[t_i]$ es un dominio de factorización única. Tomemos $F_i(t_i) \in K[t_i]$ el polinomio mónico irreducible generador de $\mathcal{P}_{[i]}$. Por el corolario I–C.2, para cada $i \geq 0$ debemos considerar dos posibilidades:

(1) $F_i \in K^p[t_i]$. En este caso, $F_{i+1}(t_{i+1}) = F_i(t_i)^{1/p}$.

(2) $F_i \notin K^p[t_i]$, entonces $\mathcal{P}_{[i+1]} = (\mathcal{P}_{[i]})^e$ y $F_{i+1}(t_{i+1}) = F_i(t_i) = F_i(t_{i+1}^p)$.

Como $\mathcal{P} \cap K^\sharp[t] = (0)$, se tiene que

$$F_0(t_0) \notin (\bigcap_{m\geq 0} K^{p^m})[t_0] = \bigcap_{m\geq 0} K^{p^m}[t_0]$$

y entonces existe un índice $m_0 \geq 0$ tal que

$$F_0(t_0) \in K^{p^{m_0}}[t_0] \text{ y } F_0(t_0) \notin K^{p^{m_0+1}}[t_0].$$

De (1) tenemos que, para $i = 0, \ldots, m_0 - 1$,

$$F_i(t_i) = F_0(t_0)^{1/p^i} \in K^{p^{m_0-i}}[t_i] \text{ y } F_{m_0}(t_{m_0}) \notin K^p[t_{m_0}].$$

Aplicando (2) repetidamente, encontramos que

$$F_{j+m_0}(t_{j+m_0}) = F_{m_0}(t_{m_0}) = F_{m_0}(t_{j+m_0}^{p^j})$$

y $\mathcal{P}_{[j+m_0]}$ es el ideal extendido de $\mathcal{P}_{[m_0]}$ para todo $j \geq 1$. ∎

Corolario III–C.2 ∎ Bajo las mismas hipótesis de la proposición III–C.1, $\mathcal{P}$ es el ideal extendido de algún $\mathcal{P}_{[m_0]}$.

Demostración. Es una consecuencia de la proposición III–C.1 y de la igualdad $\mathcal{P} = \bigcup_{m\geq 0} \mathcal{P}_{[m]}$. ∎

Sea B una álgebra libre sobre un anillo A y $S \subset A$ un subconjunto multiplicativamente cerrado. Consideremos $S^{-1}A$ y $S^{-1}B$, que es una $S^{-1}A$–álgebra libre. Denotamos por $I \mapsto I^E, J \mapsto J^C$ (resp. $I \mapsto I^e, J \mapsto J^c$) al proceso de extensión-contracción entre los anillos A o $S^{-1}A$ (resp. A o B) y los anillos B o $S^{-1}B$ (resp. $S^{-1}A$ o $S^{-1}B$).

Proposición III–C.3 ■ Con las notación anterior, sea $\mathcal{P}_1$ un ideal primo de B tal que $\mathcal{P}_1 \cap S = \varnothing$. Sea $\mathcal{P}_0 = \mathcal{P}_1^C$, $\mathfrak{P}_1 = \mathcal{P}_1^e$ y $\mathfrak{P}_0 = \mathfrak{P}_1^C$. Si $\mathfrak{P}_1 = \mathfrak{P}_0^E$, entonces $\mathcal{P}_1 = \mathcal{P}_0^E$.

Demostración. Sea $\{e_i\}$ una A–base de B. Como $\mathcal{P}_1 \cap S = \varnothing$, entonces es evidente que $\mathfrak{P}_1^c = \mathcal{P}_1$, $\mathfrak{P}_0^c = \mathcal{P}_0$ y $\mathfrak{P}_0 = \mathcal{P}_0^e$. Si $\mathfrak{P}_1 = \mathfrak{P}_0^E$, se tiene que

$$\mathcal{P}_1 = \mathcal{P}_1^{ec} = \mathfrak{P}_1^c = (\mathfrak{P}_0^E)^c = (\mathcal{P}_0^{eE})^c = (\mathcal{P}_0^{Ee})^c = (\mathcal{P}_0^E)^{ec} = \sum_{s \in S}(\mathcal{P}_0^E : s)_B \supset \mathcal{P}_0^E.$$

Para probar la otra inclusión, tomemos $s \in S \subset A$ y sea $f = \sum a_i e_i$ un elemento de $(\mathcal{P}_0^E : s)_B$ con $a_i \in A$. Entonces,

$$sf = \sum (sa_i)e_i \in \mathcal{P}_0^E$$

y de la igualdad

$$\mathcal{P}_0^E = \{\sum b_i e_i \mid b_i \in \mathcal{P}_0\},$$

deducimos que $sa_i \in \mathcal{P}_0$ y $a_i \in (\mathcal{P}_0 : s)_A$. Como $\mathcal{P}_1 \cap S = \varnothing$, entonces $\mathcal{P}_0 \cap S = \varnothing$, y se verifica que $(\mathcal{P}_0 : s)_A = \mathcal{P}_0$. Por tanto $f \in \mathcal{P}_0^E$. ■

Proposición III–C.4 ■ Sea R una k–álgebra íntegra, $K = Qt(R)$, y supongamos que $K^\sharp$ es algebraico sobre k. Entonces todo ideal primo $\mathcal{P} \in \operatorname{Spec}(R_{[\infty]})$ con $\mathcal{P} \cap k[t] = 0$ y $\mathcal{P} \cap R = 0$, es el ideal extendido de algún $\mathcal{P}_{[m_0]}$, con $m_0 \geq 0$.

Demostración. Sea $T = R - \{0\}$. Tenemos que

$$K = T^{-1}R \;\; \text{y} \;\; K_{[m]} = T^{-1}R_{[m]} \;\; \text{para todo} \;\; m \geq 0 \;\; \text{o} \;\; m = \infty.$$

Definimos $\mathfrak{P} = T^{-1}\mathcal{P}$. Fácilmente deducimos que

$$\mathfrak{P}_{[m]} = T^{-1}\mathcal{P}_{[m]} \;\; \text{para todo} \;\; m \geq 0.$$

Como $\mathcal{P} \cap k[t] = 0$, entonces $\mathfrak{P} \cap k[t] = 0$. Luego aplicando la proposición III–C.1, existe un $m_0 \geq 0$ tal que $\mathfrak{P}_{[m]}$ es el ideal extendido de $\mathfrak{P}_{[m_0]}$ para todo $m \geq m_0$.

Además, como $\mathcal{P} \cap R = 0$, entonces $\mathcal{P} \cap T = \emptyset$ y por tanto

$$\mathcal{P}_{[m]} \cap T = \mathcal{P} \cap R_{[m]} \cap T = \emptyset.$$

Luego, aplicando la proposición III–C.3, sabemos que $\mathcal{P}_{[m]}$ es el ideal extendido de $\mathcal{P}_{[m_0]}$ para todo $m \geq m_0$, y por tanto $\mathcal{P} = \bigcup_{m \geq 0} \mathcal{P}_{[m]}$ es el ideal extendido de $\mathcal{P}_{[m_0]}$. ■

Proposición III–C.5 ■ Sea K una extensión de k y supongamos que $K^\sharp$ no es algebraico sobre k. Entonces $K_{(\infty)}$ no es noetheriano.

Demostración. Sea $s \in K^\sharp$ un elemento trascendente sobre k.

Sea $L = k(s)_{per} \subset K^\sharp \subset K$. Se tiene que $L_{(\infty)} \subset K_{(\infty)}$ es una extensión de cuerpos, luego es libre y por tanto fielmente plana. Así que si $L_{(\infty)}$ no es noetheriano, entonces $K_{(\infty)}$ no puede ser noetheriano. Por tanto, podemos suponer $K = k(s)_{per}$, y en este caso $K^\sharp = K$, sí es trascendente sobre k. Entonces

$$K_{(\infty)} = k(s)_{per} \otimes_k k(t)_{per}.$$

Para cada $m \geq 0$, sea $s_m = s^{\frac{1}{p^m}} \in K$ y $\alpha_m = t_m - s_m$. Sea P el ideal de $K_{(\infty)}$ generado por los $\{\alpha_m,\ m \geq 0\}$. Se verifica que $\alpha_m = \alpha_{m+1}^p$ y $P_{(m)} = K_{(m)}\alpha_m$ para todo $m \geq 0$ es un ideal primo de $K_{(m)}$, ya que el polinomio $\alpha_m = t_m - s_m \in K[t_m]$ es mónico e irreducible.

Supongamos que P es finitamente generado, entonces existe un $m_0 \geq 0$ tal que $P = K_{(\infty)}\alpha_{m_0}$. Por ser la extensión $K_{(m_0+1)} \subset K_{(\infty)}$ fielmente plana, se tiene que

$$\alpha_{m_0+1} \in K_{(m_0+1)}\alpha_{m_0}.$$

Sea $\tau = t_{m_0+1}$, $\sigma = s_{m_0+1}$. Entonces $\alpha_{m_0+1} = \tau - \sigma \in K_{(m_0+1)}\alpha_{m_0}$ y $\alpha_{m_0} = \alpha_{m_0+1}^p = \tau^p - \sigma^p$. Por tanto, existen $\psi(\tau) \in K[\tau] = K_{[m_0+1]}$, $\varphi(\tau) \in k[\tau] \setminus \{0\}$ tales que

$$\varphi(\tau)(\tau - \sigma) = \psi(\tau)(\tau - \sigma)^p.$$

Simplificando y haciendo $\tau = \sigma$, obtenemos

$$\varphi(\sigma) = \psi(\sigma)(\sigma - \sigma)^{p-1} = 0$$

lo que contradice el hecho de que el elemento s es trascendente sobre k.

Por tanto, el ideal P no es finitamente generado y $K_{(\infty)}$ no es noetheriano. ∎

Teorema III–C.6 ∎ Sea k un cuerpo perfecto de característica $p > 0$ y sea A una k–álgebra de dimensión de Krull n. Las siguientes condiciones son equivalentes:

(a) El anillo A es noetheriano y para todo $\mathfrak{p} \in \operatorname{Spec}(A)$, el cuerpo $Qt(A/\mathfrak{p})^\sharp$ es algebraico sobre k.

(b) El anillo $A_{(\infty)}$ es noetheriano.

Demostración. Probemos (a) $\Rightarrow$ (b): Por el teorema de Cohen (cf. [Nag75], (3.4)), basta probar que todo ideal $P \in \operatorname{Spec}(A_{(\infty)}) - \{(0)\}$ es finitamente generado.

Supongamos $\operatorname{ht}(P) = r \leq n$. Entonces, utilizando los corolarios III–A.7 y III–A.10, tenemos que

$$\operatorname{ht}(P_{[m]}) = \operatorname{ht}(P_{(m)}) = \operatorname{ht}(P_{[\infty]}) = \operatorname{ht}(P) = r \leq n.$$

Consideremos el ideal primo de A:

$$\mathfrak{p} := A \cap P = A \cap P_{[\infty]} = A \cap P_{[m]} = A \cap P_{(m)}.$$

Existen dos posibles valores para la altura de $\mathfrak{p}$ (por el lema I–A.1):

(i) $\operatorname{ht}(\mathfrak{p}) = r = \operatorname{ht}(P_{[m]})$ y $P_{[m]} = \mathfrak{p}[t_m]$, para todo $m \geq 0$.

(ii) $\operatorname{ht}(\mathfrak{p}) = r - 1 = \operatorname{ht}(P_{[m]}) - 1$, y entonces $\mathfrak{p}[t_m] \subsetneq P_{[m]}$ y $A/\mathfrak{p} \subsetneq A[t_m]/P_{[m]}$ es algebraica generada por $t_m \pmod{P_{[m]}}$, para todo

$m \geq 0$.

En el caso (i), P es el ideal extendido de $\mathfrak{p}$, y por tanto está finitamente generado (ya que $\mathfrak{p} \in \operatorname{Spec}(A)$ y A es noetheriano).

