FACULTAD DE MATEMÁTICAS

DEPARTAMENTO DE ÁLGEBRA

TÍTULO

El problema de la Cancelación

María de la Paz Tirado Hernández

Tutor:
Luis Narváez Macarro

Índice general

Introducción

El *problema de la cancelación* puede enunciarse de manera muy general y tiene sentido en muy diversos contextos: dada una estructura matemática, o más precisamente una categoría, y dados objetos X, Y, Z con dicha estructura, ¿podemos deducir que si $X \bigodot Z \simeq Y \bigodot Z$ entonces $X \simeq Y$? donde $\bigodot$ representa la operación de "producto" o de "coproducto" en la categoría en cuestión. El problema de la cancelación puede plantearse fijando el objeto Z, en cuyo caso si el problema de la cancelación tiene respuesta positiva, decimos que "Z es cancelable". Este problema guarda similitud con el problema puramente algebraico de saber si un elemento de cualquier estructura algebraica (anillo, semigrupo, etc.) es cancelable en el sentido usual.

Como ejemplo básico de este problema, consideremos la categoría de los espacios vectoriales de dimensión finita sobre un cuerpo k con el producto cartesiano y sean $X = k^{n_1}$, $Y = k^{n_2}$ y $Z = k^m$ tres elementos de esta categoría. Supongamos que $X \times Z \simeq Y \times Z$, entonces estos dos espacios deben tener la misma dimensión, es decir, $n_1 + m = n_2 + m$, y en consecuencia $X \simeq Y$, luego Z es un elemento cancelable.

Hay un caso particular del problema de la cancelación que se conoce como *problema de Zariski* y que concierne el caso de la categoría de variedades afines sobre un cuerpo algebraicamente cerrado. Este es el enunciado preciso: sea k un cuerpo de característica 0 y denotemos por $\mathbb{A}_k^n$ el espacio afín n-dimensional sobre k. Dada una variedad afín X sobre k, ¿podemos deducir que si $X \times \mathbb{A}_k^1 \simeq \mathbb{A}_k^{n+1}$ entonces $X \simeq \mathbb{A}_k^n$? Este problema admite la traducción algebraica siguiente: Si A es una k-álgebra afín. i.e. una k-álgebra finitamente generada y reducida, ¿podemos deducir que si $A[X] = A \otimes_k k[X] \simeq k[X_1, \ldots, X_{n+1}] = k[X_1, \ldots, X_n] \otimes_k k[X]$, entonces $A \simeq k[X_1, \ldots, X_n]$?

Durante las últimas décadas hasta 2013 se ha dado respuesta a este problema para los casos $n = 1$ y $n = 2$. La respuesta afirmativa a esta pregunta para $n = 1$ fue dada por Shreeram S. Abhyankar, Paul Eakin y William J. Heinzer en 1972 [AEH]. Para el caso $n = 2$, debemos esperar hasta los años 1979-1980, cuando Takao Fujita, Masayoshi Miyanishi y Tohru Surgie demostraron que el problema también es cierto cuando el cuerpo es de característica cero [Fuj, MS] y fue un año después cuando Peter Russell lo probó para un cuerpo perfecto de característica positiva [Ru]. En 2004, Anthony J. Crachiola y Leonid G. Makar-Limanov en [CM] presentaron una nueva técnica para el estudio de este problema, dando a conocer a las aplicaciones exponenciales y usando el invariante AK (también conocido como el invariante de Makar-Limanov). En dicho artículo, probraron la conjetura para $n = 1$ en cuerpos algebraicamente cerrados. Más tarde, en el 2007, presentaron una prueba usando esta misma técnica para el caso $n = 2$ y en cuerpos algebraicamente cerrados en [CML].

El objeto de este trabajo fin de máster es estudiar la reciente solución negativa al problema de Zariski en el caso $n = 3$ y un cuerpo arbitrario de característica $p > 0$ dada en el artículo de Neena Gupta [Gu] titulado *On the cancellation problem for the affine space* $\mathbb{A}^3$ *in characteristic* p.

En dicho artículo se prueba la existencia de un dominio afín, el cual fue estudiado por Teruo Asanuma en [As] y en [Asa], que es un contraejemplo para el problema de Zariski en el caso anteriormente menciado. Para desarrollar este contraejemplo, el autor usa las mismas técnicas que Crachiola y Makar-Limanov en [CM] y en [CML] es decir, las aplicaciones exponenciales, ayudandose en este caso del invariente Derksen.

Debemos mencionar un nuevo preprint realizado por N. Gupta y titulado *On Zariski's Cancellation Problem in positive characteristic* [Gup], en el que demuestra la solución negativa del problema de Zariski en el caso de un cuerpo de característica positiva para $n \geq 3$ de nuevo mediante el uso de las aplicaciones exponenciales.

Este trabajo está organizado de la siguiente forma. En el primer capítulo desarrollaremos conceptos necesarios para llevar a cabo la demostración del contraejemplo del problema de la cancelación. En la primera sección, estudiaremos un resultado que nos permitirá concluir la existencia de un dominio afín, A, sobre un cuerpo de característica positiva k tal que $A[X] \cong k[X, Y, Z, T]$. En la segunda sección, daremos el concepto de aplicación exponencial y probaremos algunas de sus propiedades básicas. Continuaremos estableciendo la relación existente entre las acciones del grupo algebraico $\mathbb{G}_a := (k, +)$ sobre una variedad afín y las aplicaciones exponenciales definidas en sus anillos de coordenadas. Por último, definiremos lo que se entiende por una $\mathbb{Z}$-filtación propia admisible y expondremos un teorema con el que podremos extender una aplicación de un dominio afín con una $\mathbb{Z}$-filtración propia admisible a su anillo graduado.

En el siguiente capítulo, abordaremos el problema de la cancelación mediante la realización de algunos lemas previos, con los cuales podremos concluir la existencia o no de aplicaciones exponenciales cumpliendo ciertas condiciones para los dominios afines. Gracias a estos lemas, demostraremos que el dominio afín A presentado en la sección uno del capítulo anterior cumple que $A \ncong k[Y, Z, T]$, donde k será un cuerpo infinito de característica positiva y terminaremos concluyendo la respuesta negativa a la conjetura.

Capítulo 1

Conceptos previos

Antes de estudiar el contraejemplo al problema de la cancelación, daremos algunos conceptos necesarios para la realización de este trabajo. A lo largo de éste, denotaremos por $R^{[n]}$ al anillo de polinomios en n variables sobre el anillo R.

1.1. Primer paso para el contraejemplo

En esta sección expondremos un resultado probado en [As] que nos ayudará a obtener un colorario fundamental para el objetivo de este trabajo. Antes, definiremos los anillos de valoración discreta y daremos un ejemplo que utilizaremos para probar el corolario anteriormente citado.

Definición 1.1.1 *Sea K un cuerpo. Una* **valoración discreta** *en K es una aplicación ν de K^* sobre $\mathbb{Z}$ (donde $K^* = K \setminus \{0\}$ es el grupo multiplicativo de K) tal que*

1. *$\nu(xy) = \nu(x) + \nu(y)$, es decir ν es un homomorfismo;*
2. *$\nu(x + y) \geq \text{mín}\{\nu(x), \nu(y)\}$*

El conjunto formado de 0 y todas las $x \in K^*$ tales que $\nu(x) \geq 0$ es un anillo, llamado el **anillo de valoración** *de ν. Es algunas veces conveniente extender ν a todo K poniendo $\nu(0) = +\infty$.*

Definición 1.1.2 *Un dominio de integridad A es un* **anillo de valoración discreta** *si existe una valoración discreta en su cuerpo de fracciones K tal que A es el anillo de valoración de ν.*

Proposición 1.1.3 *Sea A un anillo de valoración discreta. Entonces A es un anillo local cuyo ideal maximal es principal. Además, todos los ideales son potencias del ideal maximal.*

Demostración.

Sean K el cuerpo de fracciones de A y $\nu : K^* \to \mathbb{Z}$ la valoración discreta en K que hace a A un anillo de valoración discreta. Consideremos el conjunto $\mathfrak{m} = \{x \in A : \nu(x) > 0\}$. Observar que este conjunto es un ideal, de hecho, será el ideal maximal de A.

Sabemos que si A es un anillo y $\mathfrak{m}$ es un ideal de A tal que cada $x \in A \setminus \mathfrak{m}$ es una unidad en A, entonces A es local y $\mathfrak{m}$ es su ideal maximal. Consideremos entonces $x \in A \setminus \mathfrak{m}$.

Para probar que x es una unidad en A, debemos ver que $x^{-1} \in K$ pertenece a A, es decir que $\mu\left(x^{-1}\right) \geq 0$ (en realidad debe darse la igualdad, ya que en caso contrario $x^{-1} \in \mathfrak{m}$ y entonces $A = \mathfrak{m}$). Como $x \notin \mathfrak{m}$, tenemos que $\nu(x) = 0$, y se tienen las siguientes igualdades

$$0 = \nu(1) = \nu\left(xx^{-1}\right) = \nu(x) + \nu\left(x^{-1}\right) = \nu\left(x^{-1}\right)$$

Por tanto $x^{-1} \in A$ y podemos concluir que x es una unidad en A. Esto prueba que A es un anillo local con ideal maximal $\mathfrak{m}$.

Para probar que el ideal maximal de este anillo local es principal vamos a realizar varias observaciones. Consideremos $x, y \in A$ tal que $\nu(x) = k_x$ y $\nu(y) = k_y$. Si $k_x = k_y$, entonces

$$\nu\left(xy^{-1}\right) = \nu(x) - \nu\left(y\right) = 0$$

y por tanto $xy^{-1} \notin \mathfrak{m}$, es decir, xy^{-1} es una unidad en A. Luego $\langle x\rangle = \langle y\rangle$.

Si $k_y > k_x$ (análogamente si $k_x > k_y$), entonces

$$\nu\left(yx^{-1}\right) = \nu(y) - \nu(x) > 0$$

es decir, $yx^{-1} \in A$, y por tanto

$$\left(yx^{-1}\right)x = y \in \langle x\rangle$$

Teniendo en cuenta estas dos observaciones, dado un ideal $\mathfrak{a}$ de A tal que $x \in \mathfrak{a}$ con $\nu(x) = k_x$, se tiene que para todo $y \in A$ tal que $\nu(y) \geq k_x$, $y \in \mathfrak{a}$. Luego, todos los ideales de A son de la forma $\mathfrak{m}_k = \{y \in A : \nu(y) \geq k\}$.

Puesto que $\nu : K^* \to \mathbb{Z}$ es una aplicación sobreyectiva, existe $x \in K^*$ tal que $\nu(x) = 1$ (por tanto $x \in A$) y se tiene que

$$\langle x\rangle = \{y \in A : \nu(y) \geq 1\} = \mathfrak{m}$$

De lo cual podemos deducir que $\mathfrak{m}$ es un ideal principal. Además, $\nu\left(x^k\right) = k$ y por tanto

$$\left\langle x^k\right\rangle = \{y \in A : \nu(y) \geq k\} = \mathfrak{m}_k$$

es decir, todos los ideales de A son potencias del ideal maximal.

□

Ejemplo 1.1.4 *Consideramos $k(X)$ el cuerpo de fracciones de $k[X]$ donde k es un cuerpo y X una indeterminada sobre k. Tomemos f un polinomio irreducible en $k[X]$. Entonces el localizado de $k[X]$ sobre el ideal $\langle f\rangle$ es un anillo de valoración discreta.*

Todo elemento $G \in k(X)$ se puede escribir de forma única como $f^\alpha g(X)$, donde $\alpha \in \mathbb{Z}$ y el numerador y el denominador de $g(X)$ ambos son primos con f. Definimos la aplicación

$$\begin{array}{rccc} \nu_f : & k(X) & \longrightarrow & \mathbb{Z} \\ & G & \longmapsto & \alpha \end{array}$$

Vamos a probar que esta aplicación es una valoración discreta. De manera obvia es sobreyectiva. Consideremos $G(X) = f^\alpha g$ y $H(X) = f^\beta h$ dos elementos de $k(X)$, donde $g, h \in k(X)$ cumplen que sus numeradores y denominadores son primos con f.

Para la primera propiedad basta observar que $G(X)H(X) = f^{\alpha+\beta}gh$, donde tanto el numerador como el denominador de gh son coprimos con f gracias a que f es irreducible, y por tanto $\nu_f(GH) = \nu_f(G)+\nu_f(H)$.

Para la segunda, sea $\delta = \text{mín}\{\alpha, \beta\}$, entonces $G(X) + H(X) = f^\delta(f^{\alpha-\delta}g + f^{\beta-\delta}h)$. Observar que o bien $\alpha - \delta = 0$ ó $\beta - \delta = 0$. Luego, si $f^{\alpha-\delta}g + f^{\beta-\delta}h \neq 0$, entonces $\nu_f(G + H) = \text{mín}\{\nu_f(G), \nu_f(H)\}$. En caso contrario, $\nu_f(G + H) = +\infty$ y por tanto podemos concluir que $\nu_f(G + H) \geq \text{mín}\{\nu_f(G), \nu_f(H)\}$.

Observar que el anillo de valoración de ν_f está formado por aquellos elementos $g \in k(X)$ para los que $\alpha \geq 0$, lo que equivale a que g no tenga factores de f en su denominador, es decir, que g pertenezca al localizado de $k[X]$ en $\langle f\rangle$, concluyendo así que el anillo de valoración de ν_f es este localizado.

El siguiente teorema que presentaremos sin demostración se encuentra en el artículo [As] (Teorema 5.1) junto con un corolario (Corolario 5.3), el cual será adaptado para un anillo en particular.

Teorema 1.1.5 *Sean R un anillo de valoración discreta con ideal maximal πR, $K = R[\pi^{-1}]$ un cuerpo de fracciones y $k = R/\pi R$ el cuerpo residual. Supongamos que $\operatorname{char} k = p > 0$. Sean e y s enteros positivos tales que $p^e \nmid sp$ y $sp \nmid p^e$. Dado un m entero positivo, sea*

$$A = R[X,Y,Z] \Big/ \Big\langle -X^{p^e} + Y + a_1^{p^e} Y^p + \ldots + a_s^{p^e} Y^{sp} + \pi^m Z \Big\rangle$$

donde $R[X,Y,Z] \cong R^{[3]}$, $a_i \in R$ para $i = 1, \ldots, s-1$ y $a_s \in R \setminus \pi R$. Entonces A satisface las siguientes condiciones:

i. $A \otimes K \cong_R K^{[2]}$.

ii. $A \otimes k \cong_R k^{[2]}$.

iii. $A^{[1]} \cong_R R^{[3]}$.

iv. $A \ncong_R R^{[2]}$.

Corolario 1.1.6 *Sean k un cuerpo de característica $p > 0$ y $R = k[X]$ el anillo de polinomios sobre k en la variable X. Sea*

$$A = R[Y,Z,T] \Big/ \Big\langle -Z^{p^e} + T + T^{sp} + X^m Y \Big\rangle$$

donde e y s son enteros positivos tales que $p^e \nmid sp$ y $sp \nmid p^e$. Entonces la R-álgebra A satisface las siguientes condiciones:

a. $A \otimes k(\mathfrak{p}) \cong_R k(\mathfrak{p})^{[2]}$ *para cada ideal primo $\mathfrak{p}$ de R.*

b. $A^{[1]} \cong_R R^{[3]} \cong_k k^{[4]}$.

c. $A \ncong_R R^{[2]}$.

Nota: $k(\mathfrak{p})$ *denota al cociente $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$, donde $\mathfrak{p}$ es un ideal primo de R.*

Demostración.

R es un D.I.P., y por tanto un D.F.U., luego dado $f \in R$, $\langle f \rangle$ es primo si y sólo si f es irreducible en R. Gracias a esto, podemos deducir que todos los ideales primos de R son generados por un elemento irreducible. Consideremos $R_{\langle f \rangle}$ con f irreducible el localizado de R en el ideal fR. Recordemos que el ideal maximal de este anillo es $fR_{\langle f \rangle}$. Además, por el ejemplo 1.1.4 $R_{\langle f \rangle}$ es un anillo de valoración discreta.

Observar que el cuerpo residual $k(\langle f \rangle) := R_{\langle f \rangle} \big/ fR_{\langle f \rangle}$ es de característica $p > 0$ (pues $k \subseteq k(\langle f \rangle)$). Consideremos el R-módulo,

$$B := A \otimes_R R_{\langle f \rangle} \cong R_{\langle f \rangle}[Y,Z,T] \Big/ \Big\langle -Z^{p^e} + T + T^{sp} + X^m Y \Big\rangle$$

Ahora, podemos aplicar el teorema 1.1.5 a $R_{\langle f \rangle}$ y a B pues cumplen todas las hipótesis. Establecemos entonces las siguientes propiedades:

i. $B \otimes_{R_{\langle f \rangle}} R_{\langle f \rangle}[f^{-1}] \cong R_{\langle f \rangle}[f^{-1}]^{[2]}$.

ii. $B \otimes_{R_{\langle f \rangle}} k(\langle f \rangle) \cong k(\langle f \rangle)^{[2]}$.

iii. $B^{[1]} \cong R_{\langle f \rangle}^{[3]}$.

iv. $B \ncong R_{\langle f \rangle}^{[2]}$.

El apartado a. de este corolario resulta de forma inmediata a partir de ii., ya que

$$k(\langle f \rangle)^{[2]} \cong B \otimes_{R_{\langle f \rangle}} k(\langle f \rangle) := A \otimes_R R_{\langle f \rangle} \otimes_{R_{\langle f \rangle}} k(\langle f \rangle) \cong A \otimes_R k(\langle f \rangle)$$

y como f es un polinomio irreducible genérico, tenemos que $A \otimes_R k(\mathfrak{p}) \cong_{R_{\langle f \rangle}} k(\mathfrak{p})^{[2]}$ donde $\mathfrak{p}$ es cualquier ideal primo de R. Debido a que $R \subseteq R_{\langle f \rangle}$, conseguimos que $A \otimes_R k(\mathfrak{p}) \cong_R k(\mathfrak{p})^{[2]}$.

Para el apartado b. vamos a considerar iii. Sabemos que $B^{[1]} \cong R^{[3]}_{\langle f \rangle}$ y sustituyendo B, obtenemos que $\left(A \otimes_R R_{\langle f \rangle}\right)^{[1]} \cong R^{[3]}_{\langle f \rangle}$, luego $A^{[1]} \otimes_R R_{\langle f \rangle} \cong R^{[3]}_{\langle f \rangle}$ para todo ideal primo de R, es decir, $A^{[1]}$ es una R-álgebra localmente polinomial. Gracias a [Ba], podemos establecer un isomorfimo entre $A^{[1]}$ y el álgebra simétrica de un módulo proyectivo M de rango 3, denotado por $S_R(M)$. Además, R es un dominio de ideales principales y por tanto M es un R-módulo libre. De esto se deduce que

$$A^{[1]} \cong S_R\left(R^3\right) \cong R^{[3]}$$

Por último, consideremos la conclusión iv. del teorema 1.1.5 escritas anteriormente. Ésta se traduce en la siguiente

$$A \otimes_R R_{\langle f \rangle} \ncong R^{[2]}_{\langle f \rangle} \cong R^{[2]} \otimes_R R_{\langle f \rangle}$$

Supongamos que $A \cong R^{[2]}$ entonces tenemos la siguiente sucesión exacta corta:

$$0 \to 0 \hookrightarrow A \twoheadrightarrow R^{[2]} \to 0$$

Tensorizando por $- \otimes_R R_{\langle f \rangle}$, obtenemos una sucesión exacta:

$$0 \to A \otimes_R R_{\langle f \rangle} \twoheadrightarrow R^{[2]} \otimes_R R_{\langle f \rangle} \to 0$$

lo que nos da un isomorfimo entre $A \otimes_R R_{\langle f \rangle}$ y $R^{[2]} \otimes_R R_{\langle f \rangle}$ llegando así a una contradicción. Concluimos por tanto que $A \ncong R^{[2]}$.

$\square$

Nota 1.1.7 *Realizando el cambio de variable $Z := -Z$, obtenemos que el corolario se puede aplicar a*

$$A = R[Y, Z, T] \Big/ \left\langle Z^{p^e} + T + T^{sp} + X^m Y \right\rangle$$

1.2. Aplicación exponencial y propiedades

En esta sección daremos a conocer a las aplicaciones exponenciales y a algunas de sus propiedades básicas. Además, expondremos algunos resultados que serán utilizados en posteriores secciones. La mayoría de estos resultados pueden encontrarse en [CM]. A partir de esta sección, k será un cuerpo y A una k-álgebra conmutativa.

Definición 1.2.1 *Sean A una k-álgebra y $\phi : A \to A^{[1]}$ un homomorfismo de k-álgebras. Para una variable U sobre A, denotaremos por ϕ_U a la aplicación $\phi : A \to A[U]$. Diremos que ϕ es una* **aplicación exponencial** *en A si ϕ satisface las dos propiedades siguientes:*

1. $\phi(a) \equiv a \mod U$
2. $\phi_V \phi_U = \phi_{V+U}$, *donde $\phi_V : A \to A[V]$ se extiende a un homomorfismo $\phi_V : A[U] \to A[U, V]$ donde $\phi_V(U) = U$.*

Diremos que una aplicación exponencial es **trivial** *si para cada $a \in A$, $\phi(a) = a$, es decir si ϕ es la inclusión de A en $A[U]$. En caso contrario, diremos que es no trivial.*

Definición 1.2.2 *Sea ϕ una aplicación exponencial sobre A. Llamaremos* **anillo de ϕ-invariantes** *al subanillo de A, definido por*

$$A^{\phi} = \{a \in A | \ \phi(a) = a\} \subseteq A$$

Observar que efectivamente es un subanillo de A gracias a que ϕ es un homomorfismo de k-álgebras. Además, si la aplicación ϕ es no trivial, entonces $A^\phi \neq A$. Gracias al anillo de ϕ-invariantes definiremos otro subanillo importante de A.

Definición 1.2.3 *El* **invariante Derksen** *de una k-álgebra A es el subanillo de A generado por los anillos A^ϕ, donde ϕ recorre todas las aplicaciones exponenciales no triviales de A. Este anillo será denotado por $DK(A)$.*

Dados una aplicación exponencial $\phi : A \to A[U]$ y a un elemento de A, denotaremos al coeficiente de U^n en el polinomio $\phi(a)$ por $D_n(a)$. Decir que ϕ es un homomorfismo de k-álgebras es equivalente a decir que la sucesión $\{D_n(a)\}_{n\geq 0}$ tiene un número finito de elementos distintos de cero, que para todo $n \in \mathbb{N}$, $D_n : A \to A$ es una aplicación k-lineal y que además cumplen la regla de Leibniz:

$$D_n(ab) = \sum_{i+j=n} D_i(a)D_j(b)$$

para todo $n \in \mathbb{N}$ y $a, b \in A$.

Para probar esta equivalencia lo único que debemos observar son los coeficientes de $\phi(ka)$, $\phi(a+b)$ y $\phi(ab)$ en comparación con $k\phi(a)$, $\phi(a)+\phi(b)$ y $\phi(a)\phi(b)$, respectivamente.

Además, las propiedades 1. y 2. de la definición de aplicación exponencial se traduce en las siguientes:

i. D_0 es la aplicación identidad en A.

ii. Para todo número natural i, j:

$$D_i D_j = \binom{i+j}{i} D_{i+j} \tag{1.1}$$

La primera es obvia pues

$$\phi(a) = D_0(a) + U\sum_{n\geq 0} D_{n+1}(a)U^n \equiv a \mod U$$

luego $D_0(a) = a$ para todo $a \in A$, y por tanto $D_0 = Id_A$.

Para ii. calculamos los coeficientes de $\phi_{U+V}(a)$ y $\phi_V\phi_U(a)$. Por un lado,

$$\begin{aligned}
\phi_{U+V}(a) = &\sum_{k\geq 0} D_k(a)(U+V)^k = \sum_{k\geq 0}\sum_{l=0}^{k}\binom{k}{l}D_k(a)V^lU^{k-l} \\
= &\sum_{j\geq 0}\left(\binom{j}{0}D_j(a) + \binom{j+1}{1}D_{j+1}V + \binom{j+2}{2}D_{j+2}V^2 + \cdots\right)U^j \\
= &\sum_{j\geq 0}\sum_{i\geq 0}\binom{i+j}{i}D_{i+j}(a)V^iU^j
\end{aligned}$$

Por otro lado se tiene que

$$\phi_V\phi_U(a) = \phi_V\left(\sum_{j\geq 0} D_j(a)U^j\right) = \sum_{j\geq 0}\phi_V\left(D_j(a)\right)U^j = \sum_{j\geq 0}\sum_{i\geq 0} D_iD_j(a)V^iU^j$$

Por la propiedad 2. de las aplicaciones exponenciales, $\phi_{U+V}(a) = \phi_V\phi_U(a)$, luego se debe cumplir que los coeficientes sean iguales y por tanto,

$$D_iD_j = \binom{i+j}{i}D_{i+j}$$

Lema 1.2.4 *Si k es un cuerpo de característica cero, cada D_n está determinado por D_1, pues*

$$(1.1) \Rightarrow D_n = \frac{D_1^n}{n!}$$

Demostración.
Sabemos que
$$D_i D_j = \frac{(i+j)!}{i!j!} D_{i+j}$$
Como el cuerpo k es de característica cero, para cualesquiera $i, j \in \mathbb{N}$, $(i+j)!$ es distinto de cero y por tanto tiene inverso en k, con lo que podemos despejar D_{i+j} de la igualdad anterior, obteniendo
$$D_{i+j} = \frac{i!j!}{(i+j)!} D_i D_j$$

Probaremos el resultado por inducción en n. D_0 cumple el lema de manera trivial ya que que por definición $0! = 1$ y $D_1^0 = Id = D_0$. Supongamos que es cierto para D_{n-1} y probémoslo para D_n.
$$D_n = D_{n-1+1} = \frac{(n-1)!1!}{n!} D_{n-1} D_1 = \frac{(n-1)!}{n!} \frac{D_1^{n-1}}{(n-1)!} D_1 = \frac{D_1^n}{n!}$$
Con lo que demostramos este lema.

□

A continuación, definiremos una función que nos permitirá probar resultados acerca de las aplicaciones exponenciales en A. Supondremos que A es, a partir de ahora, un dominio conmutativo sobre un cuerpo k.

Dada una aplicación exponencial ϕ en A, definimos el ϕ-grado de un elemento $a \in A$ de la siguiente forma
$$\deg_\phi(a) = \deg_U(\phi(a))$$
Por convenio, diremos que $\deg_\phi(0) = -\infty$.

Observación 1.2.5 *Los elementos no nulos del anillo de ϕ-invariantes son aquellos elementos de A cuyo ϕ-grado es cero.*

La función ϕ-grado verifica las mismas propiedades que la función $\deg_U$, es decir,

- $\deg_\phi(ab) = \deg_\phi(a) + \deg_\phi(b)$
- $\deg_\phi(a+b) \leq \max\{\deg_\phi(a), \deg_\phi(b)\}$

Lema 1.2.6 *Sea ϕ una aplicación exponencial en un dominio A sobre k.*

a. *A^ϕ es factorialmente cerrado en A, es decir, si a y b son dos elementos de A tales que $ab \in A^\phi \setminus 0$, entonces $a, b \in A^\phi$.*

b. *A^ϕ es algebraicamente cerrado en A.*

c. *Para cada $a \in A$, $\deg_\phi(D_i(a)) \leq \deg_\phi(a) - i$. En particular, si $a \in A \setminus 0$ y $n = \deg_\phi(a)$, entonces $D_n(a) \in A^\phi$.*

Demostración.

a. Consideremos $a, b \in A$ tales que $ab \in A^\phi \setminus 0$, entonces su ϕ-grado es cero. Además, por las propiedades de esta función, $\deg_\phi(a) + \deg_\phi(b) = \deg_\phi(ab) = 0$. Esto implica que $\deg_\phi(a) = \deg_\phi(b) = 0$ y por la observación anterior $a, b \in A^\phi$.

b. Sea $a \in A \setminus 0$ algebraico sobre A^ϕ y sea $f(x) = c_n x^n + \cdots + c_1 x + c_0$ el polinomio de menor grado tal que $f(a) = 0$, donde cada $c_i \in A^\phi$ y $c_0 \neq 0$. Si $n = 0$, entonces el polinomio se reduce a $f(x) = c_0 \in A^\phi$, pero entonces $a = c_0$ y $a \in A^\phi$ de manera trivial.

   Consideremos por tanto que $n \geq 1$. Tenemos entonces que $c_n a^n + \cdots + c_1 a + c_0 = 0$, pasando c_0 al segundo miembro y sacando a como factor común en el primero, obtenemos
   $$a(c_n a^{n-1} + \cdots + c_1) = -c_0 \in A^\phi \setminus 0$$
   Por el apartado a. A^ϕ es factorialmente cerrado en A y podemos concluir que $a \in A^\phi$.

c. Por definición de la función ϕ-grado, lo que necesitamos probar es que $\deg_U[\phi(D_i(a))] \leq \deg_\phi(a) - i$, es decir que el coeficiente de U^j en $\phi(D_i(a))$ es cero para $j > \deg_\phi(a) - i$, o equivalentemente queremos probar que $D_j D_i(a) = 0$ para $j > \deg_\phi(a) - i$.

   Consideremos pues $j \in \mathbb{N}$ tal que $j > \deg_\phi(a) - i$, entonces el coeficiente $D_{j+i}(a) = 0$ ya que $j + i > \deg_\phi(a)$. Por la igualdad (1.1), tenemos que $D_j D_i(a) = 0$ para $j > \deg_\phi(a) - i$, que es lo que queriamos probar. Luego, $\deg_\phi(D_i(a)) \leq \deg_\phi(a) - i$.

   En particular, si consideramos $a \in A \setminus 0$ tal que $n = \deg_\phi(a)$, aplicando lo probado anteriormente $\deg_\phi(D^n(a)) \leq n - n = 0$ (observar que en este caso, es una igualdad ya que $D_n(a) \neq 0$ y por tanto $\deg_\phi(D_n(a)) \geq 0$), luego por la observación 1.2.5, se tiene que $D^n(a) \in A^\phi$.

□

Lema 1.2.7 *Sea ϕ una aplicación exponencial no trivial en un dominio A sobre k un cuerpo de característica $p \geq 0$. Sea $x \in A$ un elemento con ϕ-grado mínimo positivo n. Se tienen las siguientes propiedades.*

a. $D_i(x) \in A^\phi$ para cada $i \geq 1$. Además, $D_i(x) = 0$ cuando $i > 1$ no es una potencia de p.

b. Si $a \in A \setminus 0$, entonces n divide $\deg_\phi(a)$.

c. Sea $c = D_n(x) \in A^\phi$. Entonces A es una subálgebra de $A^\phi[c^{-1}][x]$, donde $A^\phi[c^{-1}]$ es la localización de A^ϕ en c.

d. Sea $c = D_n(x)$, entonces $A[c^{-1}] = A^\phi[c^{-1}]^{[1]}$.

Demostración.

En esta prueba usaremos el siguiente hecho:

$$\textit{Si } p \textit{ es primo e } i = p^j q \textit{ para ciertos números naturales } i, j, q, \textit{ entonces } \binom{i}{p^j} \equiv q \mod p.$$

De esta forma si k es un cuerpo de característica p, esta congruencia se convierte en una igualdad [Is]. Por otro lado, observar que este x de grado mínimo positivo existe ya que ϕ es una aplicación exponencial no trivial.

a. Sea $i \geq 1$. Por el apartado c. del lema 1.2.6, $\deg_\phi(D_i(x)) \leq n - i < n$. Como x es de grado mínimo positivo, debe ocurrir que $\deg_\phi(D_i(x)) \leq 0$, por la observación 1.2.5, $D_i(x) \in A^\phi$. Esto prueba la primera parte de la afirmación de este apartado. Observar que $D_0(x) \notin A^\phi$ pues $D_0(x) = x$. Probaremos ahora que $D_i(x) = 0$ cuando $i > 1$ no sea una potencia de p. Para ello, distinguiremos dos casos, si $p = 0$ ó si es un primo p.

   Supongamos que $p = 0$ y consideremos $z \in A \setminus A^\phi$ cuyo ϕ-grado sea $m \geq 1$. Como el coeficiente del monomio de grado máximo de $\phi(x)$, $D_m(z)$, es no nulo, por el lema 1.2.4 tenemos que $D_1^m(z) \neq 0$ y por tanto, $D_1(z) \neq 0$. Además, puesto que $D_i(z) = 0$ para $i > m$, por el mismo lema podemos concluir que $D_1^i(z) = 0$ para todo $i > m$. Sea $M = m + 1 \geq 2$ y sea $x = D_1^{M-2}(z)$. Vamos a probar que el ϕ-grado de este elemento es uno.

$$D_1(x) = D_1 D_1^{M-2}(z) = D_1^{M-1}(z) = D_1^m(z) \neq 0$$

   Para los demás coeficientes excepto el término independiente (que siempre es distinto de cero si $x \neq 0$), es decir, para todo $i \geq 2$, se tiene que $M + i - 2 > m = \deg_\phi(z)$ y por tanto

$$D_i(x) = D_i D_1^{M-2}(z) = \frac{1}{i!} D_1^i D_1^{M-2}(z) = \frac{1}{i!} D_1^{M+i-2}(z) = 0$$

   Luego $\deg_\phi(x) = 1$. Con esto hemos demostrado que si $\mathrm{char}(k) = 0$, entonces existe un elemento en A de ϕ-grado 1, y la afirmación es inmediata, pues $D_i(x) = 0$ para todo $i \geq 2$ ya sean potencias o no de p.