Supongamos que nos encontramos en el caso (ii). Denotemos por $R = A/\mathfrak{p}$, $K = Qt(R)$. Entonces:

$$R_{[m]} = \frac{A_{[m]}}{\mathfrak{p}[t_m]}, \quad R_{[\infty]} = \frac{A_{[\infty]}}{A_{[\infty]}\mathfrak{p}} = \frac{A_{[\infty]}}{\bigcup_{m\geq 0} \mathfrak{p}[t_m]}.$$

Definimos

$$\mathcal{P} := R_{[\infty]}P_{[\infty]} = \frac{P_{[\infty]}}{\bigcup_{m\geq 0} \mathfrak{p}[t_m]} \in \operatorname{Spec}(R_{[\infty]}).$$

Se tiene que

$$\mathcal{P}_{[m]} = \mathcal{P} \cap R_{[m]} = \frac{P_{[m]}}{\mathfrak{p}[t_m]}, \quad \mathcal{P} \cap R = \mathcal{P} \cap k[t] = 0$$

y por tanto

$$\operatorname{ht}(\mathcal{P}_{[m]}) = \operatorname{ht}\left(\frac{P_{[m]}}{\mathfrak{p}[t_m]}\right) = 1, \quad \operatorname{ht}(\mathcal{P}) = \operatorname{ht}\left(\frac{P_{[\infty]}}{\bigcup_{m\geq 0} \mathfrak{p}[t_m]}\right) = 1.$$

Como por hipótesis $K^\sharp$ es algebraico sobre k, aplicando la proposición III–C.4, existe un $m_0 \geq 0$ tal que $\mathcal{P}$ es el ideal extendido de $\mathcal{P}_{[m_0]}$. Entonces $P_{[\infty]}$ es el ideal extendido de $P_{[m_0]}$ y $P = A_{(\infty)}P_{[\infty]} = A_{(\infty)}P_{[m_0]}$ está finitamente generado.

Probemos ahora que (b) implica (a): Puesto que $A_{(\infty)}$ es fielmente plano sobre A y por hipótesis $A_{(\infty)}$ es noetheriano, se concluye que A es noetheriano.

Sea $\mathfrak{p} \in \operatorname{Spec}(A)$ y $R = A/\mathfrak{p}$, $K = Qt(R)$. La noetherianidad de $A_{(\infty)}$ implica, en primer lugar, la noetherianidad de $R_{(\infty)}$, y en segundo lugar, la de $K_{(\infty)}$. Por último, aplicando la proposición III–C.5,

$$K^\sharp = Qt\left(\frac{A}{\mathfrak{p}}\right)^\sharp$$

es algebraico sobre k. ∎

Corolario III–C.7 ■ Sea k un cuerpo perfecto de característica $p > 0$ and sea A una k–álgebra noetheriana. Las siguientes condiciones son equivalentes:

(a) El anillo $A_{(\infty)}$ es noetheriano.

(b) El anillo $(A_{\mathfrak{m}})_{(\infty)}$ es noetheriano para todo ideal maximal $\mathfrak{m}$ de A.

Demostración. Para (a) $\Rightarrow$ (b), como $A_{(\infty)}$ es noetheriano, por el teorema III–C.6, se tiene que A es noetheriano y por tanto también $A_{\mathfrak{m}}$ para todo $\mathfrak{m} \in \Omega(A)$. Por la nota 7 de III–A.1, $(A_{\mathfrak{m}})_{(\infty)} = \left(A_{(\infty)}\right)_{\mathfrak{m}}$ y usando que

$$\left(A_{(\infty)}\right)_{\mathfrak{m}} = A_{\mathfrak{m}} \otimes_A A_{(\infty)},$$

se tiene que $(A_{\mathfrak{m}})_{(\infty)}$ es noetheriano para todo $\mathfrak{m} \in \Omega(A)$.

Para (b) $\Rightarrow$ (a), sea $\mathfrak{p} \subset A$ un ideal primo y sea $\mathfrak{m}$ un ideal maximal que contiene a $\mathfrak{p}$. Como el anillo $(A_{\mathfrak{m}})_{(\infty)}$ es noetheriano, entonces por el teorema III–C.6, deducimos que el anillo $A_{\mathfrak{m}}$ también es noetheriano y el cuerpo

$$Qt\left(\frac{A_{\mathfrak{m}}}{A_{\mathfrak{m}}\mathfrak{p}}\right)^{\sharp} = Qt\left(\frac{A}{\mathfrak{p}}\right)^{\sharp}$$

es una extensión algebraica de k. Además, como A es noetheriano, aplicando de nuevo el teorema III–C.6, obtenemos la condición (a). ■

Corolario III–C.8 ■ Sea k un cuerpo perfecto de característica $p > 0$, k' una extensión algebraica de k y $A = k'[[X_1, \ldots, X_n]]$. Entonces, el anillo $A_{(\infty)} = k(t)_{per} \otimes_k A$ es noetheriano.

Demostración. Como k es perfecto y k' es una extensión algebraica de k, por el lema III–B.4, k' también es perfecto.

En particular $A = k'[[X_1, \ldots, X_n]]$ es una k–álgebra, por ser k' una extensión algebraica de k. Sean $\mathfrak{p} \in \mathrm{Spec}(A)$ y $K = A/\mathfrak{p}$. Aplicando la proposición III–B.6, $K^\sharp$ es una extensión algebraica de k. Y además, como A es noetheriano, aplicando el teorema III–C.6, $A_{(\infty)} = k(t)_{per} \otimes_k A$ es noetheriano. ∎

Corolario III–C.9 ∎ Sea k un cuerpo perfecto de característica $p > 0$. Si $(B, \mathfrak{m})$ es una k–álgebra noetheriana local tal que $B/\mathfrak{m}$ es algebraico sobre k, entonces $B_{(\infty)} = k(t)_{per} \otimes_k B$ es noetheriano. En particular, el cuerpo $Qt(B/\mathfrak{p})^\sharp$ es algebraico sobre k para todo ideal primo $\mathfrak{p}$ de B.

Demostración. Sea $k' = B/\mathfrak{m}$ algebraico sobre k. Por el teorema de estructura de Cohen (I–B.10), la completación $\hat{B}$ de B es un cociente de un anillo de series A con coeficientes en k', $\hat{B} = A/I$, con I ideal primo de A. Además, como por la nota 6 de III–A.1 $\hat{B}_{(\infty)}$ es también un cociente of $A_{(\infty)}$ ($\hat{B}_{(\infty)} = (A/I)_{(\infty)} = A_{(\infty)}/IA_{(\infty)}$), deducimos del corolario III–C.8 que $A_{(\infty)}$ es noetheriano y por tanto $\hat{B}_{(\infty)} = A_{(\infty)}/IA_{(\infty)}$ también.

Como $(B, \mathfrak{m})$ es una k–álgebra local noetheriana, $\hat{B}$ es fielmente plano sobre B, y entonces $\hat{B}_{(\infty)}$ es también fielmente plano sobre $B_{(\infty)}$. Por tanto, B_∞ es noetheriano. Por último, aplicando el teorema III–C.6, se tiene que el cuerpo $Qt(B/\mathfrak{p})^\sharp$ es algebraico sobre k, para todo $\mathfrak{p} \in \mathrm{Spec}(B)$. ∎

Corolario III–C.10 ∎ Sea k un cuerpo perfecto de característica $p > 0$. Para cualquier k–álgebra noetheriana A, tal que el cuerpo residual $A/\mathfrak{m}$ de todo ideal maximal $\mathfrak{m}$ de A es algebraico sobre k, el anillo $A_{(\infty)}$ es noetheriano. Por tanto, si A es regular y equicodimensional, entonces $A_{(\infty)}$ es también regular y equicodimensional, de la misma dimensión que A.

Demostración. En primer lugar, como A es una k–álgebra noetheriana tal que para todo $\mathfrak{m} \in \Omega(A)$, $A/\mathfrak{m}$ es algebraico sobre A, se tiene que $A_\mathfrak{m}$ es una k–álgebra noetheriana local, tal que su cuerpo residual $A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m} = A/\mathfrak{m}$ es algebraico sobre k. Aplicando el corolario III–C.9, $(A_\mathfrak{m})_{(\infty)}$ es noetheriano para todo $\mathfrak{m} \in \Omega(A)$. Entonces, aplicando el corolario III–C.7, $A_{(\infty)}$ es noetheriano.

Por último, si la k-álgebra A es regular y equicodimensional, entonces todos los $A_{(m)}$ para todo $m \geq 0$ son regulares y de la misma dimensión (homológica global=Krull) que A (por I–A.3). Y por el corolario III–A.11 y [Ber58], $A_{(\infty)}$ es regular y equicodimensional de la misma dimensión que A. ∎

CAPÍTULO IV

Derivaciones de Hasse-Schmidt y cuerpos de coeficientes.

En este capítulo presentamos una extensión del teorema 99 de H. Matsumura ([Mat80]), al caso de las derivaciones de Hasse-Schmidt. La herramienta principal para esta demostración, se encuentra en el teorema IV–A.6, donde se muestra una condición suficiente para que todo derivación de Hasse-Schmidt pueda expresarse en función unas fijas.

IV–A Generación de Derivaciones de Hasse-Schmidt.

En primer lugar, recordamos los resultados que queremos generalizar al caso de derivaciones de Hasse-Schmidt.

Lema IV–A.1 ■ Sea A dominio de integridad y consideremos las extensiones $k_0 \subset k \subset A$, con $k_0 \subset k$ algebraica separable. Entonces $HS_{k_0}(A) = HS_k(A)$.

Demostración. Sea $\underline{D} \in HS_{k_0}(A)$, veamos que $D_i(k) = 0$, para todo $i \geq 1$: Sea $b \in k - k_0$ entonces existe

$$p(X) = \sum_{k=0}^{n} a_k X^k \in k_0[X]$$

polinomio mínimo de b (es decir $p(b) = 0$ y $p'(b) \neq 0$). En primer lugar probaremos que si

$$D_l(b) = 0$$

para $l = 1, \ldots, i$, entonces

$$D_{i+1}(p(b)) = D_{i+1}(b)p'(b), \tag{(IV–A.1)}$$

y lo haremos por inducción sobre el grado de $p(X)$:

- si el grado de $p(X) = 1$, o sea,

  $$p(X) = a_1 X + a_0,$$

  entonces

  $$p'(X) = a_1 = p'(b).$$

  Además, $a_1, a_0 \in k_0$, luego

  $$D_{i+1}(a_0) = D_{i+1}(a_1) = 0$$

  y por tanto

  $$D_{i+1}(p(b)) = a_1 D_{i+1}(b) + b D_{i+1}(a_1) + D_{i+1}(a_0) = D_{i+1}(b)p'(b).$$

- Supongamos cierto para grado de $p(X) = k = 1, \ldots, n-1$, veamos que es cierto para $k = n$: sea $p(X)$ de grado n. Escribamos $p(X)$ como

  $$p(X) = a_0 + Xq(X)$$

siendo $q(X)$ de grado $n-1$ y se tiene

$$p(b) = a_0 + bq(b)$$

y

$$p'(b) = q(b) + bq'(b).$$

Así que

$$\begin{aligned} D_{i+1}(p(b)) = {} & D_{i+1}(a_0) + D_{i+1}(bq(b)) = D_{i+1}(bq(b)) = D_{i+1}(b)q(b) + \\ + & \sum_{\substack{r+s=i+1 \\ r,s\neq 0}} D_r(b)D_s(q(b)) + bD_{i+1}(q(b)) = \\ = {} & (\text{ aplicando que } D_l(b) = 0 \text{ para } l = 1,\dots,i) = \\ = {} & D_{i+1}(b)q(b) + bD_{i+1}(q(b)) = \\ = {} & (\text{aplicando hipótesis de inducción sobre k}) = \\ = {} & D_{i+1}(b)q(b) + bD_{i+1}(b)q'(b) = D_{i+1}(b)p'(b). \end{aligned}$$

Probemos ahora que $D_i(b) = 0$ para todo $i \geq 1$:

- $D_1(p(b)) = a_n nb^{n-1}D_1(b) + \cdots + a_1D_1(b) = p'(b)D_1(b) = 0$, además como $p'(b) \neq 0$ y A es dominio de integridad, entonces $D_1(b) = 0$.
- Supongamos $D_j(b) = 0$ para $j = 1,\dots,i$, entonces

  $$0 = D_{i+1}(p(b)) = D_{i+1}(b)p'(b)$$

  (por (IV–A.1)). Usando el mismo razonamiento anterior, se tiene que $D_{i+1}(b) = 0$. ∎

A continuación enunciamos el resultado que deseamos generalizar.

Teorema IV–A.2 ∎ *(cf. teorema 99, de [Mat80])* Sea $(R, \mathfrak{m})$ anillo local, regular, equicaracterístico de dimensión n. Sea $\hat{R}$ el completado de R y k un cuerpo de coeficientes de $\widehat{R}$ que contiene a un cuerpo de casi–coeficientes k_0 de R. Sea $X_1, \ldots, X_n$ un sistema regular de parámetros de R, entonces $\widehat{R} = k[[X_1, \ldots, X_n]]$ y $\mathrm{Der}_k(\widehat{R})$ es un $\widehat{R}$–módulo libre con las derivadas parciales $\frac{\partial}{\partial X_1}, \ldots, \frac{\partial}{\partial X_n}$ como base. Bajo estas condiciones, son equivalentes:

1. $\frac{\partial}{\partial X_i}$ $(1 \leq i \leq n)$ son aplicaciones de R en R, es decir, $\frac{\partial}{\partial X_i} \in \mathrm{Der}_{k_0}(R)$.
2. Existen $D_1, \ldots, D_n \in \mathrm{Der}_{k_0}(R)$ y elementos $a_1, \ldots, a_n \in R$ tales que $D_i a_k = \delta_{ik}$.
3. Existen $D_1, \ldots, D_n \in \mathrm{Der}_{k_0}(R)$ y elementos $a_1, \ldots, a_n \in R$ tales que
$$\det(D_i a_k) \notin \mathfrak{m}.$$
4. $\mathrm{Der}_{k_0}(R)$ es un R–módulo libre de rango n, de base $\{D_1, \ldots, D_n\}$.
5. $\mathrm{rg}(\mathrm{Der}_{k_0}(R)) = n$.

Nota IV–A.3 ■ La mención a k_0 es innecesaria, puesto que $\mathrm{Der}_{k_0}(\widehat{R}) = \mathrm{Der}_k(\widehat{R})$ por el lema IV–A.1, y
$$\mathrm{Der}_{k_0}(R) = \mathrm{Der}(R) \cap \mathrm{Der}_k(\widehat{R})$$
(ver la demostración del teorema 99 *de [Mat80]).*

Corolario IV–A.4 ■ Sea $(R, \mathfrak{m})$ anillo local, regular, equicaracterístico de dimensión n. Sea $\widehat{R}$ el completado de R y k un cuerpo de coeficientes de $\widehat{R}$ que contiene a un cuerpo de casi–coeficientes k_0 de R. Sea $\{X_1, \ldots, X_n\}$ un sistema regular de parámetros de R, entonces $\widehat{R} = k[[X_1, \ldots, X_n]]$ y $\mathrm{Der}_k(\widehat{R})$ es un $\widehat{R}$–módulo libre con las derivadas parciales $\frac{\partial}{\partial X_1}, \ldots, \frac{\partial}{\partial X_n}$ como base. Si existen $D_1, \ldots, D_n \in \mathrm{Der}_{k_0}(R)$ y $a_1, \ldots, a_n \in R$ tales que $\det(D_i a_k) \notin R$, entonces sus extensiones $\widehat{D}_1, \ldots, \widehat{D}_n$ a la completación $\widehat{R}$, son una base de $\mathrm{Der}_k(\widehat{R})$.

Demostración. Por el teorema IV–A.2 ($2 \Rightarrow 4$), se tiene que $\mathrm{Der}_{k_0}(R)$ es un R-módulo libre de rango n siendo una base $\{D_1, \ldots, D_n\}$, y como la extensión de anillos $R \subset \hat{R}$ es fielmente plana, sus extensiones $\{\hat{D}_1, \ldots, \hat{D}_n\}$ al completado $\hat{R}$, siguen siendo linealmente independientes en $\hat{R}$. Además por el ~~lema~~ propr IV–A.~~1~~4, $\hat{D}_j \in \mathrm{Der}_k(\hat{R})$. Por tanto

$$\frac{\partial}{\partial X_i} = \sum_{j=1}^{n} c_{ij}\hat{D}_j \quad \text{con} \quad c_{ij} \in L = Qt(\hat{R}).$$

Además, dado que

$$\det(\hat{D}_j(a_k)) = \det(D_j(a_k)) \notin \mathfrak{m},$$

y $\det(\hat{D}_j(a_k)) = \det(D_j(a_k)) \in R$, se tiene que $\det(\hat{D}_j(a_k)) \notin \hat{\mathfrak{m}}$ y es inversible en $\hat{R}$. Por último, resolviendo las ecuaciones

$$\frac{\partial}{\partial X_i}(a_k) = \sum_{j=1}^{n} c_{ij}\hat{D}_j(a_k)$$

se tiene que los $c_{ij} \in R \subset \hat{R}$ y, por tanto, el resultado. ∎

Corolario IV–A.5 ∎ Si en el teorema IV–A.2, R contiene un cuerpo de característica 0, $D_1, \ldots, D_n$ son las derivaciones como en el apartado 3, y $\hat{D}_1, \ldots, \hat{D}_n$ sus extensiones a la completación $\hat{R}$, entonces

$$k = \{a \in \hat{R} \mid \hat{D}_i(a) = 0, \ \forall i\}.$$

Demostración. Como k es un cuerpo de coeficientes de $\hat{R}$, $\hat{R}$ es el anillo de series formales en $X_1, \ldots, X_n$ con coeficientes en el cuerpo k de característica cero y $\mathrm{Der}_k(\hat{R})$ es un $\hat{R}$-módulo libre con las derivadas parciales $\frac{\partial}{\partial X_1}, \ldots, \frac{\partial}{\partial X_n}$ como base, se tiene que

$$k = \{a \in \hat{R} \mid \frac{\partial}{\partial X_i}(a) = 0, \ \forall i\}.$$

Además, por el corolario IV–A.4, $\hat{D}_1, \ldots, \hat{D}_n$ son una base de $\mathrm{Der}_k(\hat{R})$ y de ahí el resultado. ∎

A partir de ahora, usaremos la misma notación que en I–D.10 para manejar n–uplas: Notaremos $\lambda = (\lambda_1, \ldots, \lambda_n)$, $\mu = (\mu_1, \ldots, \mu_n)$, donde $|\lambda| = \lambda_1 + \cdots + \lambda_n$.

En primer lugar probaremos el siguiente resultado:

Teorema IV–A.6 ■ Sea k un anillo y R una k–álgebra. Sean $\underline{\mathfrak{D}}, \underline{D}^1, \ldots \underline{D}^n \in HS_k(R)$

- Si $\{D_1^1, \ldots, D_1^n\}$ es un sistema generador de $Der_k(R)$ como R–módulo, entonces existen n sucesiones $\{C_{ld}\}_{l \in \mathbb{N}}$, $(1 \leq d \leq n)$ de elementos de R, tales que:

$$\mathfrak{D}_i = \sum_{m=1}^{i} \left(\sum_{\substack{|\lambda|=i,\ |\mu|=m \\ \lambda_d \geq \mu_d \geq 0}} \prod_{d=1}^{n} \sum_{\substack{l_1^d + \cdots + l_{\mu_d}^d = \lambda_d \\ l_q^d \geq 1}} \prod_{q=1}^{\mu_d} C_{l_q^d d} \right) D_\mu, \quad \forall i \geq 1; \tag{(IV–A.2)}$$

donde convenimos $D_\mu = D_{\mu_1}^1 \circ \cdots \circ D_{\mu_n}^n$, para todo $\mu \in \mathbb{N}^n$ y

$$\sum_{\substack{l_1^d + \cdots + l_{\mu_d}^d = \lambda_d \\ l_q^d \geq 1}} \prod_{q=1}^{\mu_d} C_{l_q^d d} = \begin{cases} 0 & \text{si } \mu_d = 0 < \lambda_d \\ 1 & \text{si } \mu_d = \lambda_d = 0. \end{cases}$$

- Si $\{D_1^1, \ldots, D_1^n\}$ es una base de $Der_k(R)$, entonces los $\{C_{ld}\}$ son únicos.

Ejemplo IV–A.7 ■ Supongamos $n = 2$ (es decir, $\widehat{R} = k[[X_1, X_2]]$), entonces

$\mathfrak{D}_1 = C_{11} D_1^1 + C_{12} D_1^2,$

$\mathfrak{D}_2 = C_{21} D_1^1 + C_{22} D_1^2 + C_{11}^2 D_2^1 + C_{11} C_{12} D_1^1 \circ D_1^2 + C_{12}^2 D_2^2,$

$\mathfrak{D}_3 = C_{31} D_1^1 + C_{32} D_1^2 + 2C_{11} C_{21} D_2^1 + (C_{21} C_{12} + C_{11} C_{22}) D_1^1 \circ D_1^2 + 2C_{12} C_{22} D_2^2 +$

$$+C_{11}^3 D_3^1 + C_{11}^2 C_{12} D_2^1 \circ D_1^2 + C_{11} C_{12}^2 D_1^1 D_2^2 + C_{12}^3 D_3^2.$$

$\vdots$

Demostración. La prueba se hará por inducción sobre i: Supongamos que el conjunto $\{D_1^1, \dots, D_1^n\}$ es una R–base de $Der_k(R)$ (en el caso de que dicho conjunto sea un sistema de generadores, la demostración es igual, pero no se probará la unicidad de los C_{ld}).

Para $i = 1$: $\mathfrak{D}_1$ es derivación, entonces existen unos únicos coeficientes $C_{11}, \dots, C_{1n} \in R$ tales que

$$\mathfrak{D}_1 = C_{11} D_1^1 + \cdot \cdot \cdot + C_{1n} D_1^n.$$

Supongamos construidos $C_{ld} \in R$, $1 \leq l \leq N-1$, $1 \leq d \leq n$, tales que se verifica (IV–A.2), para $1 \leq i \leq N-1$. Probaremos que

$$\mathfrak{D}_N - \sum_{m=2}^{N} \left(\sum_{\substack{|\alpha|=N, |\mu|=m \\ \alpha_d \geq \mu_d \geq 0}} \prod_{d=1}^{n} \sum_{\substack{l_1^d + \cdots + l_{\mu_d}^d = \alpha_d \\ l_q^d \geq 1}} \prod_{q=1}^{\mu_d} C_{l_q^d d} \right) D_\mu$$

es una k–derivación; y de nuevo, por ser $\{D_1^1, \dots, D_1^n\}$ una R–base de $Der_k(R)$, existen unos únicos coeficientes $C_{N1}, \dots, C_{Nn} \in R$ que cumplen lo pedido.