   Supongamos ahora que p es primo y que $i > 1$ no es una potencia de p. Entonces podemos descomponer i como el producto $p^j q$ donde j es un entero no negativo y $q \geq 2$ es un entero no divisible por p. Como

$i - p^j = p^j(q-1) \geq 1$, por la primera parte de este apartado, $D_{i-p^j}(x) \in A^\phi$. Además, utilizando (1.1) y teniendo en cuenta que $p^j \geq 1$, se tiene

$$0 = D_{p^j} D_{i-p^j}(x) = \binom{i}{p^j} D_i(x) = qD_i(x)$$

Como A es un dominio y $q \neq 0$, podemos dividir por q la igualdad anterior y concluir que $D_i(x) = 0$.

b. La prueba cuando $p = 0$ es trivial gracias a que $n = 1$ como hemos visto en la prueba del apartado anterior. Supongamos por tanto que p es primo. Como $D_n(x) \neq 0$, por el apartado a. de este lema se tiene que $n = p^m$ para un cierto $m \geq 0$. Si $m = 0$, entonces $n = 1$ y de nuevo el lema es inmediato. Consideremos entonces el caso donde $m > 0$.

   Sean $a \in A \setminus 0$ y $d = \deg_\phi(a)$ y supongamos que p no divide a d. Por el apartado c. del lema 1.2.6, $\deg_\phi(D_{d-1}(a)) \leq \deg_\phi(a) - (d-1) = 1$. Además, teniendo en cuenta que tanto d como $D_d(a)$ son distintos de cero, por (1.1)

$$D_1 D_{d-1}(a) = \binom{d-1+1}{1} D_{d-1+1}(a) = dD_d(a) \neq 0$$

   por lo que $\deg_\phi(D_{d-1}(a)) = 1 < n$ contradiciendo la minimalidad de n. De aquí se deduce que $d = p^k d_1$ donde $k > 0$ y p no divide a d_1. Razonando análogamente, $\deg_\phi(D_{d-p^k}(a)) \leq \deg_\phi(a) - (d - p^k) = p^k$ y de nuevo por (1.1)

$$D_{p^k} D_{d-p^k}(a) = \binom{d}{p^k} D_d(a) = d_1 D_d(a) \neq 0$$

   Por tanto, $\deg_\phi(D_{d-p^k}(a)) = p^k$. Como $n = p^m$ es minimal, se deduce que $k \geq m$ y que por tanto, n divide a d.

c. Sea $a \in A \setminus 0$. Por el apartado b., su ϕ-grado es un múltiplo de n y por tanto $\deg_\phi(a) = ln$ para l un número natural. Vamos a probar este resultado por inducción en l. Si $l = 0$, entonces $a \in A^\phi$, de lo que podemos concluir que $a \in A^\phi\left[c^{-1}\right][x]$. Supongamos que el resultado es cierto para elementos de grado menor o igual que $(l-1)n$ y probémoslo para este $l \geq 1$.

   Construiremos un elemento de grado menor que ln a partir de otros dos que tienen el mismo término líder. Los dos elementos que vamos a considerar son $c^l a$ y $D_{ln} x^l$.

   En primer lugar comprobemos que $c^l a$ y $D_{ln}(a)x^l$ tienen ϕ-grado ln. Para calcular estos ϕ-grado, debemos tener en cuenta que $\deg_\phi(c) = 0$ y $\deg_\phi(D_{ln}(a)) = 0$, pues c y $D_{ln}(a)$, pertenecen a $A^\phi \setminus 0$ en virtud de 1.2.6 c., entonces

$$\deg_\phi\left(c^l a\right) = l \cdot \deg_\phi(c) + \deg_\phi(a) = ln$$

$$\deg_\phi\left(D_{ln}(a)x^l\right) = \deg_\phi\left(D_{ln}(a)\right) + l \cdot \deg_\phi(x) = ln$$

   Comprobemos ahora que $D_{ln}\left(c^l a\right) = D_{ln}\left(D_{ln}(a)x^l\right)$. Gracias a que ϕ es un homomorfismo de k-álgebras y a que $\phi(c) = c$ y $\phi\left(D_{ln}(a)\right) = D_{ln}(a)$, tenemos que

$$\phi\left(c^l a\right) = c^l \phi(a) \quad \text{y} \quad \phi\left(D_{ln}(a)x^l\right) = D_{ln}(a)\phi\left(x^l\right)$$

   Observar además que si $D_n(z)$ es el coeficiente líder de $\phi(z)$, entonces $D_n(z)^l$ es el coeficiente líder de $\phi\left(z^l\right) = \phi(z)^l$, luego

$$D_{ln}\left(c^l a\right) = c^l D_{ln}(a) \quad \text{y} \quad D_{ln}\Big(D_{ln}(a)x^l\Big) = D_{ln}(a) D_n(x)^l = D_{ln}(a)c^l$$

   De esta manera queda demostrado que $D_{ln}\left(c^l a\right) = D_{ln}\left(D_{ln}(a)x^l\right)$.

   Consideremos $y = c^l a - D_{ln}(a)x^l$. Este elemento tiene ϕ-grado menor que ln y por el apartado b. menor o igual que $(l-1)n$. Por hipótesis de inducción, $y \in A^\phi[c^{-1}][x]$. Puesto que $D_{ln}(a) \in A^\phi$, tenemos que $D_{ln}(a)x^l \in A^\phi[c^{-1}][x]$, y por tanto $a = c^{-l}(y + D_{ln}(a)x^l) \in A^\phi[c^{-1}][x]$.

d. Por el apartado c. de este lema sabemos que $A \subseteq A^{\phi}[c^{-1}][x]$, luego si localizamos A en c, tenemos

$$A\left[c^{-1}\right] \subseteq A^{\phi}\left[c^{-1}\right][x]$$

Por otro lado, A^{ϕ} es un subanillo de A y por tanto $A^{\phi}[c^{-1}] \subseteq A[c^{-1}]$. Utilizando esta contención y el hecho de que x pertenece a A, podemos deducir que

$$A^{\phi}\left[c^{-1}\right][x] \subseteq A\left[c^{-1}\right][x] = A\left[c^{-1}\right]$$

Con esto concluimos que $A\left[c^{-1}\right] = A^{\phi}\left[c^{-1}\right][x]$. Además, como $x \in A \setminus A^{\phi}$, $A\left[c^{-1}\right]$ es el anillo de polinomios en una variable con coeficientes en $A^{\phi}\left[c^{-1}\right]$.

□

Lema 1.2.8 *Sea A un dominio sobre un cuerpo k. Supongamos que existe una aplicación exponencial no trivial ϕ en A. Entonces se tienen las siguientes propiedades.*

a. Si $\operatorname{tr.deg}_k(A)$ es finito, entonces $\operatorname{tr.deg}_k\left(A^{\phi}\right) = \operatorname{tr.deg}_k(A) - 1$.

b. Si $\operatorname{tr.deg}_k(A) = 1$, entonces $A = \tilde{k}^{[1]}$ donde $\tilde{k}$ es la clausura algebraica de k en A y $A^{\phi} = \tilde{k}$.

Demostración.

a. Por el apartado c. del lema 1.2.7 existe $x \in A \setminus A^{\phi}$ de ϕ-grado mínimo positivo n tal que $A \subseteq A^{\phi}[c^{-1}][x]$ donde $c = D_n(x) \in A^{\phi}$.

Tenemos que el elemento $c^{-1} \in A^{\phi}\left[c^{-1}\right][x]$ es algebraico sobre A^{ϕ} con la ecuación $f(y) = cy - 1$. Como A^{ϕ} es algebraicamente cerrado en A y $x \notin A^{\phi}$, x no puede ser algebraico sobre A^{ϕ}. De aquí, podemos deducir que

$$\operatorname{tr.deg}_k\left(A^{\phi}\left[c^{-1}\right][x]\right) = \operatorname{tr.deg}_k\left(A^{\phi}\right) + 1$$

Por otro lado, tanto x como c^{-1} son algebraicos sobre A, ya que x es un elemento de A y c^{-1} es algebraico sobre A^{ϕ} que es un subanillo de A. Concluimos que

$$\operatorname{tr.deg}_k(A) = \operatorname{tr.deg}_k\left(A^{\phi}\left[c^{-1}\right][x]\right)$$

Uniendo las dos igualdades llegamos a que

$$\operatorname{tr.deg}_k\left(A^{\phi}\right) = \operatorname{tr.deg}_k(A) - 1$$

con lo que se demuestra el resultado.

b. Si $\operatorname{tr.deg}_k(A) = 1$ entonces, gracias al apartado anterior, $\operatorname{tr.deg}_k\left(A^{\phi}\right) = 0$, es decir, $k \subseteq A^{\phi}$ es una extensión algebraica.

Consideremos un elemento $a \in A^{\phi}$, vamos a ver que a pertence a la clausura algebraica de k sobre A, la cual hemos denotado por $\tilde{k}$. Como la extensión $k \subseteq A^{\phi}$ es algebraica, existe un polinomio $f(x) \in k[x]$ tal que $f(a) = 0$. En particular, a es un elemento de A para el cual existe un polinomio en $k[x]$ del que es raíz, es decir, a partenece a $\tilde{k}$. Concluimos por tanto que

$$k \subseteq A^{\phi} \subseteq \tilde{k}$$

Observar que como k y $\tilde{k}$ son cuerpos, se deduce que A^{ϕ} también es un cuerpo. Por otro lado, por el lema 1.2.7 d. existe un $c \in A^{\phi}$ tal que

$$A^{\phi}\left[c^{-1}\right]^{[1]} = A\left[c^{-1}\right]$$

Como $c \in A^{\phi}$ y éste es un cuerpo, $c^{-1} \in A^{\phi} \subseteq A$ y por tanto la igualdad anterior queda de la siguiente forma

$$\left(A^{\phi}\right)^{[1]} = A$$

Falta ver que $A^{\phi} = \tilde{k}$, una contención ya se tiene, veamos la otra.

Consideremos $y \in \tilde{k}$, entonces existe un polinomio $f(x) \in k[x]$ con $f(y) = 0$. Pero $k \subseteq A^{\phi}$, luego $f(x)$ lo podemos ver como un polinomio con coeficientes en A^{ϕ}. Como y es un elemento de A y A^{ϕ} es algebraicamente cerrado en A, podemos concluir que $y \in A^{\phi}$ y que por tanto $\tilde{k} = A^{\phi}$.

□

Lema 1.2.9 *Sea A un dominio sobre un cuerpo k. Supongamos que existe una aplicación exponencial no trivial ϕ en A. Sea S un subconjunto multiplicativamente cerrado de $A^{\phi} \setminus 0$. Entonces ϕ se extiende a una aplicación exponencial no trivial $S^{-1}\phi$ en $S^{-1}A$ definida por $\left(S^{-1}\phi\right)(a/s) = \phi(a)/s$ para $a \in A$ y $s \in S$. Además, el anillo de invariantes de $S^{-1}\phi$ es $S^{-1}(A^{\phi})$.*

Demostración.
Vamos a utilizar la propiedad universal del anillo de fracciones. Para ello necesitamos una aplicación de A en $\left(S^{-1}A\right)[U]$ tal que si $s \in S$, entonces $g(s)$ es una unidad en $\left(S^{-1}A\right)[U]$. Consideremos en primer lugar, el siguiente homomorfismo de anillos

$$\begin{array}{cccc} \psi: & A[U] & \longrightarrow & S^{-1}A[U] \\ & \displaystyle\sum_{n\geq 0} a_n U^n & \longmapsto & \displaystyle\sum_{n\geq 0} f(a_n)U^n \end{array}$$

donde $f: A \to S^{-1}A$ es el homomorfismo de anillos tal que $f(a) = a/1$.

Definimos entonces el homomorfismo de anillos entre A y $\left(S^{-1}A\right)[U]$ como la composición $\psi \circ \phi$. Además, si $s \in S \subseteq A^{\phi}$ se tiene que $(\psi \circ \phi)(s) = \psi(s) = s/1$. Como $s \in S$, podemos formar la fracción $1/s \in \left(S^{-1}A\right)[U]$ y por tanto s es una unidad de $\left(S^{-1}A\right)[U]$. Por la propiedad universal de los anillos de fracciones, existe un único homomorfismo de anillos

$$\begin{array}{cccc} S^{-1}\phi: & S^{-1}A & \longrightarrow & \left(S^{-1}A\right)[U] \\ & \left(S^{-1}\phi\right)\left(\dfrac{a}{s}\right) & \longmapsto & \dfrac{\phi(a)}{\phi(s)} = \dfrac{\phi(a)}{s} \end{array}$$

Observar que efectivamente esta aplicación extiende a ϕ, pues si $a \in A$ entonces podemos ver este elemento dentro de $S^{-1}A$ como $a/1$ y por tanto $S^{-1}\phi(a) = \phi(a)/1 = \phi(a)$.

De manera obvia, $S^{-1}\phi$ es un homomorfismo de k-álgebras. Luego, para probar que es una aplicación exponencial, debemos ver que cumple las dos propiedades de su definición.

1. $S^{-1}\phi\left(\dfrac{a}{s}\right) = \dfrac{\phi(a)}{s} \equiv \dfrac{a}{s} \mod U$
2. $S^{-1}\phi_V S^{-1}\phi_U\left(\dfrac{a}{s}\right) = S^{-1}\phi_V\left(\dfrac{\phi_U(a)}{s}\right) = \dfrac{\phi_V\phi_U(a)}{s} = \dfrac{\phi_{U+V}(a)}{s} = S^{-1}\phi_{U+V}\left(\dfrac{a}{s}\right)$

Para terminar la demostración, veamos como son los elementos del anillo de $S^{-1}\phi$-invariantes.

$$(S^{-1}A)^{S^{-1}\phi} = \left\{\frac{a}{s} \in S^{-1}A \,\middle|\, S^{-1}\phi\left(\frac{a}{s}\right) = \frac{a}{s}\right\}$$

Aplicando la definición de $S^{-1}\phi$

$$(S^{-1}A)^{S^{-1}\phi} = \left\{\frac{a}{s} \in S^{-1}A \,\middle|\, \frac{\phi(a)}{s} = \frac{a}{s}\right\}$$

Luego a/s está en el anillo de $S^{-1}\phi$-invariantes si y sólo si $\phi(a) = a$, es decir, si $a \in A^{\phi}$, gracias a lo cual $(S^{-1}A)^{S^{-1}\phi} = S^{-1}A^{\phi}$.

□

El siguiente lema será muy importante para probar el objetivo de este trabajo.

Lema 1.2.10 *Sea A una k-álgebra afín tal que* $\operatorname{tr.deg}_k(A) > 1$. *Si $DK(A) \subsetneq A$, entonces A no es un anillo de polinomios sobre k.*

Demostración.

Probaremos el resultado por reducción al absurdo. Supongamos que $A = k[X_1, \ldots, X_n]$ es un anillo de polinomios en n variables sobre k. Observar que $n > 1$, pues en caso contrario el grado de trascendencia sobre k de A sería 1.

Consideremos, para cada $i \in \{1, \ldots, n\}$, la aplicación $\phi_i : A \to A[U]$ definida por $\phi_i\big(X_j\big) = X_j + \delta_{ij}U$ donde $\delta_{ii} = 1$ y $\delta_{ij} = 0$ en caso contrario. Es claro que estas aplicaciones son homomorfismos de k-álgebras. Probaremos que cumplen las propiedades para ser aplicaciones exponenciales.

- $\phi_i\big(X_j\big) = X_j \mod U$, luego $\phi(a) = a \mod U$ para todo $a \in A$.
- $\phi_{i_V}\phi_{i_U}\big(X_j\big) = \phi_{i_V}\big(X_j + \delta_{ij}U\big) = X_j + \delta_{ij}V + \delta_{ij}U = X_j + \delta_{ij}(V+U) = \phi_{i_{U+V}}\big(X_j\big)$ y por tanto $\phi_{i_V}\phi_{i_U}(a) = \phi_{i_{U+V}}(a)$ para todo $a \in A$.

Además, $A^{\phi_i} = k[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$, ya que $\phi_i(X_j) = X_j$ si $i \neq j$, y por tanto $\bigcup_{i=1}^{n} A^{\phi_i} = A$. De esto se deduce que $DK(A) = A$, lo cual es una contradicción y podemos concluir el lema.

□

1.3. Existencia de Aplicaciones Exponenciales

En esta sección probaremos que existen aplicaciones exponenciales no triviales en ciertos dominios afines sobre cuerpos algebraicamente cerrados. Para ello, primero veremos la existencia de éstas en el anillo de coordenadas de una variedad afín utilizando las acciones de un grupo algebraico sobre una variedad algebraica. En lo que sigue k es un cuerpo infinito.

Definición 1.3.1 *Un* **grupo algebraico** *G es una variedad afín que tiene una estructura de grupo y para la que las operaciones de grupo son morfismos de variedades.*

Ejemplo 1.3.2 *El grupo aditivo $\mathbb{G}_a := (k, +)$ es un grupo algebraico.*

Definición 1.3.3 *Una* **acción de un grupo algebraico** $(G, *)$ *sobre una variedad algebraica X es un morfismo de variedades $\mu : G \times X \to X$ tal que para todo $s, t \in G$ y $p \in X$,*

- *$\mu(e, p) = p$ donde e es el elemento neutro de G.*
- *$\mu(s * t, p) = \mu(s, \mu(t, p))$.*

El siguiente teorema se puede encontrar en el capítulo 6 de [Fu]

Teorema 1.3.4 *Sean $X \subseteq k^m$ e $Y \subseteq k^n$, dos variedades afines. Consideremos $F : X \to Y$, entonces F es un morfismo si y sólo si F es una aplicación polinómica.*

Consideremos el grupo aditivo $\mathbb{G}_a$ y utilicemos el teorema precedente para redefinir la acción del grupo algebraico $G = k$ sobre una variedad afín mediante aplicaciones polinómicas. Veamos primero en que se traducen las propiedades de la acción.