Trivialmente es k–lineal. Veamos que cumple la condición para el producto de dos elementos, para lo cual necesitamos el siguiente:

Aserto: En las condiciones anteriores, y dados $a,\ b \in R$ se tiene que

$$D_\mu(a \cdot b) = \sum_{\rho + \sigma = \mu} D_\rho(a) D_\sigma(b).$$

Demostración del Aserto.

$$D_\mu(a\cdot b) = (D^1_{\mu_1}\circ\cdots\circ D^{n-1}_{\mu_{n-1}})\left(\sum_{\substack{\rho_n+\sigma_n=\mu_n\\ \rho_n,\sigma_n\geq 0}} D_{\rho_n}(a)\cdot D_{\sigma_n}(b)\right) =$$

$$= \cdots\cdots\cdots = \sum_{\rho+\sigma} D_\rho(a)\cdot D_\sigma(b).$$

■

Dados $a, b \in R$

$$\left[\mathfrak{D}_N - \sum_{m=2}^{N}\left(\sum_{\substack{|\alpha|=N,|\mu|=m\\ \alpha_d\geq\mu_d\geq 0}}\prod_{d=1}^{n}\sum_{\substack{l_1^d+\cdots+l_{\mu_d}^d=\alpha_d\\ l_q^d\geq 1}}\prod_{q=1}^{\mu_d} C_{l_q^d d}\right) D_\mu\right](a\cdot b) =$$

$$= \mathfrak{D}_N(a)\cdot b + a\cdot\mathfrak{D}_N(b) + \sum_{\substack{v+w=N\\ 1\leq v,w\leq N-1}}\mathfrak{D}_v(a)\mathfrak{D}_w(b) -$$

$$-\sum_{m=2}^{N}\left(\sum_{\substack{|\alpha|=N,|\mu|=m\\ \alpha_d\geq\mu_d\geq 0}}\prod_{d=1}^{n}\sum_{\substack{l_1^d+\cdots+l_{\mu_d}^d=\alpha_d\\ l_q^d\geq 1}}\prod_{q=1}^{\mu_d} C_{l_q^d d}\right)\cdot\left(\sum_{\substack{\rho+\sigma=\mu\\ \rho,\sigma\geq\underline{0}}} D_\rho(a)D_\sigma(b)\right) =$$

$$= \mathfrak{D}_N(a)\cdot b + a\cdot\mathfrak{D}_N(b) + \sum_{\substack{v+w=N\\ 1\leq v,w\leq N-1}}\mathfrak{D}_v(a)\mathfrak{D}_w(b) -$$

$$-\sum_{m=2}^{N}\left(\sum_{\substack{|\alpha|=N,|\mu|=m\\ \alpha_d\geq\mu_d\geq 0}}\prod_{d=1}^{n}\sum_{\substack{l_1^d+\cdots+l_{\mu_d}^d=\alpha_d\\ l_q^d\geq 1}}\prod_{q=1}^{\mu_d} C_{l_q^d d}\right)\cdot(D_\mu(a)\cdot b + a\cdot D_\mu(b)) -$$

$$-\sum_{m=2}^{N}\left(\sum_{\substack{|\alpha|=N,|\mu|=m\\ \alpha_d\geq\mu_d\geq 0}}\prod_{d=1}^{n}\sum_{\substack{l_1^d+\cdots+l_{\mu_d}^d=\alpha_d\\ l_q^d\geq 1}}\prod_{q=1}^{\mu_d}C_{l_q^d d}\right)\cdot\left(\sum_{\substack{\rho+\sigma=\mu\\ \rho,\sigma>\underline{0}}}D_\rho(a)D_\sigma(b)\right)$$

Si probamos que

$$\sum_{\substack{v+w=N\\ 1\leq v,w\leq N-1}}\mathfrak{D}_v(a)\mathfrak{D}_w(b)=$$

$$=\sum_{m=2}^{N}\left(\sum_{\substack{|\alpha|=N,|\mu|=m\\ \alpha_d\geq\mu_d\geq 0}}\prod_{d=1}^{n}\sum_{\substack{l_1^d+\cdots+l_{\mu_d}^d=\alpha_d\\ l_q^d\geq 1}}\prod_{q=1}^{\mu_d}C_{l_q^d d}\right)\cdot\left(\sum_{\substack{\rho+\sigma=\mu\\ \rho,\sigma>\underline{0}}}D_\rho(a)D_\sigma(b)\right),$$

entonces se tiene lo pedido. En efecto:

$$\sum_{\substack{v+w=N\\ 1\leq v,w\leq N-1}}\mathfrak{D}_v(a)\mathfrak{D}_w(b)=[\text{hip. inducción}]=$$

$$=\sum_{\substack{v+w=N\\ 1\leq v,w\leq N-1}}\left[\sum_{r=1}^{v}\left(\sum_{\substack{|\tau|=v,|\rho|=r\\ \tau\geq\rho;\ \rho_t,\tau_t\geq 0}}\prod_{d=1}^{n}\sum_{\substack{l_1^d+\cdots+l_{\rho_d}^d=\tau_d\\ l_q^d\geq 1}}\prod_{q=1}^{\rho_d}C_{l_q^d d}\right)D_\rho(a)\right]\cdot$$

$$\cdot\left[\sum_{s=1}^{w}\left(\sum_{\substack{|\omega|=w,|\sigma|=s\\ \omega\geq\sigma;\ \omega_t,\sigma_t\geq 0}}\prod_{d=1}^{n}\sum_{\substack{l_1^d+\cdots+l_{\sigma_d}^d=\omega_d\\ l_{q'}^d\geq 1}}\prod_{q'=1}^{\rho_d}C_{l_{q'}^d d}\right)D_\sigma(b)\right],$$

y por otro lado

$$\sum_{m=2}^{N}\left(\sum_{\substack{|\alpha|=N,|\mu|=m\\ \alpha_d\geq\mu_d\geq 0}}\prod_{d=1}^{n}\sum_{\substack{l_1^d+\cdots+l_{\mu_d}^d=\alpha_d\\ l_q^d\geq 1}}\prod_{q=1}^{\mu_d}C_{l_q^d d}\right)\cdot\left(\sum_{\rho+\sigma=\mu}D_\rho(a)D_\sigma(b)\right)=$$

$$=\sum_{m=2}^{N}\sum_{\substack{|\alpha|=N,|\mu|=m\\ \alpha_d\geq\mu_d\geq 0}}\sum_{\rho+\sigma=\mu}\left(\prod_{d=1}^{n}\sum_{\substack{l_1^d+\cdots+l_{\mu_d}^d=\alpha_d\\ l_q^d\geq 1}}\prod_{q=1}^{\mu_d}C_{l_q^d d}\right)D_\rho(a)D_\sigma(b)=$$

$$=\sum_{m=2}^{N}\sum_{\substack{|\alpha|=N,|\mu|=m\\ \alpha_d\geq\mu_d\geq 0}}\sum_{\rho+\sigma=\mu}\sum_{\substack{v+w=N\\ 1\leq v,w\leq N-1}}\sum_{\tau_1+\cdots+\tau_n=v}\prod_{d=1}^{n}$$

$$\left(\sum_{\substack{l_1^d+\cdots+l_{\rho_d}^d=\tau_d\\ l_q^d\geq 1}}\sum_{\substack{l_{\rho_d+1}^d+\cdots+l_{\mu_d}^d=\alpha_d-\tau_d\\ l_q^d\geq 1}}\prod_{q=1}^{\rho_d}C_{l_q^d d}\cdot D_\rho(a)\prod_{q'=\rho_d+1}^{\mu_d}C_{l_{q'}^d d}\cdot D_\sigma(b)\right)=$$

$=$ [Llamamos $\alpha_1-\tau_1=\omega_1,\ldots,\alpha_n-\tau_n=\omega_n$] $=$

$$=\sum_{m=2}^{N}\sum_{\substack{|\alpha|=N,|\mu|=m\\ \alpha_d\geq\mu_d\geq 0}}\sum_{\rho+\sigma=\mu}\sum_{\substack{v+w=N\\ 1\leq v,w\leq N-1}}\sum_{\tau_1+\cdots+\tau_n=l}$$

$$\left(\prod_{d=1}^{n}\sum_{\substack{l_1^d+\cdots+l_{\rho_d}^d=\tau_d\\ l_q^d\geq 1}}\prod_{q=1}^{\rho_d}C_{l_q^d d}D_\rho(a)\right)\cdot\left(\prod_{d=1}^{n}\sum_{\substack{l_1^d+\cdots+l_{\sigma_d}^d=\omega_d\\ l_q^d\geq 1}}\prod_{q'=1}^{\sigma_d}C_{l_{q'}^d d}D_\sigma(b)\right)=$$

$$= \sum_{\substack{v+w=N \\ 1\le v,w\le N-1}} \sum_{m=2}^{N} \sum_{\substack{r+s=m \\ 1\le r\le v \\ 1\le s\le w}} \sum_{\substack{|\tau|=v,\ |\rho|=r \\ |\omega|=w,\ |\sigma|=s \\ \tau_t\ge\rho_t\ge 0,\ \omega_t\ge\sigma_t\ge 0}} \left(\prod_{d=1}^{n} \sum_{\substack{l_1^d+\cdots+l_{\rho_d}^d=\tau_d \\ l_q^d\ge 1}} \prod_{q=1}^{\rho_d} C_{l_q^d d} D_\rho(a) \right) \cdot$$

$$\cdot \left(\prod_{d=1}^{n} \sum_{\substack{l_1^d+\cdots+l_{\sigma_d}^d=\omega_d \\ l_q^d\ge 1}} \prod_{q'=1}^{\sigma_d} C_{l_{q'}^d d} D_\sigma(b) \right) =$$

$$= \sum_{\substack{v+w=N \\ 1\le v,w\le N-1}} \sum_{m=2}^{N} \sum_{\substack{r+s=m \\ 1\le r\le v \\ 1\le s\le w}} \left[\sum_{\substack{|\tau|=v,\ |\rho|=r \\ \tau_t\ge\rho_t\ge 0}} \left(\prod_{d=1}^{n} \sum_{\substack{l_1^d+\cdots+l_{\rho_d}^d=\tau_d \\ l_q^d\ge 1}} \prod_{q=1}^{\rho_d} C_{l_q^d d} \right) D_\rho(a) \right] \cdot$$

$$\cdot \left[\sum_{\substack{|\omega|=w,\ |\sigma|=s \\ \omega_t\ge\sigma_t\ge 0}} \left(\prod_{d=1}^{n} \sum_{\substack{l_1^d+\cdots+l_{\sigma_d}^d=\omega_d \\ l_q^d\ge 1}} \prod_{q'=1}^{\sigma_d} C_{l_{q'}^d d} \right) D_\sigma(b) \right] =$$

si llamamos

$$\varphi_{r,v} = \sum_{\substack{|\tau|=v,\ |\rho|=r \\ \tau_t\ge\rho_t\ge 0}} \left(\prod_{d=1}^{n} \sum_{\substack{l_1^d+\cdots+l_{\rho_d}^d=\tau_d \\ l_q^d\ge 1}} \prod_{q=1}^{\rho_d} C_{l_q^d d} \right) D_\rho(a),$$

$$\psi_{s,w} = \sum_{\substack{|\omega|=w,\ |\sigma|=s \\ \omega_t \geq \sigma_t \geq 0}} \left(\prod_{d=1}^{n} \sum_{\substack{l_1^d+\cdots+l_{\sigma_d}^d=\omega_d \\ l_q^d \geq 1}} \prod_{q'=1}^{\sigma_d} c_{l_{q'}^d d} \right) D_\sigma(b).)$$

$$= \sum_{\substack{v+w=N \\ 1\leq v,w\leq N-1}} \sum_{m=2}^{N} \sum_{\substack{r+s=m \\ 1\leq r\leq v \\ 1\leq s\leq w}} \varphi_{r,v}\psi_{s,w} = \sum_{\substack{v+w=N \\ 1\leq v,w\leq N-1}} \sum_{\substack{(r,s) \\ 1\leq r\leq v \\ 1\leq s\leq w}} \varphi_{r,v}\psi_{s,w} =$$

$$= \sum_{\substack{v+w=N \\ 1\leq v,w\leq N-1}} \left[\sum_{r=1}^{v} \sum_{\substack{|\tau|=v,\ |\rho|=r \\ \tau_t\geq\rho_t\geq 0}} \left(\prod_{d=1}^{n} \sum_{\substack{l_1^d+\cdots+l_{\rho_d}^d=\tau_d \\ l_q^d\geq 1}} \prod_{q=1}^{\rho_d} c_{l_q^d d} \right) D_\rho(a) \right] \cdot$$

$$\cdot \left[\sum_{s=1}^{w} \sum_{\substack{|\omega|=w,\ |\sigma|=s \\ \omega_t\geq\sigma_t\geq 0}} \left(\prod_{d=1}^{n} \sum_{\substack{l_1^d+\cdots+l_{\sigma_d}^d=\omega_d \\ l_q^d\geq 1}} \prod_{q'=1}^{\rho_d} c_{l_{q'}^d d} \right) D_\sigma(b) \right].$$

■

Nota IV–A.8 ■ En el caso $n = 1$, si $\underline{D} \in HS_k(R)$ es tal que D_1 es un generador como R–módulo de $Der_k(R)$, entonces dada otra $\underline{\mathfrak{D}} \in HS_k(R)$, existe un $\underline{c} \in R^{\mathbb{N}}$ tal que

$$\mathfrak{D}_i = \sum_{m=1}^{i} \left(\sum_{\substack{l_1+\cdots+l_m=i \\ l_q\geq 1}} \prod_{q=1}^{m} c_{l_q} \right) D_m$$

y notaremos $\underline{\mathfrak{D}} = \underline{c} \star \underline{D}$. Podemos considerar $\star$ como una "nueva" operación, que juega un papel análogo a la estructura de R–módulo sobre

$Der_k(R)$.

La siguiente proposición generaliza el lema IV–A.1, al caso de extensiones formalmente étale.

Proposición IV–A.9 ■ Sea A dominio de integridad y consideremos las extensiones $k_0 \subset k \subset A$, con $k_0 \subset k$ formalmente étale. Entonces $HS_{k_0}(A) = HS_k(A)$.

Demostración. Sea $\underline{D} \in HS_{k_0}(A)$, veamos que $D_i(k) = 0$ para todo $i \geq 1$: Consideremos

$$k_0 \overset{i}{\hookrightarrow} k \xrightarrow{f} A \xrightarrow{1_A} A$$

homomorfismos de anillos. Sea t una indeterminada sobre A. Consideremos los anillos

$$A_m = A[t]/(t^{m+1}) \quad (m \geq 0) \text{ y } A_\infty = A[[t]].$$

Podemos considerar, de manera natural, a A_m ($m \leq \infty$) como una k–álgebra, y en particular, como una k_0–álgebra. Sabemos por el lema I–D.2, que la aplicación $E_t : A \longrightarrow A_m$ definida por

$$E_t(x) = \sum_{i=0}^{\infty} D_i(x) t^i$$

es un homomorfismo de k_0–álgebras que verifica

$$E_t(x) \equiv x \pmod{t}.$$

Consideremos el siguiente diagrama

$$\begin{array}{ccc}
k & \xrightarrow{f} & A = \dfrac{A[t]}{(t)} \\
\uparrow i & E_t \searrow\searrow \varphi & \uparrow j \\
k_0 & \xrightarrow{h} & A_{m+1} = \dfrac{A[t]}{(t^{m+2})}
\end{array}$$

donde h, j son las aplicaciones naturales, y E_t y φ dos levantamientos que hacen conmutativos ambos diagramas siendo

$$E_t : k \longrightarrow A_{m+1}$$

definida por

$$E_t(\lambda) = \lambda + D_1(\lambda)t + \cdots + D_{m+1}(\lambda)t^{m+1}$$

y φ la aplicación natural. Al ser $k_0 \subset k$ formalmente étale, sabemos que el levantamiento es único y entonces, para todo $\lambda \in k$:

$$\begin{aligned}\varphi(\lambda) &= \overline{\lambda} = \overline{\lambda + 0 \cdot t + \cdots + 0 \cdot t^{m+1}} = E_t(\lambda) = \\ &= \overline{\lambda + D_1(\lambda)t + \cdots + D_{m+1}(\lambda)t^{m+1}}.\end{aligned}$$

Por tanto

$$D_1(\lambda) = \cdots = D_{m+1}(\lambda) = 0.$$

Por último, podemos levantar f sucesivamente a $k \longrightarrow A[[t]]$ y se tiene $D_i(k) = 0$ para todo $i \geq 1$. ■

Veamos a continuación el teorema que generaliza al teorema IV–A.2 al caso de derivaciones de Hasse-Schmidt, cuya demostración sigue el esquema de la prueba dada en [Mat80] (teorema 99), pues la extensión de las derivaciones de Hasse-Schmidt al completado es posible gracias a que son I–continuas (véanse las proposiciones I–D.14 y I–D.15). Sin embargo, mientras que en el citado teorema 99, las derivaciones forman una base, en $HS_{k_0}(R)$ ésto no es en principio posible. No obstante, podemos expresarlas unas en función de otras como se ha visto en el teorema IV–A.6 y por tanto existe la posibilidad de usar este hecho.

Teorema IV–A.10 ■ Sea $(R, \mathfrak{m})$ anillo noetheriano, local, regular, de dimensión n, equicaracterístico de característica $p > 0$. Sean k_0 un cuerpo de casi-coeficientes de R, $\hat{R}$ el completado de R y k el cuerpo de coeficientes de $\hat{R}$ que contiene a k_0. Sea $X_1,\dots,X_n$ un sistema regular de parámetros de R y por tanto, $\hat{R} = k[[X_1,\dots,X_n]]$. Sean $\underline{\Delta}^1,\dots,\underline{\Delta}^n \in HS_k(\hat{R})$ las definidas en la proposición I-D.11. Entonces son equivalentes:

1. $\Delta_i^j(R) \subset R$, para todo $j = 1,\dots,n$, $i \geq 0$.
2. Existen $\underline{D}^1,\dots,\underline{D}^n \in HS_{k_0}(R)$ y $a_1,\dots,a_n \in R$ tales que

$$D_i^j(a_k) = \begin{cases} 0 & i \geq 2,\ \forall j \\ 1 & i = 1,\ k = j \\ 0 & i = 1,\ k \neq j. \end{cases}$$

Demostración.

$1 \Longrightarrow 2$: Trivial tomando $\underline{D}^j = \underline{\Delta}^j$ y $a_k = X_k$ para $k,j = 1,\dots,n$.

$2 \Longrightarrow 1$: Sean $\hat{\underline{D}}^1,\dots,\hat{\underline{D}}^n$ las extensiones de $\underline{D}^1,\dots,\underline{D}^n$ a $\hat{R}$. Dado que existen $a_1,\dots,a_n \in R$ tales que $D_1^j(a_k) = \delta_{jk}$, se tiene que $Der_{k_0}(R)$ es un R-módulo libre de rango n de base $\{D_1^1,\dots,D_1^n\}$ y sus extensiones al completado $\{\hat{D}_1^1,\dots,\hat{D}_1^n\}$, forman una $\hat{R}$-base de $Der_k(\hat{R})$ (veáse la nota IV-A.3). Aplicando el teorema IV-A.6 a $\hat{R}$ y $\hat{\underline{D}}^1,\dots,\hat{\underline{D}}^n \in HS_k(\hat{R})$, sabemos que existen unos únicos $\{C_{ld}^j\}_{l\in\mathbb{N}}$ $(1 \leq j, d \leq n)$ elementos de $\hat{R}$ tales que:

$$\Delta_i^j = \sum_{m=1}^{i} \sum_{\substack{|\lambda|=i,|\mu|=m \\ \lambda_d \geq \mu_d \geq 0}} \left(\prod_{d=1}^{n} \sum_{\substack{l_1^d+\cdots+l_{\mu_d}^d=\lambda_d \\ l_q^d \geq 1}} \prod_{q=1}^{\mu_d} C_{l_q^d d}^j \right) \hat{D}_\mu,$$

donde $D_\mu = D_{\mu_1}^1 \circ \cdots \circ D_{\mu_n}^n$, para todo $\mu \in \mathbb{N}^n$ y

$$\sum_{\substack{l_1^d+\cdots+l_{\mu_d}^d=\lambda_d \\ l_q^d \geq 1}} \prod_{q=1}^{\mu_d} C_{l_q^d d} = \begin{cases} 0 & \text{si } \mu_d = 0 < \lambda_d \\ 1 & \text{si } \mu_d = \lambda_d = 0. \end{cases}$$

Vamos a probar que los $C_{ld}^j \in R$ para todo $l \geq 1$, $d,j = 1,\dots,n$: Para $l = 1$, se tiene que

$$\Delta_1^j(a_k) = \sum_{s=1}^{n} C_{1s}^j \hat{D}_1^p(a_k).$$

Por el teorema IV–A.2, $\Delta_1^j(a_k) \in R$ y como

$$det(D_1^j(a_k)) = det(\delta_{jk}) \notin \mathfrak{m}$$

es una unidad en R, deducimos que los $C_{1d}^j \in R$ para $d, j = 1, \dots, n$.

Supongamos que para todo $l < i$, $C_{l1}^j, \dots, C_{ln}^d \in R$, con $i \geq 2$. Veamos si $C_{i1}^j, \dots, C_{in}^j \in R$: Se tiene que

$$\Delta_i^j(X_j) - \sum_{m=2}^{i} \sum_{\substack{|\lambda|=i, |\mu|=m \\ \lambda_d \geq \mu_d \geq 0}} \left(\prod_{d=1}^{n} \sum_{\substack{l_1^d + \cdots + l_{\mu_d}^d = \lambda_d \\ l_q^d \geq 1}} \prod_{q=1}^{\mu_d} C_{l_q^d d}^j \right) \hat{D}_\mu(X_j) =$$
$$= \sum_{s=1}^{n} C_{is}^j \hat{D}_1^s(X_j).$$

Dado que $\Delta_i^j(X_j) = 0$ y aplicando hipótesis de inducción se tiene que el segundo término pertenece a R. Además, como

$$\hat{D}_1^s = \sum_{r=1}^{n} D_1^s(X_r) \frac{\partial}{\partial X_r}, \qquad s = 1, \dots, n$$

y $\{\hat{D}_1^1, \dots, \hat{D}_1^n\}$ forman una $\hat{R}$–base de $Der_k(\hat{R})$, la matriz $(D_1^s(X_r))$ tiene determinante inversible en $\hat{R}$, y por tanto en R (pues $R \subseteq \hat{R}$ es fielmente plana). Luego los $C_{is}^j \in R$ para todo $i \geq 1$; $s, j = 1, \dots, n$. Entonces se tiene que

$$\Delta_i^j(R) \subseteq R$$

para todo $j = 1, \dots, n$ y todo $i \geq 1$. ∎

En último lugar, damos una generalización del corolario IV–A.5.

Teorema IV–A.11 ■ Sea $(R, \mathfrak{m})$ anillo noetheriano, local, regular, de dimensión n, equicaracterístico de característica $p > 0$. Sea k_0 un cuerpo de casi–coeficientes de R. Sean $\underline{D}^1, \dots, \underline{D}^n \in HS_{k_0}(R)$ tales que existen $a_1, \dots, a_n \in R$ verificando que

$$D_i^j(a_k) = \begin{cases} 0 & i \geq 2, \ \forall j \\ 1 & i = 1, \ k = j \\ 0 & i = 1, \ k \neq j \end{cases}$$

Sean $\underline{\hat{D}}^1, \dots, \underline{\hat{D}}^n$ las extensiones de $\underline{D}^1, \dots, \underline{D}^n$ a $\hat{R}$. Entonces

$$\{a \in \hat{R} \mid \hat{D}_i^j(a) = 0 \quad \forall j = 1, \dots, n, \ i \geq 1\}$$

es un cuerpo de coeficientes de $\hat{R}$ (y es el único que contiene al cuerpo k_0).