Consideremos $X \subseteq k^n$ una variedad afín y $F_1, \ldots, F_n$ polinomios en $k^{[n+1]}$ cuyas variables denotaremos $\underline{x}, U$, donde $\underline{x} = (x_1, \ldots, x_n)$. Supongamos que la acción del grupo algebraico $\mathbb{G}_a$, a la que llamaremos $\mu : k \times X \to X$ viene dada por $\mu(s, p) = (F_1(p, s), \ldots, F_n(p, s))$.

Gracias a que $\mu(0, p) = p$, tenemos que $(F_1(p, 0), \ldots, F_n(p, 0)) = p$, es decir, para cada $i \in \{1, \ldots, n\}$, $F_i(p, s) = p_i + sF_i'(p, s)$ con $F_i'(p, s) \in k^{[n]}[U]$, luego $F_i(\underline{x}, U) \equiv x_i \mod U$.

La segunda propiedad nos dice que $\mu(s+t,p)=\mu(s,\mu(t,p))$, lo que implica que

$$\Big(F_1(p,s+t),\dots,F_n(p,s+t)\Big)=\Big(F_1\big(F_1(p,t),\dots,F_n(p,t),s\big),\dots,F_n\big(F_1(p,t),\dots,F_n(p,t),s\big)\Big)$$

luego $F_i(\underline{x},U+V)=F_i(F_1(\underline{x},V),\dots,F_n(\underline{x},V),U)$ para cada $i\in\{1,\dots,n\}$. Podemos definir entonces la acción del grupo $\mathbb{G}_a$ como:

Definición 1.3.5 *Dada una variedad afín $X\subseteq k^n$, se define la* **acción del grupo aditivo** $\mathbb{G}_a$ *como una aplicación polinómica $\mu: k\times X\to X$ tal que si $F_i\in k^{[n]}[U]$ para $i=1,\dots,n$ son los polinomios que la definen, entonces se cumplen las siguientes propiedades:*

1. $F_i(\underline{x},U)\equiv x_i \mod U$ *para todo* $i=1,\dots,n$
2. $F_i(\underline{x},U+V)=F_i\big(F_1(\underline{x},V),\dots,F_n(\underline{x},V),U\big)$ *para todo $i=1,\dots,n$ y donde $\underline{x}$ denota a $(x_1,\dots,x_n)$.*

Queremos definir una aplicación exponencial entre los anillos de coordenas de una variedad afín X y $k\times X$, a los cuales denotaremos por $A(X)$ y $A(k\times X)$. Observar que $A(k\times X)\cong A(k)\otimes_k A(X)=k^{[1]}\otimes_k A(X)\cong A(X)^{[1]}$. Además, recordar que toda aplicación polinómica entre dos variedades afines induce un homomorfismo de anillos entre sus anillos de coordenadas. En nuestro caso, cualquier acción del grupo algebraico $\mathbb{G}_a$ sobre una variedad afín X, induce un homomorfismo de anillos $\phi: A(X)\to A(X)^{[1]}$.

Lema 1.3.6 *Cualquier acción del grupo algebraico $\mathbb{G}_a$ en una variedad afín X induce una aplicación exponencial $\phi: A(X)\to A(X)^{[1]}$ donde $A(X)$ es el anillo de coordenadas de X.*

Demostración.

Consideremos $X\subseteq k^n$ una variedad afín y $\mu: k\times X\to X$ una acción del grupo algebraico $\mathbb{G}_a$. Como es una aplicación polinómica, consideremos $F_i(\underline{x},U)\in k^{[n]}[U]$ los polinomios que la definen para $i=1,\dots,n$. Por el párrafo anterior, esta acción define un homomorfismo de anillos entre $A(X)$ y $A(X)^{[1]}$. Este homomorfismo, al que denotaremos ϕ, viene definido de la siguiente forma:

$$\phi: f+I(X)\in A(X)\mapsto f(F_1,\dots,F_n)+I(X)\in A(X)^{[1]}$$

donde $g(\underline{x},U)+I(X)=\sum_{n\geq 0}[h_n(\underline{x})+I(X)]U^n$ y recordemos que $I(X)=\{f\in k^{[n]}: f(x)=0\ \forall x\in X\}$ es el ideal de la variedad X. Observar que realmente la aplicación queda definida por las imágenes de los x_i, las cuales son $\phi(x_i)=F_i(\underline{x},U)+I(X)$.

Queremos probar que este homomorfismo ϕ es una aplicación exponencial. Notar que ϕ es un homomorfismo de k-álgebras con lo que falta comprobar que las otras dos propiedades de estas aplicaciones se cumplen.

1. De la definición de acción de grupo algebraico 1.3.5 se tiene que $F_i(\underline{x},U)\equiv x_i \mod U$. Por tanto, $F_i(\underline{x},U)+I(X)\equiv x_i+I(X) \mod U$ y

$$\phi(f+I(X))=f(\phi(x_1),\dots,\phi(x_n))+I(X)\mod U=f+I(X)$$

   Luego $\phi=Id \mod U$.

2. Para comprobar la propiedad 2. de las aplicaciones exponenciales, debemos componer $\phi_V\phi_U$ entendiendo que ϕ_U,ϕ_V son ambas la aplicación $\phi: A(X)\to A(X)[U]$ donde ϕ_V se extiende a $A(X)[U]\to A(X)[U,V]$ con $\phi_V(U)=U$. Entonces, para todo $i=1,\dots,n$ se tiene que

$$\begin{aligned}\phi_V\phi_U(x_i)&=\phi_V\left(F_i(\underline{x},U)+I(X)\right)\\&=F_i(F_1(\underline{x},V),\dots,F_n(\underline{x},V),U)+I(X)\\&=F_i(\underline{x},U+V)+I(X)=\phi_{U+V}(x_i)\end{aligned}$$

y entonces se cumple la segunda propiedad, pues

$$\begin{aligned} \phi_V\phi_U(f+I(X)) = &\ f(\phi_V\phi_U(x_1),\dots\phi_V\phi_U(x_n)) \\ = &\ f(\phi_{U+V}(x_1),\dots,\phi_{U+V}(x_n)) \\ = &\ \phi_{U+V}(f+I(X)) \end{aligned}$$

Con lo que hemos probado el resultado.

□

Lema 1.3.7 *Una acción del grupo algebraico $\mathbb{G}_a$ en una variedad afín $X \subseteq k^n$ es no trivial si y sólo si la aplicación exponencial asociada también es no trivial.*

Demostración.

$\Rightarrow$ Consideremos una acción de grupo no trivial $\mu : k \times X \to X$. Entonces, debe existir $(s,p) \in k \times X$ tal que $\mu(s,p) = (F_1(p,s),\dots,F_n(p,s)) \neq p$. Esto equivale a decir que existe $i \in \{1,\dots,n\}$ tal que $F_i(p,s) \neq p_i$, pero por las propiedades de μ, $F_i(p,0) = p_i$. Podemos deducir entonces que

$$F_i(p,s) = p_i + sF_i'(p,s)$$

con $F_i' \in k^{[n]}[U]$ tal que $F_i'(p,s) \neq 0$.

Consideremos la aplicación exponencial inducida por μ, denotada por $\phi : A(X) \to A(X)[U]$. Entonces

$$\phi(x_i + I(X)) = x_i + UF_i'(\underline{x},U) + I(X)$$

Falta ver que $F_i'(\underline{x},U) + I(X) \neq 0$.

Supongamos que $F_i'(\underline{x},U) + I(X) := \sum_{j\geq 0} G_j(\underline{x})U^j + I(X) = 0$, tenemos pues que $G_j(\underline{x}) \in I(X)$ para todo $j \geq 0$, es decir, $G_j(q) = 0$ para todo $q \in X$. Teniendo en cuenta que $p \in X$ y por tanto que $G_j(p) = 0$ para todo $j \geq 0$,

$$F_i'(p,s) = \sum_{j\geq 0} G_j(p)s^j = 0$$

contradiciendo el hecho de que $F_i(p,s) \neq p_i$. De esta manera $\phi(x_i+I(X)) \neq x_i+I(X)$ y la aplicación exponencial ϕ también es no trivial.

$\Leftarrow$ Supongamos que $\mu : k \times X \to X$ es la acción de grupo trivial. Entonces, con la notación del apartado anterior, tenemos que para todo $i = 1,\dots,n$, $F_i(\underline{x},U) = x_i$. Podemos deducir que la aplicación exponencial ϕ inducida por μ es trivial, ya que $\phi(x_i + I(X)) = x_i + I(X)$ para todo $i = 1,\dots,n$ y por tanto $\phi(f + I(X)) = f(\phi(x_1),\dots,\phi(x_n)) = f + I(X)$.

Luego, si la aplicación exponencial inducida es no trivial, entonces la acción debe ser no trivial.

□

Ejemplo 1.3.8 *Aplicación exponencial no trivial en $k^{[4]}$.*

Vamos a construir una aplicación exponencial no trivial en $k^{[4]}$, donde k es un cuerpo infinito de característica $p > 0$. Como $I\left(k^4\right) = \{0\}$, entonces $A\left(k^4\right) = k^{[4]}$ y por los razonamientos anterior, basta encontrar una acción del grupo algebraico $\mathbb{G}_a$ en k^4 no trivial. Consideremos $\mu : k \times k^4 \to k^4$ definida por los siguientes polinomios:

$$\begin{array}{ll} F_1(X,Y,Z,T,U) = X, & F_2(X,Y,Z,T,U) = Y - X^{m(p^e-1)}U^{p^e} \\ F_3(X,Y,Z,T,U) = Z + X^mU, & F_4(X,Y,Z,T,U) = T \end{array}$$

donde m, e son enteros tales que $e, m > 1$. De manera obvia, dados un par $(t,q) \in k \times k^4$,

$$\Big(F_1(q,t), F_2(q,t), F_3(q,t), F_4(q,t)\Big) \in k^4$$

Falta ver que cumplen las propiedades de la definición 1.3.5.

1. $$F_1 \equiv X \mod U, \quad F_2 \equiv Y \mod U, \quad F_3 \equiv Z \mod U, \quad F_4 \equiv T \mod U$$

2. Denotemos por $\underline{X} = (X, Y, Z, T)$, para simplificar la notación.
   - ⋆ $F_1(\underline{X}, U + V) = X$ y
   $$F_1(F_1(\underline{X}, V), F_2(\underline{X}, V), F_3(\underline{X}, V), F_4(\underline{X}, V), U) = F_1(\underline{X}, V) = X$$
   - ⋆ $F_2(\underline{X}, U + V) = Y - X^{m(p^e-1)}(U + V)^{p^e}$ y
   $$\begin{aligned} F_2(F_1(\underline{X}, V), F_2(\underline{X}, V), F_3(\underline{X}, V), F_4(\underline{X}, V), U) = & \; F_2(\underline{X}, V) - F_1(\underline{X}, V)^{m(p^e-1)}U^{p^e} \\ = & \; Y - X^{m(p^e-1)}(V + U)^{p^e} \end{aligned}$$
   - ⋆ $F_3(\underline{X}, U + V) = Z + X^m(U + V)$ y
   $$\begin{aligned} F_3(F_1(\underline{X}, V), F_2(\underline{X}, V), F_3(\underline{X}, V), F_4(\underline{X}, V), U) = & \; F_3(\underline{X}, V) + F_1(\underline{X}, V)^m U \\ = & \; Z + X^m(U + V) \end{aligned}$$
   - ⋆ $F_4(\underline{X}, U + V) = T$ y
   $$F_4(F_1(\underline{X}, V), F_2(\underline{X}, V), F_3(\underline{X}, V), F_4(\underline{X}, V), U) = F_4(\underline{X}, V) = T$$

Notar que esta aplicación es no trivial, basta considerar $(1, 0, 0, 0, 1) \in k^5$, pues $\mu(1, 0, 0, 0, 1) = (1, -1, 1, 0)$.

A continuación estudiaremos cuando los dominios afines sobre un cuerpo algebraicamente cerrado poseen aplicaciones exponenciales no triviales. Recordemos el teorema de los ceros de Hilbert.

Teorema 1.3.9 (Teorema de los ceros de Hilbert) *Si k es un cuerpo algebraicamente cerrado, entonces*

$$\sqrt{\mathfrak{p}} = I(V(\mathfrak{p}))$$

donde $I(X) = \left\{f \in k^{[n]} : f(x) = 0 \ \forall x \in X \subseteq k^n\right\}$ y $V(S) = \left\{x \in k^n : f(x) = 0 \ \forall f \in S \subseteq k^{[n]}\right\}$.

Lema 1.3.10 *Sea $B = k^{[n]}/\mathfrak{p}$ un dominio afín sobre un cuerpo k algebraicamente cerrado y supongamos que $V(\mathfrak{p})$ admite una acción de grupo no trivial, entonces existe una aplicación exponencial no trivial en B.*

Demostración.
Como B es un dominio, $\mathfrak{p}$ es un ideal primo y por el teorema de los ceros de Hilbert, $\mathfrak{p} = \sqrt{\mathfrak{p}} = I(V(\mathfrak{p}))$. Por tanto, B es el anillo de coordenadas para la variedad afín $V(\mathfrak{p})$, la cual admite una acción de grupo no trivial. Por los lemas 1.3.6 y 1.3.7 podemos definir una aplicación exponencial no trivial en B.

□

Ejemplo 1.3.11

Consideremos un cuerpo k infinito algebraicamente cerrado de característica $p > 0$. Sea

$$B = k[X, Y, Z, T] \Big/ \left\langle X^m Y + T^s + Z^{p^e} \right\rangle$$

donde m, e, s son enteros positivos tales que $s = p^r q$ con $q > 1$ y $p \nmid q$, $e > r \geq 1$ y $m > 1$.
Observar que $f(X, Y, Z, T) = X^m Y + T^s + Z^{p^e}$ es un polinomio irreducible en $k[X, Y, Z, T]$ y por tanto B es un dominio afín sobre un cuerpo algebraicamente cerrado. Vamos a dar un ejemplo de aplicación exponencial no trivial. Como es un domínio afín, podemos ver que B es el anillo de coordenadas de la variedad afín $V(\mathfrak{p})$ y por el lema anterior, debemos definir una aplicación del grupo algebraico $\mathbb{G}_a$ no trivial en esta variedad afín.

Para definir esta acción, consideremos la acción de grupo definida en el ejemplo 1.3.8. Vamos a comprobar que también es una acción de grupo en X, es decir que $\mu(k \times X) \subseteq X$.

Sea el par $(l, w) \in k \times X$, entonces $f(w) = 0$ ya que $w \in V(f)$. Para demostrar que $\mu(l, w) \in X$, basta ver que $f(\mu(l, w)) = 0$.

$$\mu(l, w) = \left(w_1, w_2 - w_1^{m(p^e-1)} l^{p^e}, w_3 + w_1^m l, w_4\right)$$

Entonces

$$f(\mu(l, w)) = w_1^m \left(w_2 - w_1^{m(p^e-1)} l^{p^e}\right) + w_4^s + (w_3 + w_1^m l)^{p^e} = w_1^m w_2 + w_4^s + w_3^{p^e} = 0$$

Para ver que esta acción es no trivial considerar el punto $w = (1, 0, 0, 0) \in X = V(f)$, entonces $\mu(1, w) = (1, -1, 1, 0) \neq w$.

1.4. Graduación y Aplicaciones Exponenciales

A lo largo de esta sección, consideraremos A un dominio afín sobre un cuerpo k. En ella, daremos el concepto de $\mathbb{Z}$-filtración propia admisible y probaremos la existencia de aplicaciones exponenciales no triviales para el anillo graduado $gr(A)$ con estas filtraciones admisible, resultado expuesto en [Cr].

Definición 1.4.1 *Sea A un dominio afín sobre k. Se dice que A tiene una* **$\mathbb{Z}$-filtración propia** *si existe una colección de k-espacios lineales $\{A_n\}_{n\in\mathbb{Z}}$ de A satisfaciendo*

i. $A_n \subseteq A_{n+1}$ *para todo* $n \in \mathbb{Z}$.

ii. $A = \bigcup_{n\in\mathbb{Z}} A_n$.

iii. $\bigcap_{n\in\mathbb{Z}} A_n = (0)$.

iv. $(A_n \setminus A_{n-1}) \cdot (A_m \setminus A_{m-1}) \subseteq A_{n+m} \setminus A_{n+m-1}$ *para todo* $n, m \in \mathbb{Z}$.

Cualquier $\mathbb{Z}$-filtración propia en A determina el siguiente anillo $\mathbb{Z}$-graduado

$$gr(A) := \bigoplus_{i\in\mathbb{Z}} A_i/A_{i-1}$$

Lema 1.4.2 *$gr(A)$ es un dominio de integridad.*

Demostración.
Gracias a la condición iv. de la definición de $\mathbb{Z}$-filtración propia, si $a \in A_n \setminus A_{n-1}$ y $b \in A_m \setminus A_{m-1}$ son dos elementos de A distintos de cero, se tiene que $ab \in A_{n+m} \setminus A_{n+m-1}$ y por tanto, el producto de sus clases es distinto de cero.

□

Consideremos la aplicación

$$\rho : A \to gr(A) \quad \text{definida por} \quad \rho(a) = a + A_{n-1} \quad \text{si } a \in A_n \setminus A_{n-1}$$

Observar que ρ no es un homomorfismo de anillo en general, pues si $i < n$ y $a_1, \ldots, a_l \in A_n \setminus A_{n-1}$ tal que $a_1 + \cdots + a_l \in A_i \setminus A_{i-1} (\subseteq A_{n-1})$, entonces $\rho(a_1 + \cdots + a_l) \neq 0$ pero $\rho(a_1) + \cdots + \rho(a_l) = (a_1 + \cdots + a_l) + A_{n-1} = 0$.

Definición 1.4.3 *Diremos que una $\mathbb{Z}$-filtración propia $\{A_n\}_{n\in\mathbb{Z}}$ de un dominio afín A sobre un cuerpo k es* **admisible** *si existe un conjunto de generadores finito Γ de A tal que, para cualquier $n \in \mathbb{Z}$ y $a \in A_n$, a puede ser escrito como una suma finita de monomios en elementos de Γ y cada uno de estos monomios son elementos de A_n. Es decir, si $\Gamma = \{a_1, \ldots, a_l\}$, entonces*

$$a = \sum_{\underline{i}\in I} \alpha_{\underline{i}} a_1^{i_1} \cdots a_l^{i_l}$$

donde $\alpha_{\underline{i}} \in k$, I es un conjunto finito de índices con $\underline{i} = (i_1, \ldots, i_l)$ y $a_1^{i_1} \cdots a_l^{i_l} \in A_n$ para todo $\underline{i} \in I$.

Observación 1.4.4 *Supongamos que A tiene una $\mathbb{Z}$-filtración propia y $\Gamma = \{a_1, \ldots, a_l\}$ un conjunto finito de generadores que hacen a la filtración admisible. Entonces $gr(A)$ está generado por $\rho(\Gamma)$.*

Demostración.

Sea $a \in A_n \setminus A_{n-1}$, entonces por definición de $\mathbb{Z}$-filtración propia admisible, existen elementos $\alpha_{\underline{i}} \in k$ con $\underline{i} = (i_1, \ldots, i_l) \in I$ un conjunto de índices finito tales que

$$a = \sum_{\underline{i} \in I} \alpha_{\underline{i}} a_1^{i_1} \cdots a_l^{i_l}$$

donde cada sumando pertenece a A_n. Gracias a que $a \notin A_{n-1}$, debe existir al menos un sumando que no pertenezca a A_{n-1}. Sea $J \subseteq I$ el conjunto de índices para los que los sumandos de a no están en A_{n-1}. Entonces

$$\begin{aligned} \rho(a) &= \rho\left(\sum_{\underline{i} \in I} \alpha_{\underline{i}} a_1^{i_1} \cdots a_l^{i_l}\right) = \left(\sum_{\underline{i} \in I} \alpha_{\underline{i}} a_1^{i_1} \cdots a_l^{i_l}\right) + A_{n-1} \\ &= \sum_{\underline{i} \in J} \left(\alpha_{\underline{i}} a_1^{i_1} \cdots a_l^{i_l} + A_{n-1}\right) = \sum_{\underline{i} \in J} \alpha_{\underline{i}} \rho(a_1)^{i_1} \cdots \rho(a_l)^{i_l} \end{aligned}$$

y por tanto todo elemento de $gr(A)$ se puede expresar como una combinación de elementos de $\rho(\Gamma)$, con lo que $gr(A)$ está generado por $\rho(\Gamma)$.

$\square$

Lema 1.4.5 *Supongamos que A tiene un estructura de $\mathbb{Z}$-álgebra graduada, $A = \bigoplus_{i \in \mathbb{Z}} C_i$. Entonces existe una $\mathbb{Z}$-filtración propia $\{A_n\}_{n \in \mathbb{Z}}$ en A definida por $A_n = \bigoplus_{i \leq n} C_i$. Además, $gr(A) \cong A$ y, para cualquier elemento $a \in A$, la imagen de $\rho(a)$ bajo el isomorfismo $gr(A) \to A$ es la componente de a en A de grado máximo. Si A es finitamente generado como k-álgebra, entonces la filtración definida anteriormente en A es admisible.*

Demostración.

Probaremos en primer lugar que $\{A_n\}_{n \in \mathbb{Z}}$ es una $\mathbb{Z}$-filtración propia verificando cada una de las propiedades.

i. La propiedad *i.*, se tiene por definición de los A_n, pues $A_n := \bigoplus_{i \leq n} C_i \subseteq \bigoplus_{i \leq n+1} C_i =: A_{n+1}$.

ii. Para la segunda propiedad, observar que

$$A = \bigoplus_{n \in \mathbb{Z}} C_i = \bigcup_{n \in \mathbb{Z}} \bigoplus_{i \leq n} C_i = \bigcup_{n \in \mathbb{Z}} A_n$$

iii. Consideremos $0 \neq a \in \bigcap_{n \in \mathbb{Z}} A_n$, entonces $a \in \bigoplus_{i \leq n} C_i$ para todo $n \in \mathbb{Z}$. Luego $a = \sum_{i \leq n} c_i$ para todo $n \in \mathbb{Z}$. Como $a \neq 0$, existe $c_m \neq 0$, con $c_m \in C_m$ en la expresión de a, pero entonces $a \notin \bigoplus_{i \leq m-1} C_i$ dando una contradicción. Por tanto $\bigcap_{n \in \mathbb{Z}} A_n = (0)$ con lo que se tiene la propiedad *iii.*

iv. Por último, consideremos $a \in A_n \setminus A_{n-1}$ y $b \in A_m \setminus A_{m-1}$, entonces $a = \sum_{i \leq n} c_i$ con $c_n \neq 0$ y $b = \sum_{j \leq m} d_j$ con $d_m \neq 0$. Como $\{C_i\}_{i \in \mathbb{Z}}$ es una graduación de A, $C_i C_j \subseteq C_{i+j}$ y además el término de mayor grado en ab es $c_n d_m \in C_{n+m}$, por tanto, $ab \in A_{n+m}$. Como A es un dominio, $c_n d_m \neq 0$ luego, $ab \notin A_{n+m-1}$, obteniendo así la propiedad *iv*.

Probaremos ahora que $gr(A) \cong A$ considerando la aplicación $\varphi : gr(A) \to A$ definida por:

Dado $a \in A_n \setminus A_{n-1}$, $\varphi(\rho(a)) = c_n$, donde c_n es la componente de mayor grado de $a \in A$.

Para probar que esta aplicación es un isomorfismo de k-álgebras, consideremos $\varphi_n : A_n / A_{n-1} \to C_n$, definida como antes.

- Debemos ver que φ_n está bien definida. Primero observar que si $a \in A_n \setminus A_{n-1}$, entonces su componente de mayor grado pertenece a C_n.

  Además, si dos elementos $a, b \in A_n \setminus A_{n-1}$ son dos representantes de la misma clase en A_n/A_{n-1}, entonces las componentes de grado máximo de a y b son iguales, luego $\varphi_n(\rho(a) - \rho(b)) = 0$, lo que prueba que está bien definida.

- Es obvio que φ_n es un homomorfismo de k-módulos para todo $n \in \mathbb{Z}$. Bastar ver que dado $\alpha \in k$ y $a, b \in A_n \setminus A_{n-1}$, las componentes de grado máximo de αa y $a+b$ son αc_n y $c_n + d_n$ respectivamente, donde c_n y d_n son las componentes de mayor grado de a y b.

- Observar que si $a \in A_n \setminus A_{n-1}$ y $b \in A_m \setminus A_{m-1}$, entonces $\varphi_{n+m}(\rho(ab)) = \varphi_n(\rho(a))\varphi_m(\rho(b))$, gracias a que el término de mayor grado de ab es el producto de los términos de mayor grado de a y b. Luego $\varphi : gr(A) \to A$ es un homomorfismo de anillos.

- Por último probaremos la biyectividad. Para la inyectividad basta observar que si la componente de a en C_n es cero, entonces $a \in A_{n-1}$ y por tanto $a + A_{n-1} = 0$. La sobreyectividad se tiene pues si $c \in C_n$, entonces $c \in \bigoplus_{i \leq n} C_i = A_n$, luego $\varphi(\rho(c)) = c$.

Con esto podemos concluir que $gr(A) \cong A$.

Para terminar con la demostración de este lema, supongamos que A es una k-álgebra de generación finita y que $\Gamma = \{a_1, \ldots, a_l\}$ es el conjunto de generadores de A como k-álgebra. Entonces, dado $a \in A$, podemos escribir a en los generadores de la forma

$$a = \sum_{\underline{i} \in I} \alpha_{\underline{i}} a_1^{i_1} \cdots a_l^{i_l}$$

donde $0 \neq \alpha_{\underline{i}} \in k$, e $\underline{i} = (i_1, \ldots, i_n) \in I$ con I un conjunto finito de índices. Por otro lado, $a \in \bigoplus_{n \in \mathbb{Z}} C_n$ y por tanto existe un entero n, tal que $a \in A_n \setminus A_{n-1}$. Esto implica que cada término de la expresión de a debe pertenecer a $A_i \subseteq A_n$ y por tanto la $\mathbb{Z}$-filtración propia es admisible.

□

Teorema 1.4.6 *Sea A un dominio afín sobre k con una $\mathbb{Z}$-filtración propia que es admisible. Supongamos que existe ϕ una aplicación exponencial no trivial en A. Entonces ϕ induce una aplicación no trivial $\overline{\phi}$ en $gr(A)$ tal que $\rho\left(A^{\phi}\right) \subseteq gr(A)^{\overline{\phi}}$.*

Demostración.

Sea $\Gamma = \{a_1, \ldots, a_l\}$ el conjunto de generadores de A que hacen a la $\mathbb{Z}$-filtración admisible y definimos la función $\mathrm{gr.deg} : gr(A) \to \mathbb{Z}$ de la siguiente forma:

$$\text{Dado } a \in A_n \setminus A_{n-1}, \quad \mathrm{gr.deg}(\rho(a)) = n.$$

Por convenio, diremos que $\mathrm{gr.deg}(0) = -\infty$ y por comodidad $\mathrm{gr.deg}(\rho(a))$ lo denotaremos $\mathrm{gr.deg}(a)$.

Consideremos $a \in A_n \setminus A_{n-1}$ y $b \in A_m \setminus A_{m-1}$. Por definición de $\mathbb{Z}$-filtación propia, $ab \in A_{n+m} \setminus A_{n+m-1}$ y por tanto $\mathrm{gr.deg}(ab) = \mathrm{gr.deg}(a) + \mathrm{gr.deg}(b)$. Por otro lado, observar que $a + b \in A_{\text{máx}\{n,m\}}$ aunque no podemos garantizar que no esté en $A_{\text{máx}\{n,m\}-1}$, luego $\mathrm{gr.deg}(a+b) \leq \text{máx}\{\mathrm{gr.deg}(a), \mathrm{gr.deg}(b)\}$.

En resumen, esta función cumple las propiedades:

- $\mathrm{gr.deg}(ab) = \mathrm{gr.deg}(a) + \mathrm{gr.deg}(b)$

- $\mathrm{gr.deg}(a+b) \leq \text{máx}\{\mathrm{gr.deg}(a), \mathrm{gr.deg}(b)\}$

Vamos a extender esta función a $gr(A)[U]$, asignando un valor racional adecuado a $\mathrm{gr.deg}(U)$.

Consideremos

$$C = \left\{ \frac{\mathrm{gr.deg}\,(a_j) - \mathrm{gr.deg}\,(D_i\,(a_j))}{i} \middle| a_j \in \Gamma, D_i\,(a_j) \neq 0, i \in \mathbb{Z}_+ \right\}$$

Veamos que debido a que ϕ es una aplicación exponencial no trivial este conjunto es no vacío. Decir que C es no vacío equivale a que exista un $a_j \in \Gamma$ tal que $\phi(a_j) \neq a_j$, pues si se cumple la desigualdad, existe $i \in \mathbb{Z}_+$ tal que $D_i(a_j) \neq 0$.

Supongamos que $\phi(a_j) = a_j$ para todo $a_j \in \Gamma$ y sea $a \in A$. Como Γ es un conjunto de generadores de A, existen $\alpha_{\underline{i}} \in k$ tales que

$$a = \sum_{\underline{i} \in I} \alpha_{\underline{i}} a_1^{i_1} \cdots a_l^{i_l}$$

donde $\underline{i} = (i_1, \ldots, i_l) \in I$, conjunto finito de índices. Si aplicamos ϕ,

$$\phi(a) = \phi\left(\sum_{\underline{i} \in I} \alpha_{\underline{i}} a_1^{i_1} \cdots a_l^{i_l}\right) = \sum_{\underline{i} \in I} \alpha_{\underline{i}} \phi(a_1)^{i_1} \cdots \phi(a_l)^{i_l} = \sum_{\underline{i} \in I} \alpha_{\underline{i}} a_1^{i_1} \cdots a_l^{i_l} = a$$

Con esto hemos demostrado que $A = A^{\phi}$, lo cual es una contradicción con el hecho de que la aplicación ϕ es no trivial y por tanto $C \neq \emptyset$.

Además, para todo $j \in \{1, \ldots, l\}$, $D_m(a_j) = 0$ para $m \geq deg(a_j)$. Luego cada $a_j \in \Gamma$ aporta un número finito de elementos al conjunto, gracias a lo cual C tiene mínimo. Definimos $\operatorname{gr.deg}(U)$ como mínimo del conjunto C.

A continuación, daremos una desigualdad que nos será de utilidad para probar la existencia de una aplicación exponencial en $gr(A)$.

Aplicando las propiedades de la función gr. deg, se tiene que para cada $a_j \in \Gamma$ y $n \in \mathbb{N}$ tal que $D_n(a_j) \neq 0$,

$$\operatorname{gr.deg}(D_n(a_j)U^n) = \operatorname{gr.deg}(D_n(a_j)) + n \cdot \operatorname{gr.deg}(U) \leq \operatorname{gr.deg} D_n(a_j) + n \cdot \frac{\operatorname{gr.deg}(a_j) - \operatorname{gr.deg}(D_n(a_j))}{n} = \operatorname{gr.deg}(a_j)$$

Observar que si $D_n(a) = 0$, entonces la desigualdad se cumple de manera trivial ya que $\operatorname{gr.deg}(D_n(a)U^n) = \operatorname{gr.deg}(0) = -\infty$. Se deduce que

$$\operatorname{gr.deg}(\phi(a_j)) \leq \operatorname{gr.deg}(a_j)$$

Además esta desigualdad se alcanza, basta tomar $n \in \mathbb{Z}_+$ y $a_j \in \Gamma$ tales que den el mínimo del conjunto C. Veamos que gracias a que la filtración es admisible también se tiene que

$$\operatorname{gr.deg}(D_n(a)U^n) \leq \operatorname{gr.deg}(a) \tag{1.2}$$

para $a \in A$.

Consideremos $a \in A$. Este elemento a se puede escribir como

$$a = \sum_{\underline{i} \in I} \alpha_{\underline{i}} a_1^{i_1} \cdots a_l^{i_l}$$

donde $\alpha_{\underline{i}} \in k$, $i = (i_1, \ldots, i_l) \in I$, con I conjunto finito de índices. Entonces,

$$\begin{aligned}
\operatorname{gr.deg}(\phi(a)) = \quad & \operatorname{gr.deg}\left[\phi\left(\sum_{\underline{i} \in I} \alpha_{\underline{i}} a_1^{i_1} \cdots a_l^{i_l}\right)\right] = \operatorname{gr.deg}\left(\sum_{\underline{i} \in I} \alpha_{\underline{i}} \phi(a_1)^{i_1} \cdots \phi(a_l)^{i_l}\right) \\
\leq \quad & \max_{\underline{i} \in I} \left\{\operatorname{gr.deg}\left(\alpha_{\underline{i}} \phi(a_1)^{i_1} \cdots \phi(a_l)^{i_l}\right)\right\} \\
= \quad & \max_{\underline{i} \in I} \left\{\operatorname{gr.deg}\left(\alpha_{\underline{i}}\right) + i_1 \operatorname{gr.deg}(\phi(a_1)) + \cdots + i_l \operatorname{gr.deg}(\phi(a_l))\right\} \\
\leq \quad & \max_{\underline{i} \in I} \left\{\operatorname{gr.deg}\left(\alpha_{\underline{i}}\right) + i_1 \operatorname{gr.deg}(a_1) + \cdots + i_l \operatorname{gr.deg}(a_l)\right\} \\
= \quad & \max_{\underline{i} \in I} \{\operatorname{gr.deg}\left(\alpha_{\underline{i}} a_1^{i_1} \cdots a_l^{i_l}\right)\} = \operatorname{gr.deg}(a)
\end{aligned}$$

Ahora, como $\operatorname{gr.deg}(D_n(a)U^n) \leq \operatorname{gr.deg}(\phi(a))$, tenemos la desigualdad que queriamos probar.