Demostración. Sea $\hat{R}$ el completado de R y k el único cuerpo de coeficientes de $\hat{R}$ que contiene a k_0 (ver teorema 91 de [Mat80]). Sea $\{X_1, \dots, X_n\}$ un sistema regular de parámetros de R, entonces $\hat{R} = k[[X_1, \dots, X_n]]$. Consideremos $\underline{\Delta}^1, \dots, \underline{\Delta}^n \in HS_k(\hat{R})$ las definidas en la proposición I–D.11. Entonces

$$k = \{a \in \hat{R} \mid \Delta_i^j(a) = 0 \quad j = 1, \dots, n; \ i \geq 1\}.$$

Queremos probar

$$\{a \in \hat{R} \mid \hat{D}_i^j(a) = 0 \quad \forall j = 1, \dots, n; \ i \geq 1\} = k.$$

Como $D_1^1, \dots, D_1^n \in Der_{k_0}(R)$ y $a_1, \dots, a_n \in R$ tales que $D_1^j(a_k) = \delta_{jk}$, se tiene que $\{\hat{D}_1^1, \dots, \hat{D}_1^n\}$ forman una $\hat{R}$–base de $Der_k(\hat{R})$ (ver nota IV–A.3). Aplicando el teorema IV–A.6 a $\hat{R}$ y $\underline{\hat{D}}^1, \dots, \underline{\hat{D}}^n$, sabemos que los Δ_i^j se pueden poner en función de los $\hat{D}_i^j$. Por tanto, donde se anulan los $\hat{D}_i^j$, se anulan los Δ_i^j, es decir

$$\{a \in \hat{R} \mid \hat{D}_i^j(a) = 0 \quad \forall j = 1, \dots, n, \ i \geq 1\} \subset k.$$

Por otro lado, como k_0 es un cuerpo de casi–coeficientes de R, $k_0 \subset k$ es una extensión formalmente étale. Además, los $\hat{D}_i^j$ $(i \geq 1)$ se anulan en los elementos de k_0, puesto que son las extensiones de D_i^j. Luego aplicando la proposición IV–A.9, se tiene que $\hat{D}_i^j$ se anulan en los elementos de k, y por tanto se verifica la otra inclusión. ∎

Nota IV–A.12 ∎ En la situación del teorema IV–A.10, se tiene claramente que

$$HS(R) \cap HS_k(\hat{R}) \subseteq HS_{k_0}(R),$$

por lo que la conclusión de dicho teorema sigue siendo cierta si en (2) suponemos tan solamente que

$$\underline{D}^j \in HS(R) \cap HS_k(\hat{R}).$$

CAPÍTULO V

Cuerpos de coeficientes y extensión de escalares $k \longrightarrow k(t)_{per}$.

En este capítulo damos una generalización del teorema 2.3 de [Nar91], el teorema V–A.1, para el caso de característica positiva, que ha sido la motivación de la presente memoria.

V–A Cuerpos de coeficientes y extensión de escalares $k \longrightarrow k(t)_{per}$.

A lo largo de esta sección, R será el anillo de series formales en n variables con coeficientes en k, un cuerpo perfecto de característica positiva.

Consideramos la extensión de k, $k_{(\infty)}$, y el anillo $R_{(\infty)}$ definidos en la sección III–A. Bajo estas condiciones, sabemos por el corolario III–C.8, que $R_{(\infty)}$ es noetheriano. Usaremos la siguiente notación: Si $\underline{\mathfrak{D}} \in HS_k(R)$ es una k–derivación de Hasse-Schmidt, notaremos también por $\underline{\mathfrak{D}} \in HS_{k_{(\infty)}}(R_{(\infty)})$ a la derivación de Hasse-Schmidt extendida. Si $\mathfrak{m} \subset R_{(\infty)}$ es un ideal maximal, notaremos por $\underline{\mathfrak{D}}_{\mathfrak{m}}$ y $\hat{\underline{\mathfrak{D}}}_{\mathfrak{m}}$ a las correspondientes derivaciones de Hasse-Schmidt extendidas a $(R_{(\infty)})_{\mathfrak{m}}$ y $\widehat{(R_{(\infty)})_{\mathfrak{m}}}$, respectivamente. Al igual que en la sección III–A, notaremos $t_m = t^{\frac{1}{p^m}}$. Para cualquier $\mathbb{F}_p$–álgebra B, notaremos por $B^{\sharp} = \bigcap_{e \geq 0} B^{p^e}$ (como en la sección III–B).

El teorema que obtenemos para característica positiva es el siguiente (compárese con el teorema 2.3 de [Nar91]).

Teorema V–A.1 ■ Sean k un cuerpo perfecto de característica positiva, $R = k[[X_1, \dots, X_n]]$ y consideremos el anillo $R_{(\infty)}$. Para cada $j = 1, \dots, n$, sean las derivaciones de Hasse-Schmidt $\underline{\Delta}^j = (1_R, \Delta_1^j, \Delta_2^j, \dots) \in HS_k(R)$, definidas en 9 de I–D.11. Si $\mathfrak{m} \subset R_{(\infty)}$ es un ideal maximal, entonces

$$\{a \in \widehat{(R_{(\infty)})_{\mathfrak{m}}} \mid \widehat{(\Delta_i^j)_{\mathfrak{m}}}(a) = 0 \quad \forall j = 1, \dots, n; \ \forall i \geq 1\}$$

es un cuerpo de coeficientes de $\widehat{(R_{(\infty)})_{\mathfrak{m}}}$.

Demostración. La dividiremos en dos partes: reducción al caso $n = 1$ y tratamiento de éste.

Paso 1: la reducción. Sean $\mathfrak{m} \in \Omega(R_{(\infty)})$, $P = \mathfrak{m} \cap R_{[\infty]}$, $\mathfrak{m}_{(m)} = \mathfrak{m} \cap R_{(m)}$, $P_{[m]} = P \cap R_{[m]} = \mathfrak{m}_{(m)} \cap R_{[m]}$. Sabemos que los ideales $\mathfrak{m}_{(m)}$ son maximales y $\mathrm{ht}(\mathfrak{m}_{(m)}) = \mathrm{ht}(\mathfrak{m})$ para todo $m \geq 0$. Sea $\mathfrak{p} = \mathfrak{m} \cap R = P \cap R$ ideal primo de R. Por la nota (1.8) de [Nar91], existen dos posibilidades para la altura de $\mathfrak{p}$:

(i) $\mathrm{ht}(\mathfrak{p}) = n$, es decir, el ideal $\mathfrak{p}$ es maximal, así que $\mathfrak{p} = (X_1, \dots, X_n)$. Entonces $\mathfrak{m} = \mathfrak{p}^e$, y por consiguiente $k_{(\infty)}$ es un cuerpo de coeficientes de $(R_{(\infty)})_{\mathfrak{m}}$ (y por tanto de su completación).

(ii) $\mathrm{ht}(\mathfrak{p}) = n - 1$.

Luego sólo consideraremos el segundo caso. Aplicamos el lema de normalización (II–A.6) a $R = k[[X_1, \ldots, X_n]]$, $\mathfrak{p}$, siendo $dim(R/\mathfrak{p}) = 1$. Entonces existe $X_1 \in R$ (donde por comodidad seguimos llamando igual a la nueva variable) tal que

- $\mathfrak{p} \cap k[[X_1]] = (0)$,
- la extensión $k[[X_1]] \hookrightarrow R/\mathfrak{p}$ es entera, y como $R/\mathfrak{p}$ es finitamente generado sobre $k[[X_1]]$, entonces $R/\mathfrak{p}$ es un $k[[X_1]]$–módulo finito,
- la extensión $k((X_1)) \hookrightarrow Qt(R/\mathfrak{p})$ es finita separable.

Sea $\mathbf{K} = R_{(\infty)}/\mathfrak{m}$. Entonces $\mathbf{K}$ coincide con el cuerpo cociente de $R_{[\infty]}/P$, puesto que $R_{(\infty)}$ es una localización de $R_{[\infty]}$. A partir de ahora, notaremos $A = R/\mathfrak{p}$ y sean $\mathcal{P} = \dfrac{P}{\mathfrak{p}R_{[\infty]}} \in Spec(A_{[\infty]})$ con $\mathrm{ht}(\mathcal{P}) = 1$ y $A_{[\infty]} = \dfrac{R_{[\infty]}}{\mathfrak{p}R_{[\infty]}}$, $A_{[m]} = \dfrac{R_{[m]}}{\mathfrak{p}R_{[m]}}$. Además, para cada $m \geq 0$,

$$
\begin{array}{ccc}
 & A = \dfrac{R}{\mathfrak{p}} & \\
\swarrow & & \searrow \\
\dfrac{R}{\mathfrak{p}}[t_m] & \stackrel{\varphi_m}{\to} & \dfrac{R[t_m]}{P_{[m]}} \\
t_m & \to & \bar{t}_m
\end{array}
$$

las aplicaciones $\varphi_{[m]}$ así definidas son sobreyectivas, y por tanto el límite inductivo de todas ellas, φ,

$$\varphi : A_{[\infty]} \to \frac{R_{[\infty]}}{P}.$$

Sean $R' = k[[X_1]]$, $\mathfrak{m}' = \mathfrak{m} \cap R'_{(\infty)}$, $P' = P \cap R'_{[\infty]} = \mathfrak{m}' \cap R'_{[\infty]}$ siendo $\mathfrak{m}' \cap R' = (0)$ y por tanto $P' \cap R' = (0)$. Veamos que $\mathfrak{m}'$ es maximal y para ello consideremos el siguiente diagrama conmutativo de inclusiones:

$$\begin{array}{ccccc} & & R'[t]/P'_{[0]} & & \\ & \nearrow & & \searrow & \\ R' & & & & R[t]/P_{[0]} \\ & \searrow & & \nearrow & \\ & & A = R/\mathfrak{p} & & \end{array}$$

Las inclusiones inferiores son algebraicas por el lema de normalización y por I–A.1, luego las superiores también. En particular $R'[t]/P'_{[0]}$ es algebraico sobre R', lo que implica que $P'_{[0]} \neq 0$, $\mathfrak{m}'_{(0)} \neq 0$ y entonces $\mathfrak{m}' \neq 0$. Por lo tanto $\mathfrak{m}'$ es maximal, pues $dim(R') = 1$.

Veamos ahora que la inclusión

$$(R'_{(\infty)})_{\mathfrak{m}'} \subset (R_{(\infty)})_{\mathfrak{m}},$$

induce una extensión algebraica separable entre sus cuerpos residuales, pero primero veamos lo que ocurre en los cuerpos intermedios.

Sean $L' = Qt(R') = k((X_1))$ y $L = Qt(R/\mathfrak{p})$, entonces se tiene el siguiente diagrama de extensiones:

$$\begin{array}{ccccc} L' = Qt(R') & \subset & Qt\left(\dfrac{R'_{[0]}}{P'_{[0]}}\right) & = L'[\bar{t}] \\ \cap & & \cap & \\ L = Qt(A) & \subset & Qt\left(\dfrac{R_{[0]}}{P_{[0]}}\right) & = L[\bar{t}] \end{array}$$

De estas extensiones sabemos lo siguiente:

- Por el lema de normalización sabemos que la extensión $L' \subset L$ es finita y separable, luego podemos suponer por el teorema del elemento primitivo que $L = L'(e)$ donde e verifica un cierto $f(X) \in L'[X]$ con $f'(X) \neq 0$;
- sabemos, por I–A.1, que la extensión $A \subset \dfrac{R_{[0]}}{P_{[0]}}$ es algebraica finita generada por $\bar{t}$ (o sea, t mod $P_{[0]}$), luego $L \subset Qt\left(\dfrac{R_{[0]}}{P_{[0]}}\right)$ es

finita y por tanto podemos suponer $Qt\left(\dfrac{R_{[0]}}{P_{[0]}}\right) = L[\bar{t}]$;

- como las extensiones $L' \subset L$ y $L \subset L[\bar{t}]$ son finitas, se tiene que $L' \subset Qt\left(\dfrac{R'_{[0]}}{P'_{[0]}}\right)$ también es finita, luego podemos suponer $Qt\left(\dfrac{R'_{[0]}}{P'_{[0]}}\right) = L'[\bar{t}]$;

así que $L = L'(e)$, donde e verifica un cierto polinomio $f(X) \in L'[X]$ separable; además $L[\bar{t}] = L'(e)[\bar{t}]$ siendo $\bar{t}$ trascendente. Por tanto e verifica también un cierto $g(X) \in L'[\bar{t}][X]$ que será un divisor de $f(X)$ y por tanto también separable. Así que la extensión $L'[\bar{t}] \subset L[\bar{t}] = L'(e)[\bar{t}]$, además de ser finita es separable.

Todo lo anterior también es cierto si se sustituye 0 por m para todo $m \geq 0$, es decir, para todo $m \geq 0$ las extensiones

$$\frac{R'_{(m)}}{\mathfrak{m}'_{(m)}} \subset \frac{R_{(m)}}{\mathfrak{m}_{(m)}}$$

son finitas separables, por tanto la extensión

$$\mathbf{K}' = Qt\left(\frac{R'_{[\infty]}}{P'}\right) = \frac{R'_{(\infty)}}{\mathfrak{m}'} \subset \frac{R_{(\infty)}}{\mathfrak{m}} = Qt\left(\frac{R_{[\infty]}}{P}\right) = \mathbf{K}$$

es algebraica, por ser unión creciente de extensiones finitas. Además, dicha extensión es separable: cualquier $\alpha \in K$ verifica un cierto polinomio mínimo f con coeficientes en K' (por ser algebraica), pero

$$K = \bigcup_{m \geq 0} \frac{R_{(m)}}{\mathfrak{m}_{(m)}},$$

luego existirá un $m \geq 0$ tal que $\alpha \in \dfrac{R_{(m)}}{\mathfrak{m}_{(m)}}$ y por tanto verifica otro polinomio g con coeficientes en $\dfrac{R'_{(m)}}{\mathfrak{m}'_{(m)}}$, que es separable. Luego f será un divisor de g y por tanto separable.

Supongamos el teorema probado para $n = 1$, entonces

$$K'_0 = \{a \in \widehat{(R'_{(\infty)})}_{\mathfrak{m}'} \mid \widehat{(\Delta^1_i)}_{\mathfrak{m}'}(a) = 0 \quad \forall i \geq 1\},$$

es un cuerpo de coeficientes de $\widehat{(R'_{(\infty)})}_{\mathfrak{m}'}$, $(K'_0 \xrightarrow{\sim} K')$. Ahora bien, K'_0 es un subcuerpo de $\widehat{(R_{(\infty)})}_{\mathfrak{m}}$ mediante $\widehat{(R'_{(\infty)})}_{\mathfrak{m}'} \to \widehat{(R_{(\infty)})}_{\mathfrak{m}}$, y evidentemente para todo $a \in K'_0$

$$\widehat{(\Delta^j_i)}_{\mathfrak{m}}(a) = 0 \quad \forall j = 1, \ldots, n; \ \forall i \geq 1.$$

Además, es un cuerpo de casi-coeficientes de $\widehat{(R_{(\infty)})}_{\mathfrak{m}}$, porque K es una extensión algebraica separable de $K' = K'_0$.

Por el teorema IV-A.11 sabemos que

$$\{a \in \widehat{(R_{(\infty)})}_{\mathfrak{m}} \mid \widehat{(\Delta^j_i)}_{\mathfrak{m}}(a) = 0 \quad \forall j = 1, \ldots, n; \ \forall i \geq 1\}$$

es un cuerpo de coeficientes de $\widehat{(R_{(\infty)})}_{\mathfrak{m}}$.

Paso 2: el caso n=1. Sea ahora $R = k[[X]]$ y $\mathfrak{m}$ un ideal maximal de $R_{(\infty)}$. Notemos $P = \mathfrak{m} \cap R_{[\infty]}$, $\mathfrak{m}_{(m)} = \mathfrak{m} \cap R_{(m)}$ y $P_{[m]} = P \cap R_{[m]} = \mathfrak{m} \cap R_{[m]}$. Sabemos que

$$\mathrm{ht}(\mathfrak{m}) = \mathrm{ht}(\mathfrak{m}_{(m)}) = \mathrm{ht}(P_{[m]}) = \mathrm{ht}(P) = 1.$$

Al igual que en el paso 1, nos centraremos en el caso $\mathfrak{m} \cap R = (0)$ (y por tanto $P \cap R = (0)$). Cada $R_{[m]} = R[t_m]$ es un dominio de factorización única y $P_{[m]}$ es un ideal primo de $R_{[m]}$ de altura 1. Por tanto, $P_{[m]}$ está generado por un polinomio irreducible en $k[[X]][t_m]$, $F_m(t_m)$, de grado mayor o igual que 1 (ya que $P \cap R = (0)$). El polinomio $F_m(t_m)$ tiene algún coeficiente no constante porque $P_{[m]} \cap k[t_m] = (0)$ (ya que $R_{(m)} = S_m^{-1} R_{[m]}$ con $S_m = k[t_m]$). Además, al menos uno de sus coeficientes debe ser una unidad debido a la irreducibilidad (pues si no, sacaríamos factor común la X), y podemos suponer que es 1 (dividiendo por la unidad en $k[[X]][t_m]$).

Dado que $R_{(\infty)}$ y cada $R_{(m)}$ son localizaciones de $R_{[\infty]}$ y $R_{[m]}$ respectivamente, se tiene que los cuerpos residuales K (resp. K_m) de $R_{(\infty)}$

(resp. de $R_{(m)}$) sobre $\mathfrak{m}$ (resp. sobre $\mathfrak{m}_{(m)}$), coinciden con los cuerpos residuales de $R_{[\infty]}$ (resp. de $R_{[m]}$) sobre P (resp. sobre $P_{[m]}$):

$$K = \frac{R_{(\infty)}}{\mathfrak{m}} = Qt\left(\frac{R_{[\infty]}}{P}\right) = \frac{Qt(R)_{[\infty]}}{P^e} \quad \text{y} \quad K_m = \frac{R_{(m)}}{\mathfrak{m}_{(m)}} = Qt\left(\frac{R_{[m]}}{P_{[m]}}\right) = \frac{Qt(R)_{[m]}}{P^e_{[m]}}.$$

Si llamamos $L = Qt(R) = k((X))$, se verifica que

$$L^\sharp = (k((X)))^\sharp = k$$

(donde $L^\sharp = \bigcap_{e\geq 0} L^{p^e}$). Luego $L^\sharp$ es algebraico sobre k. Por tanto, aplicando la proposición 3.4 a R, L y P ideal primo de $R_{[\infty]}$ con $P \cap k[t] = (0)$ y $P \cap R = (0)$ (pues $\mathfrak{m} \cap R = (0)$), existe $m_0 \geq 0$ tal que P es el ideal extendido de $P_{[m_0]} = (F_{m_0}(t_{m_0}))$ en $R_{[\infty]}$. Notemos $\mu = F_{m_0}(t_{m_0})$, luego P es el ideal generado por μ en $R_{[\infty]}$ y por tanto $\mathfrak{m}$ es el ideal generado por μ en $R_{(\infty)}$. Además, para todo $j \geq 1$

$$P_{[m_0+j]} = (P_{m_0})^e \quad \text{y} \quad F_{m_0+j}(t_{m_0+j}) = F_{m_0}(t_{m_0}) = F_{m_0}(t^{p^j}_{m_0+j}).$$

Más aún, no todos los coeficientes de

$$\mu = F_{m_0}(t_{m_0}) = a_d t^d_{m_0} + \cdots + a_0$$

pueden ser potencias p–ésimas. En caso contrario, es decir, $a_i = (b_i)^p$, el ideal extendido de $P_{[m_0]}$ en $K[t_{m_0+1}]$ es el generado por el polinomio

$$G = b_d t^d_{m_0+1} + \cdots + b_0.$$

Luego los correspondientes ideales extendidos a $R_{[\infty]}$, $(F_{m_0}) \cdot R_{[\infty]}$ y $(G) \cdot R_{[\infty]}$, son distintos, puesto que el grado en t_{m_0} de F_{m_0} sería d y el de G sería pd lo que se contradice con

$$P = (P_{[m_0]})^e = (P_{[m_0+1]})^e = \cdots.$$

Para cada m tenemos

$$\begin{array}{ccccc}
R & \to & Qt(R)[t_m] & \leftarrow & R_{[m]} \\
\downarrow & & \downarrow \lambda_m & & \downarrow \\
\dfrac{R_{[m]}}{P_{[m]}} & \hookrightarrow & \dfrac{R_{(m)}}{\mathfrak{m}_{(m)}} & \leftarrow & R_{(m)}
\end{array}$$

donde λ_m es sobreyectiva (ya que $\mathfrak{m}_{(m)} \cap R = 0$), y $Ker(\lambda_m) = (F_m(t_m))$ (puesto que $F_m(t_m)$ es irreducible en $R[t_m]$ y por tanto en $Qt(R)[t_m]$, y al ser el núcleo un ideal principal). Tomando límite inductivo de los λ_m, obtenemos un homomorfismo λ_∞, también sobreyectivo,

$$Qt(R)_{[\infty]} \xrightarrow{\lambda_\infty} \frac{R_{(\infty)}}{\mathfrak{m}},$$

que factoriza

$$\begin{array}{ccc} Qt(R)_{[\infty]} & \xrightarrow{\lambda_\infty} & \frac{R_{(\infty)}}{\mathfrak{m}} \\ \uparrow & & \uparrow \\ R_{[\infty]} & \longrightarrow & R_{(\infty)} \end{array}$$

y debido a la estabilidad de los $F_m(t_m)$,

$$Ker(\lambda_\infty) = (F_{m_0}(t_{m_0})) = (\mu).$$

El k–homomorfismo

$$k_{(\infty)} \hookrightarrow K = \bigcup_{m\geq 0} K_m = \bigcup_{m\geq 0} k((X))[\theta_m]$$

envía cada t_m en θ_m, donde $\theta_m \equiv t_m \pmod{P_{[m]}}$ y el polinomio mínimo que verifica θ_m sobre $k((X))$ es $F_m(t_m)$ para todo $m \geq 0$. Además la extensión de cuerpos $k_{(\infty)} \subseteq K$ es separable, puesto que $k_{(\infty)}$ es perfecto (es el cierre perfecto de $k(t)$).

El anillo $\widehat{(R_{(\infty)})_{\mathfrak{m}}}$ es noetheriano, local regular, completo, de dimensión 1. Por el teorema de estructura de Cohen, debe existir un $k_{(\infty)}$–isomorfismo

$$\varphi : \widehat{(R_{(\infty)})_{\mathfrak{m}}} \xrightarrow{\sim} K[[s]]$$

que envía el parámetro regular μ en s, y que induce un isomorfismo entre los cuerpos residuales:

$$\begin{aligned} \varphi(\mu) = \varphi(a_d(X)t_{m_0}^d + \cdots + a_0(X)) &= s \\ \varphi(t_m) &= \theta_m \\ \varphi(X) &= X + \xi \quad \text{con} \quad \xi \in (s). \end{aligned}$$

A partir de ahora, notaremos por

$$\underline{\Delta}^X = (\Delta_1^X, \Delta_2^X, \dots) \in HS_K(K[[X]])$$

la derivación de Hasse-Schmidt definida en I–D.11. Supongamos que el homorfismo φ verifica:

$$\varphi(b(X)) = b(X+\xi) \subseteq k[[X,\xi]] \subseteq K[[\xi]], \qquad ((\text{V–A.1}))$$

para todo $b \in R = k[[X]]$. Entonces

$$s = \varphi(\mu) = \varphi(\sum_{k=0}^{d} a_k(X) t_{m_0}^k) = \sum_{k=0}^{d} \varphi(a_k(X))\theta_{m_0}^k = \sum_{k=0}^{d} a_k(X+\xi)\theta_{m_0}^k \overset{(I\text{—}\underline{D}.11)}{=}$$
$$= \sum_{k=0}^{d}(\sum_{i=0}^{\infty} \Delta_i^X(a_k(X))\xi^i)\theta_{m_0}^k = \sum_{i\geq 1}^{\infty}(\sum_{k=0}^{d} \Delta_i^X(a_k(X))\theta_{m_0}^k)\xi^i \in K[[\xi]].$$

Por tanto ξ debe ser de orden 1 en s, luego $K[[\xi]] = K[[s]]$ y ξ se puede considerar una variable. Notemos

$$\underline{\Delta}^\xi = (\Delta_1^\xi, \Delta_2^\xi, \dots) \in HS_K(K[[\xi]]) = HS_K(K[[s]]).$$