Para definir la aplicación exponencial en $gr(A)$, necesitamos el siguiente conjunto: Dado $a \in A$ definimos

$$S(a) = \{n \in \mathbb{N} \mid \operatorname{gr.deg}(D_n(a)U^n) = \operatorname{gr.deg}(a)\}$$

Observar que $0 \in S(a)$, pues $D_0(a) = a$ y por tanto obviamente, tienen el mismo grado. Además, notar que si $n \in S(a)$, entonces $\operatorname{gr.deg}(U^n) \in \mathbb{Z}$, ya que $\operatorname{gr.deg}(U^n) = \operatorname{gr.deg}(a) - \operatorname{gr.deg}(D_n(a)) \in \mathbb{Z}$

Definimos para cada $a \in A$,

$$\overline{\phi}(\rho(a)) = \sum_{n \in S(a)} \rho(D_n(a))U^n$$

Extendemos linealmente esta definición para obtener una aplicación $\overline{\phi} : gr(A) \to gr(A)[U]$. Vamos a probar que es una aplicación exponencial no trivial.

Lo primero que debemos ver es que está bien definida. Consideremos $\rho(a) = \rho(b)$ para $a, b \in A_n \setminus A_{n-1}$, entonces $a = b + a_{n-1}$ donde $a_{n-1} \in A_{n-1}$. Queremos probar la siguiente igualdad

$$\overline{\phi}(\rho(a)) = \sum_{m \in S(a)} \rho(D_m(a))U^m = \sum_{m' \in S(b)} \rho(D_{m'}(b))U^{m'} = \overline{\phi}(\rho(b))$$

Para ello debemos ver que $S(a) = S(b)$ y que los coeficientes son iguales. Probaremos primero que $S(a) = S(b)$ por doble inclusión.

Sea $m \in S(a)$, entonces por definición

$$\operatorname{gr.deg}(D_m(a)U^m) = \operatorname{gr.deg}(D_m(b + a_{n-1})U^m) = \operatorname{gr.deg}(a) = \operatorname{gr.deg}(b)$$

Recordemos que D_m es k-lineal, y por tanto

$$\operatorname{gr.deg}(D_m(b + a_{n-1})U^m) = \operatorname{gr.deg}([D_m(b) + D_m(a_{n-1})]U^m)$$

Por las propiedades de esta función,

$$\begin{aligned}\operatorname{gr.deg}([D_m(b) + D_m(a_{n-1})]U^m) \quad &\leq \text{máx}\{\operatorname{gr.deg}(D_m(b)U^m),\ \operatorname{gr.deg}(D^m(a_{n-1})U^m)\} \\ &\leq \text{máx}\{\operatorname{gr.deg}(D_m(b)U^m),\ \operatorname{gr.deg}(a_{n-1})\}\end{aligned}$$

Uniendo las desigualdades obtenemos que

$$\operatorname{gr.deg}(b) \leq \text{máx}\{\operatorname{gr.deg}(D_m(b)U^m),\ \operatorname{gr.deg}(a_{n-1})\}$$

Pero, como $a_{n-1} \in A_{n-1}$ y $b \in A_n \setminus A_{n-1}$, $\operatorname{gr.deg}(a_{n-1}) < \operatorname{gr.deg}(b)$ y podemos concluir que

$$\operatorname{gr.deg}(b) \leq \operatorname{gr.deg}(D_m(b)U^m)$$

Por (1.2), tenemos la igualdad. La otra inclusión es análoga, pues $a = b + a_{n-1}$ y por tanto $b = a - a_{n-1}$, luego podemos aplicar el mismo razonamiento.

Para terminar de probar que está bien definida, tenemos que ver que $\rho(D_m(a)) = \rho(D_m(b))$. Supongamos que $D_m(a), D_m(b) \in A_j \setminus A_{j-1}$, observar que deben estar en la misma componente homogénea pues

$$\operatorname{gr.deg}(D_m(a)) = \operatorname{gr.deg}(a) - \operatorname{gr.deg}(U^m) = \operatorname{gr.deg}(b) - \operatorname{gr.deg}(U^m) = \operatorname{gr.deg}(D_m(b))$$

Notar además que tanto $D_m(a)$ como $D_m(b)$ son distintos de cero si $a, b \neq 0$ pues $m \in S(a) \cap S(b)$.

Por la linealidad de la aplicación D_m, se tiene que

$$\rho(D_m(a)) = D_m(b + a_{n-1}) + A_{j-1} = D_m(b) + A_{j-1} + D_m(a_{n-1}) + A_{j-1}$$

Veamos que $D_m(a_{n-1}) + A_{j-1} = 0$. Supongamos lo contrario, entonces $D_m(a_{n-1}) \in A_j \setminus A_{j-1}$ ya que $D_m(a) \in A_j$. Esto implica que $\operatorname{gr.deg}(D_m(a_{n-1})) = j = \operatorname{gr.deg}(D_m(a))$. Consideremos la siguiente cadena de desigualdades:

$$\begin{aligned}\operatorname{gr.deg}(a_{n-1}) \quad &\geq \operatorname{gr.deg}(D_m(a_{n-1})U^m) = \operatorname{gr.deg}(D_m(a_{n-1})) + \operatorname{gr.deg}(U^m) \\ &= j + \operatorname{gr.deg}(U^m) = \operatorname{gr.deg}(D_m(a)) + \operatorname{gr.deg}(U^m) \\ &= \operatorname{gr.deg}(D_m(a)U^m) = \operatorname{gr.deg}(a)\end{aligned}$$

Esto nos lleva a una contradicción, pues $\mathrm{gr.deg}(a_{n-1}) < \mathrm{gr.deg}(a)$. Deducimos entonces,

$$D_m(a) + A_{j-1} = D_m(b) + A_{j-1} \Rightarrow \overline{\phi}(\rho(a)) = \overline{\phi}(\rho(b))$$

Como la definición se extiende por linealidad, tenemos que es un homomorfismo de k-módulos. Debemos probar que es un homomorfismo de anillo. Consideremos $a, b \in A$, entonces

$$\overline{\phi}(\rho(a))\overline{\phi}(\rho(b)) = \left(\sum_{i\in S(a)} \rho(D_i(a))U^i\right)\left(\sum_{j\in S(b)} \rho(D_j(b))U^j\right) =$$

$$= \sum_{n\geq 0} \sum_{\substack{i+j=n \\ i\in S(a), j\in S(b)}} \rho(D_i(a)D_j(b))U^n \overset{*}{=} \sum_{n\geq 0} \rho\left(\sum_{\substack{i+j=n \\ i\in S(a), j\in S(b)}} D_i(a)D_j(b)\right) U^n = \sum_{\substack{i+j\geq 0 \\ i\in S(a), j\in S(b)}} \rho(D_{i+j}(ab))U^{i+j}$$

donde en $*$, debemos notar que para todo par $(i,j) \in S(a) \times S(b)$, con $i + j = n$, los productos $D_i(a)D_j(b)$ pertencen a la misma componente homogénea $A_{m-\mathrm{gr.deg}(U^n)} \setminus A_{m-\mathrm{gr.deg}(U^n)-1}$ con $m = \mathrm{gr.deg}(a) + \mathrm{gr.deg}(b)$. Esto se tiene ya que para todo par $(i,j) \in S(a) \times S(b)$,

$$\mathrm{gr.deg}(D_i(a)D_j(b)U^n) = \mathrm{gr.deg}(a) + \mathrm{gr.deg}(b) \Rightarrow \mathrm{gr.deg}(D_i(a)D_j(b)) = \mathrm{gr.deg}(a) + \mathrm{gr.deg}(b) - \mathrm{gr.deg}(U^n)$$

Por otro lado,

$$\overline{\phi}(\rho(ab)) = \sum_{n\in S(ab)} \rho(D_n(ab))U^n$$

Luego, debemos ver que $n \in S(ab)$ si y sólo si existe un par (i,j) tal que $n = i + j$, $i \in S(a)$ y $j \in S(b)$.

$\Leftarrow$ Sean $i \in S(a)$ y $j \in S(b)$, por definición

$$\mathrm{gr.deg}\left(D_i(a)U^i\right) = \mathrm{gr.deg}(a) \quad \text{y} \quad \mathrm{gr.deg}\left(D_j(b)U^j\right) = \mathrm{gr.deg}(b)$$

Sumando estas dos igualdades obtenemos

$$\mathrm{gr.deg}\left(D_i(a)D_j(b)U^{i+j}\right) = \mathrm{gr.deg}(ab)$$

Denotando por $n = i + j$, se tiene además que,

$$\mathrm{gr.deg}(D_i(a)D_j(b)U^n) \leq \mathrm{gr.deg}\left(\sum_{i+j=n} D_i(a)D_j(b)U^n\right) = \mathrm{gr.deg}\left(D_n(ab)U^n\right)$$

Entonces

$$\mathrm{gr.deg}(ab) \leq \mathrm{gr.deg}\left(D_n(ab)U^n\right)$$

Por (1.2), tenemos la igualdad y por tanto $n \in S(a)$.

$\Rightarrow$ Sea $n \in \mathbb{N}$ y supongamos que para cada par (i,j) que cumple que $n = i + j$, $i \notin S(a)$. Entonces

$$\begin{aligned} \mathrm{gr.deg}(D_n(ab)U^n) &= \mathrm{gr.deg}\left(\sum_{i+j=n} D_i(a)D_j(b)U^n\right) \leq \max_{(i,j)}\left\{\mathrm{gr.deg}\left(D_i(a)D_j(b)U^n\right)\right\} \\ &= \max_{(i,j)}\left\{\mathrm{gr.deg}\left(D_i(a)U^i\right) + \mathrm{gr.deg}\left(D_j(b)U^j\right)\right\} < \mathrm{gr.deg}(a) + \mathrm{gr.deg}(b) = \mathrm{gr.deg}(ab) \end{aligned}$$

y por tanto $n \notin S(ab)$. Análogamente si consideramos j en lugar de i.

A continuación probaremos que cumple las propiedades de una aplicación exponencial.

1. Como $0 \in S(a)$,

$$\overline{\phi}(a) = \rho(D_0(a)) + U \sum_{n\in S(a)\setminus 0} \rho(D_n(a))U^{n-1} \equiv \rho(D_0(a)) = \rho(a) \mod U$$

2. Por un lado,

$$\overline{\phi}_V\overline{\phi}_U(\rho(a)) = \overline{\phi}_V\left(\sum_{n\in S(a)}\rho(D_n(a))U^n\right) = \sum_{n\in S(a)}\sum_{m\in S(D_n(a))}\rho(D_mD_n(a))V^mU^n$$

Por otro lado, usando (1.1)

$$\overline{\phi}_{U+V}(\rho(a)) = \sum_{n\in S(a)}\rho(D_n(a))(U+V)^n = \sum_{m+n\in S(a)}\binom{m+n}{m}\rho(D_{m+n}(a))V^mU^n = \sum_{m+n\in S(a)}\rho(D_mD_n(a))V^mU^n$$

Para que $\overline{\phi}_V\overline{\phi}_U(a) = \overline{\phi}_{U+V}(a)$ tenemos que ver que $n+m\in S(a)$ si y sólo si $n\in S(a)$ y $m\in S(D_n(a))$.
$\Leftarrow$ Suponemos que $n\in S(a)$ y $m\in S(D_n(a))$, entonces

$$\begin{aligned} \mathrm{gr.deg}\,(D_n(a)U^n) = \mathrm{gr.deg}(a) \quad &\to \quad \mathrm{gr.deg}(D_n(a)) + n\cdot\mathrm{gr.deg}(U) = \mathrm{gr.deg}(a) \\ \mathrm{gr.deg}(D_m(D_n(a))U^m) = \mathrm{gr.deg}(D_n(a)) \quad &\to \quad \mathrm{gr.deg}(D_m(D_n(a))) + m\cdot\mathrm{gr.deg}(U) = \mathrm{gr.deg}(D_n(a)) \end{aligned}$$

Sustituyendo la expresión de $\mathrm{gr.deg}(D_n(a))$,

$$\mathrm{gr.deg}(a) = (n+m)\,\mathrm{gr.deg}(U) + \mathrm{gr.deg}(D_m(D_n(a)))$$

En particular, $\binom{n+m}{n}D_{n+m} = D_m(D_n(a)) \neq 0$ por tanto,

$$(n+m)\,\mathrm{gr.deg}(U) + \mathrm{gr.deg}(D_{n+m}(a)) = \mathrm{gr.deg}(a)$$

y por tanto $m+n\in S(a)$.
$\Rightarrow$ Supongamos que $n\notin S(a)$, entonces

$$n\,\mathrm{gr.deg}(U) + \mathrm{gr.deg}(D_n(a)) < \mathrm{gr.deg}(a)$$

o bien, supongamos que $m\notin S(D_n(a))$, entonces

$$m\,\mathrm{gr.deg}(U) + \mathrm{gr.deg}(D_mD_n(a)) < \mathrm{gr.deg}(D_n(a))$$

En los dos casos tenemos

$$(n+m)\,\mathrm{gr.deg}(U) + \mathrm{gr.deg}(D_{m+n}) < \mathrm{gr.deg}(a)$$

Con esto concluimos que esta aplicación cumple la segunda propiedad de las aplicaciones exponenciales y por tanto, efectivamente es una aplicación exponencial.

Esta aplicación es no trivial, para ello basta considerar $a_j\in\Gamma$ y $n\in\mathbb{Z}_+$ tales que dan el mínimo del conjunto C, es decir, aquellos que definen el número racional $\mathrm{gr.deg}(U)$ y observar que $D_n(a_j)\neq 0$ es un elemento tal que

$$\mathrm{gr.deg}(D_n(a_j)U^n) = \mathrm{gr.deg}(a_j)$$

Luego $n\in S(a_j)$ y por tanto $\overline{\phi}(\rho(a_j)) \neq \rho(a_j)$.

Para finalizar con esta demostración, probaremos que $\rho(A^\phi)\subseteq gr(A)^{\overline{\phi}}$.

Sea $\rho(a)\in\rho(A^\phi)$ para un $a\in A_n\setminus A_{n-1}$. Como $a\in A^\phi$, se tiene que $\phi(a)=a$, luego $D_n(a)=0$ para todo $n\geq 1$. Calculemos $\overline{\phi}(\rho(a))$.

$$\overline{\phi}(\rho(a)) = \sum_{n\in S(a)}\rho(D_n(a))U^n = \rho(D_0(a)) = \rho(a)$$

Por tanto $\rho(a)\in gr(A)^{\overline{\phi}}$.

□

Capítulo 2

Problema de la Cancelación

El problema de la cancelación nos plantea la siguiente cuestión: Si A es una k-álgebra afín tal que $A^{[1]}$ es isomorfo al anillo de polinomios $k^{[n+1]}$, ¿Implica esto que A es isomorfo a $k^{[n]}$?

El objetivo de este trabajo es estudiar y explicar un contraejemplo para esta conjetura con k un cuerpo infinito de característica positiva y $n = 3$ (2.14). Este contraejemplo ha sido realizado por Neena Gupta y publicado en el artículo [Gu] en 2013. Al igual que en este artículo, comenzaremos la sección presentando algunos lemas y proposiciones previas.

Definición 2.1 *Sea L un cuerpo cuya clausura algebraica denotaremos por $\overline{L}$. Una L-álgebra D es* **geométricamente íntegra** *si $D \otimes_L \overline{L}$ es un dominio de integridad.*

Lema 2.2 *Si D es una L-álgebra geométricamente íntegra entonces D es un dominio de integridad.*

Demostración.

Como L es un cuerpo, todo L-módulo es plano (de hecho es libre, pues es un espacio vectorial). Si consideramos $L \hookrightarrow \overline{L}$ y tensorizamos, obtenemos que

$$D = D \otimes_L L \hookrightarrow D \otimes_L \overline{L}$$

Podemos deducir por tanto que D es un dominio de integridad, ya que es un submódulo de $D \otimes_L \overline{L}$, el cual hemos supuesto dominio de integridad.

$\square$

Lema 2.3 *Si D es una L-álgebra geométricamente íntegra entonces L es algebraicamente cerrado en D.*

Demostración.

Sea $x \in D$ un elemento que sea algebraico sobre L y consideremos el homomorfismo de evaluación en x:

$$\begin{array}{cccc} E: & L[T] & \longrightarrow & D \\ & g(T) & \longmapsto & g(x) \end{array}$$

Como D es un dominio por el lema anterior, 2.2, el núcleo de E debe ser un ideal primo, al ser éste el ideal contraido mediante E del ideal cero de D, que es primo. Además, también debe ser no nulo pues x es algebraico, luego existe $g(T) \neq 0$ tal que $g(x) = 0$ y por tanto $g(T) \in \ker E$. Como $L[T]$ es un D.I.P., $\ker E$ estará generado por un único elemento, $f(T)$ de grado $d \geq 1$, que será irreducible para que este ideal sea primo. Este elemento $f(T)$ es el polinomio mínimo de x sobre L.