Veamos que Δ_i^ξ resultan ser las extensiones de Δ_i^X, mediante φ, a $K[[s]]$ y por tanto

$$\varphi^{-1}(K) = \{a \in \widehat{(R_{(\infty)})}_m \mid \Delta_i^X(a) = 0, \quad \forall i\}$$

es un cuerpo de coeficientes de $\widehat{(R_{(\infty)})}_m$: dada $a(X) \in k[[X]]$, (recuérdese cómo se habían definido los Δ_n^X en I–D.11),

$$a(X+Y) = \sum_{k=0}^{\infty} \Delta_k^X(a(X))Y^k$$

siendo Y otra indeterminada). Consideremos el siguiente diagrama

$$\begin{array}{ccccccc}
k[[X]] & \xrightarrow{\varphi} & k[[X,\xi]] & \subseteq & K[[\xi]] & = K[[s]] \\
X & \to & X+\xi & & & \\
i' \downarrow & & i\downarrow & & \cap & \\
k[[X,Y]] & \xrightarrow{\varphi} & k[[X,\xi,Y]] & \subset & K[[\xi,Y]] & \\
X & \to & X+\xi & & & \\
Y & \to & Y & & &
\end{array}$$

que verifica

$$i \circ \varphi(X) = i(X + \xi) = X + \xi + Y,$$

y por otro lado

$$\varphi \circ i'(X) = \varphi(X + Y) = \varphi(X) + \varphi(Y) = X + \xi + Y;$$

así que

$$i \circ \varphi = \varphi \circ i'.$$

Luego

$$a(X + Y) = \sum_{k=0}^{\infty} \Delta_k^X(a(X))Y^k \xrightarrow{\varphi} a(X + \xi + Y) = \sum_{k=0}^{\infty}(\Delta_k^{\xi}(a(X + \xi))Y^k.$$

Por tanto

$$\varphi(\Delta_n^X(a(X))) = \Delta_n^{\xi}(a(X + \xi)),$$

y por otro lado

$$\Delta_n^{\xi}(\varphi(a(X))) = \Delta_n^{\xi}(a(X + \xi)) = \Delta_n^{\xi}(b(\xi)),$$

siendo $b(\xi) = a(X + \xi) = \varphi(a(X))$, y

$$b(\xi + Y) = a(X + \xi + Y) = \sum_{k=0}^{\infty}(\Delta_k^{\xi}(a(X + \xi)))Y^k.$$

Luego

$$\Delta_i^{\xi}(b(\xi)) = \Delta_i^{\xi}(a(X + \xi)).$$

De donde se concluye

$$\varphi(\Delta_n^X(a(X))) = \Delta_n^{\xi}(a(X + \xi)) = \Delta_n^{\xi}(b(\xi)) = \Delta_n^{\xi}(\varphi(a(X)))$$

para toda $a(X) \in k[[X]]$. Además Δ_n^X se extienden de manera única a $R_{[\infty]}$, pues $\Delta_n^X(t_m) = 0$ y $\Delta_n^{\xi}(\theta_m) = 0$. También se extienden a $R_{(\infty)}$ porque es una localización de $R_{[\infty]}$ y a $(R_{(\infty)})_{\mathrm{m}}$, puesto que $\varphi^{-1}((s)) = (F_{m_0}(t_{m_0}))$. Por último, también se extienden al completado, al ser las aplicaciones Δ_n^X I–continuas para la topología I–ádica.

Construyamos ahora un homomorfismo φ que cumpla (V-A.1) encontrando primero $\varphi(X)$, para lo que necesitamos el siguiente lema, que es una generalización del lema (2.3.3) de [Nar91].

Lema V-A.2 ■ Existe un único $\xi \in K[[s]]$ tal que $\xi(0) = 0$, de orden 1 tal que

$$a_d(X+\xi)\theta_{m_0}^d + \cdots + a_0(X+\xi) = s.$$ [1]

Demostración. El lema es una consecuencia del teorema de la función implícita. Sea $G(s,\sigma) = a_d(X+\sigma)\theta_{m_0}^d + \cdots + a_0(X+\sigma) - s \in K[[s,\sigma]]$. Dado que

$$G(0,0) = a_d(X)\theta_{m_0}^d + \cdots + a_0(X) = F_{m_0}(\theta_{m_0}) = 0,$$

si probamos que

$$\left(\frac{\partial G}{\partial \sigma}\right)|_{s=\sigma=0} = a_d'(X)\theta_{m_0}^d + \cdots + a_0'(X) \neq 0 \quad \text{en} \quad K,$$

aplicando el teorema de la función implícita, se tiene el resultado. Supongamos lo contrario, entonces

$$a_d'(X)t_{m_0}^d + \cdots + a_0'(X)$$

debe ser un múltiplo de $F_{m_0}(t_{m_0})$ en $k((X))[t_{m_0}]$. Luego para todo $k = 0, 1, \ldots, d$

$$a_k'(X) = \alpha(X)a_k(X) \quad \text{con} \quad \alpha(X) \in k((X)),$$

como sabemos que algún a_k es 1, para ese k se tiene que $0 = \alpha(X)\cdot 1$, y entonces $\alpha(X) = 0$. Por tanto, para todo $k = 0, 1, \ldots, d$, $a_k'(X) = 0$ y como estamos en característica $p > 0$,

$$a_k(X) = b_k(X^p) = (\text{como } k \text{ es perfecto}) = (b_k(X))^p \quad \text{con} \quad b_k(X) \in k[[X]].$$

---

[1] Nótese que $K = \dfrac{k((X))_{[\infty]}}{(F_{m_0}(t_{m_0}))} = \bigcup_{m\geq 0} K_m = \bigcup_{m\geq 0}(k((X))[\theta_m])$ y $a_k(X+\xi) \in k[[X,\xi]] \subseteq K[[\xi]] = K[[s]]$ para $k = 0, 1, \ldots, d$.

Así que

$$F_{m_0}(t_{m_0}) = (b_d(X))^p t_{m_0}^d + \cdot \cdot \cdot + (b_0(X))^p,$$

lo que es una contradicción, puesto que sabemos que no todos sus coeficientes pueden ser potencias p–ésimas. ∎

Continuemos con la prueba del teorema V–A.1. Sea $\xi \in K[[s]]$ como en el lema V–A.2; entonces ξ tiene orden 1 en s porque

$$\left(\frac{\partial \xi}{\partial s}\right)(0) = \left[\left(\frac{\partial G}{\partial \sigma}\right)(0,0)\right]^{-1} \neq 0.$$

Consideremos el k–homomorfismo

$$\varphi : \ R = k[[X]] \to k[[X, \xi]] \subseteq K[[\xi]] = K[[s]]$$

tal que $\varphi(X) = X + \xi$; podemos extender φ a $R_{(\infty)}$ haciendo $\varphi(t_m) = \theta_m \in K_m \subseteq K$. Así tenemos un $k_{(\infty)}$–homomorfismo $\varphi : R_{(\infty)} \to K[[s]]$ que satisface la ecuación (V–A.1) (por construcción), y que envía

$$\mu = F_{m_0}(t_{m_0}) = a_d(X)t_{m_0}^d + \cdot \cdot \cdot + a_0(X)$$

en el elemento

$$a_d(X + \xi)\theta_{m_0}^d + \cdot \cdot \cdot + a_0(X + \xi) = s.$$

Por lo tanto, la contracción del ideal maximal (s) mediante φ es $\mathfrak{m} = (\mu)$, lo que nos permite extender φ a un $k_{(\infty)}$–homomorfismo local que también denotamos por $\varphi : \widehat{(R_{(\infty)})_{\mathfrak{m}}} \to K[[s]]$. Tal φ induce un isomorfismo entre los cuerpos residuales, que envía el parámetro regular $F_{m_0}(t_{m_0})$ sobre s. Por regularidad $\mathrm{gr}(\varphi)$ es un isomorfismo, y dado que ambos anillos son completos, tenemos que $\varphi : \widehat{R_{(\infty)\mathfrak{m}}} \to K[[s]]$ es un $k_{(\infty)}$–isomorfismo que verifica la ecuación (V–A.1). ∎

Con ésto se concluye la demostración del teorema V–A.1.

BIBLIOGRAFÍA

[Abh64] S. S. Abhyankar. *Local Analytic Geometry.* Academic Press, 1964.

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to Commutative Algebra.* Addison-Wesley Publishing Company, 1969.

[Ber58] I. Beršteĭn. On the dimension of modules and algebras IX, direct limits. *Nagoya Math. Journal*, 13:83–84, 1958.

[Ber72] J. Bernstein. The analytic continuation of generalized functions with respect to a parameter. *Funz. Anal. Appl.*, 6:26–40, 1972.

[Che79] A. Chenciner. *Courbes Algebriques Planes*, volume VII. Publications Mathématiques de L'Université Paris, 1979.

[Gab81] O. Gabber. The integrability of the characteristic variety. *Amer. J. Math.*, 103:445–468, 1981.

[Gar86] D. J. H. Garling. *A course in Galois theory*, volume III. Cambridge University Press, 1986.

[GD64] A. Grothendieck and J. Dieudonné. *Eléments de géométrie algébrique IV: Étude locale des schémas et de morphismes de schémas (I Partie)*, volume 20 of *Institut Hautes Études Scientifiques.* Publications Mathématiques, 1964.

[GD65] A. Grothendieck and J. Dieudonné. *Eléments de géométrie algébrique IV: Étude locale des schémas et de morphismes de schémas (II Partie)*, volume 24 of *Institut Hautes Études Scientifiques.* Publications Mathématiques, 1965.

[GD67] A. Grothendieck and J. Dieudonné. *Eléments de géométrie algébrique IV: Etude locale des schémas et de morphismes de schémas (IV partie)*, volume 32 of *Institut des Hautes Études Scientifiques*. Publications Mathématiques, 1967.

[HS37] H. Hasse and F. K. Schmidt. Noch eine begründung der theorie der höheren differrentialquotienten in einem algebraischen funktionenkorper einer unbestimmten. *J. reine u. angew. Math.*, 177:223–239, 1937.

[Ish77] Y. Ishibashi. A note on a lemma of zariski. *Bull. Funoka University Ed. III*, 27:1–3, 1977.

[Jou83] J. P. Jouanolou. *Théorèmes de Bertini et Applications.* Birkhäuser, 1983.

[Mat80] H. Matsumura. *Commutative Algebra, 2nd edition.* Benjamin & Cummings, 1980.

[Mat82] H. Matsumura. Integrable derivations. *Nagoya Math. Journal*, 87:227–245, 1982.

[Mat86] H. Matsumura. *Commutative Ring Theory.* Studies in Advanced Mathematics. Cambridge University Press, 1986.

[MNM91] Z. Mebkhout and L. Narváez-Macarro. La théorie du polynôme de Bernstein-Sato pour les algèbres de Tate et de Dwork-Monsky-Washnitzer. *Ann. Sci. E.N.S.*, 24:227–256, 1991.

[Mol79] S. Molinelli. Sul modulo delle derivazioni integrabili in caractteristica positiva. *Ann. Mat. Pura Appl.*, 121:25–38, 1979.

[MV69] K. Mount and O. E. Villamayor. Taylor series and higher derivations. *Universidad de Buenos Aires*, 18, 1969.

[Nag75] M. Nagata. *Local Rings.* Robert E. Krieger Publishing Co, 1975.

[NaK70] Y. NaKai. High order derivations I. *Osaka J. Math.*, 7:1–27, 1970.

[Nar91] L. Narváez. A note on the behaviour under a ground field extension of quasicoefficient fields. *J. London Math. Soc. (2)*, 43:12–22, 1991.

[Tra00] W. N. Traves. Tight closure and differential simplicity. *Journal of Algebra*, 228:457–476, 2000.

[ZS79] O. Zariski and P. Samuel. *Commutative Algebra*, volume I and II. Springer-Verlag, 1979.

UNIVERSIDAD DE SEVILLA

Reunido el Tribunal integrado por los abajo firmantes en el día de la fecha, para juzgar la Tesis Doctoral de

D.ª Magdalena Fernández Lebrón

titulada Derivaciones de Hasse-Schmidt, cuerpos de coeficientes y extensión de escalares en característica positiva

acordó otorgarle la calificación de Sobresaliente Cum Laude (por unanimidad)

Sevilla, 8 de marzo 2002

El Vocal, El Vocal, El Vocal,

Mark Spivakovsky

El Presidente, El Secretario, El Doctorado,

José M.ª Giral

Magdalena Fernández