Gracias al primer teorema de isomorfía y al homomorfismo de evaluación podemos deducir que el anillo cociente $R = L(T)/\langle f(T) \rangle$ es un subanillo de D, que de hecho es un cuerpo.

De nuevo por la planitud, tendremos que

$$R \otimes_L \overline{L} \hookrightarrow D \otimes_L \overline{L}$$

y por tanto $R \otimes_L \overline{L}$ debe ser un dominio, pero

$$R \otimes_L \overline{L} = L[T]/\langle f(T) \rangle \otimes_L \overline{L} = \overline{L}[T]/\langle f(T) \rangle$$

Para que este anillo sea un dominio hace falta que $f(T)$ sea irreducible en $\overline{L}[T]$, pero $\overline{L}$ es algebraicamente cerrado y por tanto $f(T)$ ha de tener grado 1, lo que implica que $x \in L$.

□

Lema 2.4 *Sea L un cuerpo y D una L-álgebra geométricamente íntegra tal que* $\operatorname{tr.deg}_L(D) = 1$*. Si D admite una aplicación exponencial no trivial entonces $D = L^{[1]}$.*

Demostración.
Por el lema 2.2, si D es geométricamente íntegra, podemos concluir que D es un dominio de integridad. Además, como $\operatorname{tr.deg}_L(D) = 1$, por el lema 1.2.8 b. $D = \tilde{L}^{[1]}$ donde $\tilde{L}$ es la clausura algebraica de L en D. Por otra parte, L es algebraicamente cerrado en D (2.3) y por tanto $L = \tilde{L}$. De esto se deduce que $D = L^{[1]}$.

□

Lema 2.5 *Sea L un cuerpo de característica $p > 0$ y Z, T dos indeterminadas sobre L. Sea $g = Z^{p^e} - \alpha T^m + \beta$ donde $0 \neq \alpha$, $0 \neq \beta \in L$, $e \geq 1$ y $m > 1$ son enteros tales que m es coprimo con p. Entonces $D = L[Z, T]/\langle g \rangle$ no admite ninguna aplicación exponencial no trivial.*

Demostración.
Probaremos primero que D es una L-álgebra geométricamente íntegra por lo que debemos considerar $\overline{L}$ la clausura algebraica de L.

Como m es coprimo con p, el polinomio $\alpha T^m - \beta$ tiene una derivada distinta de cero, $m\alpha T^{m-1}$, cuyo máximo común divisor con ésta es uno. Luego $\alpha T^m - \beta$ es libre de cuadrado en $\overline{L}$. Por el criterio de Einstein, g es un polinomio irreducible en $\overline{L}[T][Z]$ (basta tomar cualquier polinomio irreducible de $\alpha T^m - \beta$ para aplicar este criterio). Por tanto $D \otimes_L \overline{L} \cong \overline{L}[Z, T]/\langle g \rangle$ es un dominio de integridad, luego D es geométricamente íntegra. Observar que como g también es irreducible en $L[Z, T]$, tenemos que $\operatorname{tr.deg}_L(D) = 1$.

Consideremos λ una raíz de $Z^{p^e} + \beta \in \overline{L}[Z]$. Observar que entonces $\lambda^{p^e} = -\beta$ y que

$$(Z - \lambda)^{p^e} = Z^{p^e} + (-\lambda^{p^e}) = Z^{p^e} - \lambda^{p^e} = Z^{p^e} + \beta$$

Sea $M = (T, Z - \lambda)\overline{L}[Z, T]$. Este ideal es maximal, pues $\overline{L}$ es algebraicamente cerrado, de hecho M es el ideal maximal correspondiente al punto $(0, \lambda)$. Además, $g \in M^2$ pues, teniendo en cuenta que $m, p^e > 1$, podemos escribir g de la siguiente forma

$$g = -\alpha T^m + (Z - \lambda)^{p^e} = -\alpha T^{m-2}T^2 + (Z - \lambda)^{p^e - 2}(Z - \lambda)^2 \in M^2$$

Es decir, $(0, \lambda)$ es un punto singular de la curva $V(g)$ y por tanto, el anillo local de la curva en p no es un anillo local regular.

Como $D \otimes_L \overline{L}$ es un dominio noetheriano de dimensión 1 y existe un localizado de éste en un ideal maximal que no es un anillo local regular, podemos deducir que $D \otimes_L \overline{L}$ no es un dominio normal, en particular $D \ncong L^{[1]}$, ya que $L^{[1]}$ si es un dominio normal gracias a que es un D.F.U.

En resumen, hemos probado que D es una L-álgebra geométricamente íntegra con grado de trascendencia sobre L igual a uno y que $D \ncong L^{[1]}$. Por el lema 2.4, podemos concluir que D no admite ninguna aplicación exponencial no trivial.

□

Lema 2.6 *Sea B un dominio afín sobre un cuerpo infinito k. Sea $f \in B$ tal que $f - \lambda$ es un elemento primo de B para infinitos $\lambda \in k$. Supongamos que existe $\phi : B \to B[U]$ una aplicación exponencial no trivial en B tal que $f \in B^\phi$. Entonces existe $\beta \in k$ tal que $f - \beta$ es un elemento primo de B y ϕ induce una aplicación exponencial no trivial en $B/\langle f - \beta \rangle$.*

Demostración.

Sea $x \in B \setminus B^{\phi}$. Aplicando ϕ obtenemos que $\phi(x) = x + D_1(x)U + \cdots + D_n(x)U^n$ para algún $n \geq 1$ donde $D_i(x) \in B$ y $D_n(x) \neq 0$. Como B es afín y k es infinito, afirmamos que existe $\beta \in k$ tal que $f - \beta$ es un elemento primo de B y $D_n(x) \notin (f - \beta)B$.

Supongamos que $D_n(x) \in \langle f - \beta \rangle$ para infinitos ideales primos de B con $\beta \in k$. Entonces $\langle D_n(x) \rangle \subsetneq \langle f - \beta \rangle$ para infinitos ideales primos. Como B es dominio, el cero es un ideal primo y por tanto $\langle f - \beta \rangle$ es un ideal primo de altura 1. Tenemos entonces

$$0 \subsetneq \langle D_n(x) \rangle \subsetneq \langle f - \beta \rangle$$

Luego $\langle D_n(x) \rangle$ no puede ser un ideal primo. Gracias a estas contenciones y a que la altura de los ideales generados por $f - \beta$ es uno, se tiene que éstos deben ser los primos minimales de $\langle D_n(x) \rangle$, es decir, tiene infinitos ideales primos minimales. Pero B es noetheriano y por tanto existen un número finito de ideales minimales que contienen a $\langle D_n(x) \rangle$. Esto lleva a una contradicción y a concluir que la afirmación es cierta.

Denotemos por $\overline{a}$ la imagen de a en $B/\langle f - \beta \rangle$, donde $D_n(x) \notin \langle f - \beta \rangle$ y definimos

$$\begin{array}{rccc} \phi_1 : & B/\langle f - \beta \rangle & \longrightarrow & (B/\langle f - \beta \rangle)[U] \\ & \overline{a} & \longmapsto & \sum_{n \geq 0} \overline{D_n(a)} U^n \end{array}$$

Para ver que está bien definida, basta ver que $\phi_1(f - \beta) = 0$, pero esto se tiene gracias a que $\phi(f - \beta) = \phi(f) - \phi(\beta) = f - \beta$. Debido a que las aplicaciones D_n son k-lineales y que verifican la regla de Leibniz, se tiene que ϕ_1 es un homomorfismo de k-álgebras.

Además,

$$\phi_1(\overline{a}) = \overline{D_0(a)} + U \sum_{n \geq 1} \overline{D_n(a)} U^{n-1} \equiv \overline{D_0(a)} \equiv \overline{a} \mod U$$

Por otra parte,

$$\phi_{1_{U+V}}(\overline{a}) = \sum_{m \geq 0} \overline{D_m(a)}(U+V)^m = \sum_{m \geq 0, n \geq 0} \binom{m+n}{n} \overline{D_{m+n}(a)} U^m V^n = \sum_{m \geq 0, n \geq 0} \overline{D_n D_m(a)} U^m V^n = \phi_{1_V} \phi_{1_U}(\overline{a})$$

Luego, ϕ_1 es una aplicación exponencial de $B/\langle f - \beta \rangle$. Esta aplicación es no trivial gracias a que $D_n(x) \neq 0$ no pertence al ideal generado por $f - \beta$, luego $\overline{D_n(x)} \neq 0$ en $\phi_1(\overline{x})$.

□

Nota 2.7 *Observar que para demostrar la existencia de la aplicación exponencial no trivial en el lema 2.6, sólo nos hace falta encontrar un elemento $\beta \in k$ tal que $\langle f - \beta \rangle$ sea un ideal primo y que exista $x \in B \setminus B^{\phi}$ que cumpla que el coeficiente líder de $\phi(x)$, no pertenezca al ideal $\langle f - \beta \rangle$.*

Lema 2.8 *a. Sea $B = k[X, Y, Z, T]/\langle X^m Y - g \rangle$ donde $m > 1$ y $g \in k[Z, T]$. Sea f un elemento primo de $k[Z, T]$ tal que $g \notin fk[Z, T]$ y sea $D = B/fB$. Entonces D es un dominio de integridad.*

b. Supongamos que existe un ideal maximal M de $k[Z, T]$ tal que $f \in M$ y $g \in fk[Z, T] + M^2$. Entonces no existe ninguna aplicación exponencial ϕ en D tal que la imagen de Y en D pertenece a D^{ϕ}.

Demostración.

a. Denotemos por $\overline{g}$ a la imagen de g en $C := k[Z, T]/\langle f \rangle$, el cual gracias a que f es primo, es un dominio de integridad. Se tienen lo siguientes isomorfismos

$$C[X, Y]/\langle X^m Y - \overline{g} \rangle \cong k[Z, T, X, Y]/\langle f, X^m Y - g \rangle \cong (k[X, Y, Z, T]/\langle X^m Y - g \rangle)/\langle f + \langle X^m Y - g \rangle \rangle \cong B/fB = D$$

Debido a esto, basta ver que $C[X, Y]/\langle X^m Y - \overline{g} \rangle$ es un dominio de integridad. Es decir, debemos ver que $\mathfrak{p} := \langle X^m Y - \overline{g} \rangle$ es un ideal primo en $C[X, Y]$. Consideremos K el cuerpo de fracciones de C, entonces $K[X, Y]$ es un D.F.U. Por otra parte, como $g \notin fk[Z, T]$, $\overline{g} \neq 0$ y $X^m Y - \overline{g}$ es un polinomio irreducible en $K[X][Y]$ (observar que es de grado 1 en Y) y por tanto $\langle X^m Y - \overline{g} \rangle$ es un ideal primo en $K[X, Y]$.

Consideremos el homomorfismo de anillos $C[X,Y] \hookrightarrow K[X,Y]$, notar que es inyectivo gracias a que C es un dominio de integridad. Vamos a probar que el ideal contraido de $\langle X^mY - \overline{g}\rangle$, el cual sabemos que será primo, es $\mathfrak{p}$, es decir, que

$$\mathfrak{p} = \mathfrak{p}^{ec} = (X^mY - \overline{g})K[X,Y] \cap C[X,Y]$$

Sabemos que $\mathfrak{p} \subseteq \mathfrak{p}^{ec}$, debemos ver la inclusión contraria.

Sea $h(X,Y) \in K[X,Y]$ tal que $h(X,Y)(X^mY - \overline{g}) \in C[X,Y]$. El polinomio $h(X,Y)$ es de la forma

$$h(X,Y) = h_d(X)Y^d + h_{d-1}(X)Y^{d-1} + \cdots + h_0$$

donde $h_i(X) \in K[X]$. Multipliquemos $h(X,Y)$ por el polinomio $X^mY - \overline{g}$,

$$h(X,Y)(X^mY - \overline{g}) = h_d(X)X^mY^{d+1} + (h_{d-1}(X)X^m - \overline{g}h_d(X))\,Y^d + \ldots + (h_0X^m - \overline{g}h_1(X))\,Y - \overline{g}h_0(X)$$

Como $h(X,Y)(X^mY - \overline{g}) \in C[X,Y]$,todos los coeficientes de los monomios Y^i con $i = 0,\ldots,d+1$ en $h(X,Y)$ deben pertenecer a $C[X]$. Luego, $h_d(X)X^m \in C[X]$, y por tanto $h_d(X) \in C[X]$. Consideremos ahora el coeficiente de Y^{d-1}, éste es $h_{d-1}(X)X^m - \overline{g}h_d(X) \in C[X]$, como $\overline{g}h_d(X) \in C[X]$, entonces $h_{d-1}(X) \in C[X]$. Continuando con este razonamiento hasta $h_0(X)$, podemos concluir que $h_i(X) \in C[X]$ y que por tanto $h(X,Y) \in C[X,Y]$.

Teniendo es cuenta que $\mathfrak{p}$ es un ideal primo, podemos deducir que D es un dominio de integridad.

b. Como $g \in fk[Z,T] + M^2$, sea $\alpha \in k[Z,T]$ tal que $g - \alpha f \in M^2$. Llamemos $R = k(Y)[X,Z,T]$. R es una anillo noetheriano regular por ser un anillo de polinomios con coeficientes en un cuerpo. Observar que (M,X) es un ideal maximal en $K[X,T,Z]$, en particular es primo y entonces $\mathfrak{n} = (M,X)K[X,Y,Z,T]$ es un ideal primo en $k[X,Y,Z,T]$. Además, ya que $(M,X)k[X,Z,T]$ es un ideal de altura tres, $\mathrm{ht}(\mathfrak{n}) \geq 3$, y gracias a que $\mathfrak{n}$ no corta a $k[Y] \setminus 0$, $\mathrm{ht}((M,X)R) \geq \mathrm{ht}(\mathfrak{n}) \geq 3$. Como $\dim(R) = 3$, $(M,X)R$ es un ideal maximal. Llamemosle $\mathfrak{m} := (M,X)R$. Como $m > 1$ y $g - \alpha f \in M^2$, tenemos que $h := X^mY - g + \alpha f \in \mathfrak{m}^2$

Consideremos la sucesión exacta corta

$$\langle X^mY - g, f\rangle \overset{i}{\hookrightarrow} k[X,Y,Z,T] \twoheadrightarrow D\,(\cong k[X,Y,Z,T]/\langle X^mY - g, f\rangle)$$

tensorizando por $- \otimes_{k[Y]} k(Y)$, se tiene la sucesión exacta

$$\langle X^mY - g, f\rangle \otimes_{k[Y]} k(Y) \xrightarrow{i\otimes 1} k[X,Y,Z,T] \otimes_{k[Y]} k(Y) \twoheadrightarrow D \otimes_{k[Y]} k(Y)$$

Por tanto, teniendo en cuenta que $Im(i \otimes 1) = \langle X^mY - g, f\rangle \otimes_{k[Y]} k(Y)$

$$\big(k[X,Y,Z,T] \otimes_{k[Y]} k(Y)\big) \,/\, \big(\langle X^mY - g, f\rangle \otimes_{k[Y]} k(Y)\big) \cong D \otimes_{k[Y]} k(Y)$$

Por otra parte, $k[X,Y,Z,T] \otimes_{k[Y]} k(Y) \cong R$ y el extendido de $\langle X^mY - g, f\rangle \otimes_{k[Y]} k(Y)$ bajo este isomorfismo es $\langle X^mY - g, f\rangle$ en R. Luego, el isomorfismo anterior queda

$$D \otimes_{k[Y]} k(Y) \cong R/\langle X^mY - g, f\rangle$$

Además, observar que $\langle h, f\rangle = \langle X^mY - g, f\rangle$ y que por tanto

$$D \otimes_{k[Y]} k(Y) \cong R/\langle h, f\rangle$$

Vamos a probar que $S := D \otimes_{k[Y]} k(Y)$ no es un dominio normal.

Primero vamos a calcular la altura del ideal primo $\langle h, f\rangle$ en R. Como R es noetheriano, $\mathrm{ht}(\langle h, f\rangle) \leq 2$. Por otro lado, $(f)R$ es un ideal primo contenido en $\langle h, f\rangle$. Además, R es un dominio de integridad y tenemos la cadena de ideales primos siguiente

$$\langle 0\rangle \subset \langle f\rangle \subset \langle h, f\rangle$$

Luego $\mathrm{ht}(\langle h, f\rangle) \geq 2$ y por tanto, exactamente igual a dos. Podemos observar entonces que S es un dominio de integridad de dimensión de Krull uno, pues $\dim S = \dim R = 3 - \mathrm{ht}(\langle h, f\rangle)$. Denotemos por $\overline{\mathfrak{m}}$ al ideal maximal de S extendido de $\mathfrak{m}$.

El anillo local $S_{\overline{\mathfrak{m}}}$ es noetheriano de dimensión uno, la noetherianidad se tiene gracias a que el localizado de un anillo noetheriano. Para la dimensión, tener en cuenta que $ht(\overline{\mathfrak{m}}) \geq 1$, pues S es dominio y que $\dim S = \sup\{\dim S_{\mathfrak{n}} | \mathfrak{n}$ ideal maximal de $S\} = 1$. Entonces $1 \leq ht(\overline{\mathfrak{m}}) = \dim S_{\overline{\mathfrak{m}}} \leq 1$. Sabemos por tanto que $S_{\overline{\mathfrak{m}}}$ es normal si y sólo si $S_{\overline{\mathfrak{m}}}$ es regular.

Para probar que S no es normal, basta probar que $S_{\overline{\mathfrak{m}}}$ no es normal y por lo anterior que $S_{\overline{\mathfrak{m}}}$ no es regular.

Ahora bien,

$$S_{\overline{\mathfrak{m}}} \cong R_{\mathfrak{m}}/\langle h, f\rangle$$

donde $R_{\mathfrak{m}}$ es un anillo noetheriano local regular, pues R es regular. Además, la dimensión de este anillo es tres ya que $\mathrm{ht}(\mathfrak{m}) = 3$.

Supongamos que $R_{\overline{\mathfrak{m}}}/\langle h, f\rangle$ fuera regular, entonces gracias al teorema 36, 4 de [Ma], podríamos ampliar $\{h, f\}$ a un sistema minimal de tres generadores del ideal maximal, pero por el lema de Nakayama esto no es posible pues $h \in \mathfrak{m}^2$ (un sistema minimal de generadores, si reducimos módulo $\mathfrak{m}^2$ debe darnos una base sobre el cuerpo residual, pero $h \mod \mathfrak{m}^2 = 0$).

Podemos deducir que $D \otimes_{k[Y]} k(Y)$ no es un dominio normal. En particular, $D \otimes_{k[Y]} k(Y)$ no es una anillo de polinomios sobre un cuerpo.

Supongamos que existe $\phi : D \to D[U]$ una aplicación exponencial no trivial, con $Y \in D^{\phi}$. Entonces, deducimos que $k[Y] \subseteq D^{\phi}$. Tomamos el subconjunto multiplicativamente cerrado $T = k[Y] \setminus \{0\}$. Luego $T^{-1}D = D \otimes_{k[Y]} k(Y) =: S$. Por el lema 1.2.9 existe una aplicación no trivial $T^{-1}\phi : S \to S[U]$.

Como S es un dominio afín sobre $k(Y)$, $\mathrm{tr.deg}_{k(Y)} S = \dim S = 1$. Por el lema 1.2.8, tenemos que $S = \widetilde{k(Y)}^{[1]}$, donde $\widetilde{k(Y)}$ es la clausura algebraica de $k(Y)$ sobre S, en particular S es un anillo de polinomios sobre un cuerpo, lo cual es una contradicción. Luego no existe ninguna aplicación exponencial en D tal que $Y \in D^{\phi}$

□

Lema 2.9 *Sea k un cuerpo infinito de característica positiva p. Sea*

$$B = k[X, Y, Z, T] \Big/ \left\langle X^m Y + T^s + Z^{p^e} \right\rangle$$

donde m, e, s son enteros positivos tales que $s = p^r q$, $p \nmid q$, $q > 1$, $e > r \geq 1$ y $m > 1$. Denotemos por x, y, z, t a las imagenes de X, Y, Z, T en B. Entonces no existe ninguna aplicación exponencial ϕ en B tal que $y \in B^{\phi}$.

Demostración.

Nos reduciremos al caso en el que k es un cuerpo algebraicamente cerrado. Esto se debe a la siguiente razón.

Supongamos que k no es algebraicamente cerrado y consideremos $\overline{k}$ su clausura algebraica que será un cuerpo infinito de característica p. Denotemos por $\overline{B} := B \otimes_k \overline{k} \cong \overline{k}[X, Y, Z, T] \Big/ \left\langle X^m Y + T^s + Z^{p^e} \right\rangle$. Como el polinomio $X^m Y + T^s + Z^{p^e}$ es irreducible en $\overline{k}[X, Y, Z, T]$, B es geométricamente íntegra y $\overline{B}$ es un dominio afín.

Supongamos que hemos demostrado el resultado para $\overline{k}$ y $\overline{B}$ y además que existe una aplicación exponencial no trivial en B, a la que denotaremos ϕ, tal que $y \in B^{\phi}$. Entonces, podemos definir una aplicación exponencial no trivial en $\overline{B}$ como sigue:

$$\begin{array}{cccc} \overline{\phi}: & \overline{B} & \longrightarrow & \overline{B}[U] \\ & f(\overline{x}, \overline{y}, \overline{z}, \overline{t}) & \longmapsto & f\left(\overline{\phi(x)}, \overline{\phi(y)}, \overline{\phi(z)}, \overline{\phi(t)}\right) \end{array}$$

donde $\overline{x}, \overline{y}, \overline{z}$ y $\overline{t}$ son las clases en $\overline{B}$ de X, Y, Z y T, que cumple que $\overline{y} \in \overline{B}^{\overline{\phi}}$ con lo que llegaríamos a una contradicción. Asumimos, por tanto que k es algebraicamente cerrado.

Como $X^mY+T^s+Z^{p^e}$ es un polinomio irreducible en $k[X,Y,Z,T]$, B es un dominio. Además, todo elemento de B puede ser escrito como un polinomio en x,y,z,t con coeficientes en k. Luego B es un dominio afín.

Observar que B tiene una estructura de $\mathbb{Z}$-álgebra graduada sobre k con los siguientes pesos de los generadores:

$$wt(x)=-1,\quad wt(y)=m,\quad wt(z)=0,\quad wt(t)=0$$

Esto se debe a que el polinomio $x^my+t^s+z^{p^e}$ es homogéneo con estos pesos. Gracias al lema 1.4.5, esta graduación define un $\mathbb{Z}$-filtración propia de B tal que $gr(B)$ es isomorfo a B. Además, como B es un dominio afín, es decir, un dominio de generación finita como k-álgebra, también podemos concluir por el mismo lema que la $\mathbb{Z}$-filtración propia es admisible con $\Gamma=\{x,y,z,t\}$.

Tenemos que B es un dominio afín sobre k con una $\mathbb{Z}$-filtración propia admisible. Además, gracias a que k es algebraicamente cerrado de característica positiva, por el ejemplo 1.3.11 sabemos que existe al menos una aplicación exponencial no trivial, sea ϕ una de ellas. Podemos entonces aplicar el teorema 1.4.6 y deducir que ϕ induce una aplicación exponencial no trivial $\widehat{\phi}$ en $B(\cong gr(B))$. Además, $\rho(B^{\phi})\subseteq gr(B)^{\widehat{\phi}}$. Es decir, si $g\in B^{\phi}$, entonces $\rho(g)\in gr(B)^{\widehat{\phi}}$. Aplicando el isomorfismo entre $gr(B)$ y B, tenemos que $\widehat{g}\in B^{\widehat{\phi}}$, donde $\widehat{g}$ es la componente homogénea de mayor grado de $g\in B$.

Consideremos $g\in B$. Debido a que B es de generación finita como k-álgebra, podemos ver g como

$$g=\sum_{i,j\geq 0} g_{ij}(z,t)x^iy^j=\sum_{n\geq 0} g_n(z,t)x^n+\sum_{j>0,i\geq 0} g_{ij}(z,t)x^iy^j$$

En B, los elementos x,y,z,t cumplen la relación $x^my=-(z^{p^e}+t^s)$. Por esta razón, todo término de la forma $g_{ij}(z,t)x^iy^j$ con $i\geq m$ y $j>0$, puede ser sustituido por $g'_{ij}(z,t)x^iy^j$ donde o bien $j=0$ e $i\in\mathbb{Z}_+$ o bien $j>0$ e $i<m$. Luego g se puede escribir de manera única como

$$g=\sum_{n\geq 0} g_n(z,t)x^n+\sum_{\substack{j>0\\ 0\leq i<m}} g_{ij}(z,t)x^iy^j \tag{2.1}$$

donde $g_n(z,t),g_{ij}(z,t)\in k[z,t]$.

Vamos a describir los elementos homogéneos de este anillo graduado, es decir, aquellos elementos en los que todos sus términos pertenecen a la misma componente homogénea o equivalentemente, tienen el mismo grado con los pesos definidos anteriormente.

Consideremos los términos del primer sumatorio de (2.1), es decir, aquellos de forma $g_n(z,t)x^n$ con $n\geq 0$. Gracias a esto último y debido a que $wt(x)=-1$, el grado de estos términos es siempre menor o igual que cero.

Por otro lado, si consideramos los términos del segundo sumatorio de (2.1), es decir, los términos $g_{ij}(z,t)x^iy^j$, con $0\leq i<m$ y $j>0$, éstos tienen grado $-i+mj$. Como $0\leq i<m$ y $j>0$, el grado de estos términos es siempre positivo. Entonces tenemos los siguiente casos:

- Si la componente homogénea es de grado l con $l\leq 0$, entonces esta componente es de la forma $g_{-l}(z,t)x^{-l}$.
- Si la componente homogénea es de grado $l>0$. Entonces debe ser suma de términos de la forma $g_{ij}(z,t)x^iy^j$ con $j>0$ y $0\leq i<m$. Veamos ahora que en realidad sólo está formado por un sumando.

  Supongamos que posee dos términos, $g_{ij}x^iy^j$ y $g_{i'j'}x^{i'}y^{j'}$, entonces $-i+mj=-i'+mj'=l>0$. Como $i\neq i'$, supongamos por ejemplo que $i>i'$, es decir, $mj-l>mj'-l$ y por tanto que $j>j'$. Restando las igualdades $-i'+mj'=l$ y $-i+mj=l$, llegamos a que $i-i'=m(j-j')\geq m$ y por tanto $i\geq i'+m$, lo cual es una contradicción pues $i<m$.

  Luego, los elementos homogéneos de grado positivo son $g_{ij}(z,t)x^iy^j$ con $0\leq i<m$ y $j>0$.

En resumen, cada elemento homogéneo de B es de la forma $x^iy^jg_1(z,t)$, donde $g_1(z,t)\in k[z,t]$.

Probaremos el resultado del lema por reducción al absurdo. Suponemos que $y\in B^{\phi}$ con ϕ aplicación exponencial no trivial en B. Entonces $y(=\widehat{y})\in B^{\widehat{\phi}}$. Vamos a probar que existe un polinomio $h(z,t)\in k[z,t]\setminus k$ tal que $h(z,t)\in B^{\widehat{\phi}}$.

Se tiene que $\operatorname{tr.deg}_k(B) = 3$. Por 1.2.8 a., entonces $\operatorname{tr.deg}_k(B^{\phi}) = 2$. Además, como $y \in B^{\phi}$, el anillo de polinomios $k[y]$ está contenido en B^{ϕ}. Afirmamos que existe $g \in B^{\phi}$ tal que $\widehat{g} \notin k[y]$.

Supongamos que para todo $g \in B^{\phi}$, $\widehat{g} \in k[y]$. Como B^{ϕ} es un anillo y $\widehat{g} \in k[y] \subseteq B^{\phi}$, se tiene que $g-\widehat{g} \in B^{\phi}$ y por hipótesis, $\widehat{g-\widehat{g}} \in k[y]$. Como $g \in B$, éste está formado por un número finito de sumandos, y realizando este proceso tantas veces como sumandos tiene g, obtenemos que $g \in k[y]$. Con esto hemos probado que $B^{\phi} = k[y]$, pero entonces $\operatorname{tr.deg}_k\left(B^{\phi}\right) = 1$ lo que nos lleva a una contradicción. En conclusión, existe $g \in B^{\phi}$ tal que $\widehat{g} \notin k[y]$.

Consideremos entonces un elemento de esta forma, es decir, $g \in B^{\phi}$, tal que $\widehat{g} \notin k[y]$. Como $\widehat{g}$ es homogéneo, tenemos que $\widehat{g} = g_1(z,t)x^iy^j$ para algún $g_1(z,t) \in k[z,t]$. Además, ya que $\widehat{g} \notin k[y]$, se deduce que $g_1(z,t) \notin k^*$ o bien $x \mid \widehat{g}$. Si $g_1(z,t) \notin k^*$, entonces definimos $h(z,t) := g_1(z,t)$ y en caso contrario, $h(z,t) := z^{p^e} + t^s = -x^my$.

Como $\widehat{g} \in B^{\widehat{\phi}}$, por observaciones realizadas anteriormente, y gracias al lema 1.2.6 a., donde probamos que $B^{\widehat{\phi}}$ es factorialmente cerrado, tenemos que $g_1(z,t)$ e y pertenecen a $B^{\widehat{\phi}}$ y si $i > 0$, entonces también $x \in B^{\widehat{\phi}}$ y por tanto $x^my \in B^{\widehat{\phi}}$. En cualquier caso, $h(z,t) \in B^{\widehat{\phi}}$ y entonces se tiene que $k[y, h(z,t)] \subseteq B^{\widehat{\phi}}$ para algún $h(z,t) \in k[z,t] \setminus k$, que es lo que queríamos encontrar.

Consideremos los siguientes pesos para los generadores:

$$wt(x) = 0, \quad wt(y) = qp^e, \quad wt(z) = q, \quad wt(t) = p^{e-r}$$

El polinomio $x^my + t^s + z^{p^e}$ es homogéneo de grado qp^e y por tanto estos pesos definen otra estructura de $\mathbb{Z}$-álgebra graduada en B.

Análogamente, esta graduación define otra $\mathbb{Z}$-filtración propia admisible en B tal que $gr(B) \cong B$. Para cada $g \in B$, denotamos por $\overline{g}$ a la imagen de g bajo la composición $B \to gr(B) \cong B$. Aplicando de nuevo el teorema 1.4.6, $\widehat{\phi}$ induce una aplicación exponencial $\overline{\phi}$ no trivial en $B(\cong gr(B))$ tal que $k\left[y, \overline{h(z,t)}\right] \subseteq B^{\overline{\phi}}$ puesto que $y, h(z,t) \in B^{\widehat{\phi}}$ y por tanto, $y, \overline{h(z,t)} \in B^{\overline{\phi}}$.

Queremos buscar un elemento primo $\omega \in B$ tal que $\omega - \lambda$ sea un elemento primo en B para casi todo $\lambda \in k$ con el objetivo de aplicar el lema 2.6. Para ello, vamos a factorizar el polinomio $\overline{h(z,t)}$.

Como es homogéneo, todos sus términos tienen el mismo grado, denotemos este grado por d. De esta manera, podemos expresar $\overline{h(z,t)}$ como

$$\overline{h(z,t)} = \sum \theta_{ij} z^i t^j$$

con $\theta_{ij} \in k$ y $qi + p^{e-r}j = d$. Consideremos dos sumando de $\overline{h(z,t)}$, cuyos grados estén dados por $qi + p^{e-r}j = d$ y $qi' + p^{e-r}j' = d$. Buscamos una relación entre i, j e i', j' respectivamente.

Restando las dos igualdades anteriores, obtenemos que

$$q(i-i') + p^{e-r}(j-j') = 0 \to q(i-i') = -p^{e-r}(j-j')$$

Como $q \nmid p^{e-r}$, entonces $q \mid j'-j$. Por otra parte, $p \nmid q$ luego $p^{e-r} \mid i-i'$. Con esto tenemos que $j'-j = lq$ e $i - i' = np^{e-r}$. Pero $nqp^{e-r} = lqp^{e-r}$ y por tanto $n = l$. Tenemos entonces que la relación entre los grados es:

$$i' = i - np^{e-r}, \qquad j' = j + nq$$

Gracias a esto, si $\theta_0 z^{i_0} t^{j_0}$ es el término de $\overline{h(z,t)}$ tal que i_0 es el grado máximo de este polinomio en z, entonces los exponentes de z y t en $\overline{h(z,t)}$ son

$$i = i_0 - np^{e-r}, \qquad j = j_0 + nq \qquad \text{con } n \in \mathbb{N}$$

Teniendo en cuenta esta expresión de los exponentes y desarrollando el sumatorio que define $\overline{h(z,t)}$, obtenemos

$$\overline{h(z,t)} = \theta_0 z^{i_0} t^{j_0} + \theta_1 z^{i_0 - p^{e-r}} t^{j_0+q} + \cdots + \theta_n z^{i_0 - np^{e-r}} t^{j_0+nq}$$

donde $i_0 - np^{e-r}$ es el menor grado de z. Sacando factor común, y denotando $Z_1 = z^{p^{e-r}}$ y $T_1 = t^q$, la igualdad anterior queda

$$\overline{h(z,t)} = \theta_0 t^{j_0} z^{i_0 - np^{e-r}} \left(Z_1^n + \theta_1' Z_1^{n-1} T_1 + \cdots + \theta_n' T_1^n\right)$$

Consideramos $H(Z_1,T_1) = Z_1^n + \theta_1' Z_1^{n-1}T_1 + \cdots + \theta_n' T_1^n$ y sea $U = Z_1/T_1$. Entonces

$$H(UT_1,1) = U^n T_1^n + \theta_1' U^{n-1}T_1^n + \cdots + \theta_n' T_1^n = T_1^n \left(U^n + \theta_1' U^{n-1} + \cdots + \theta_n'\right)$$

Como k es un cuerpo algebraicamente cerrado, podemos factorizar $U^n + \theta_1' U^{n-1} + \cdots + \theta_n'$ en factores irreducibles, resultando:

$$H(UT_1,1) = T_1^n \prod_{l\in\Lambda}(U-\mu_l)$$

con $\mu_l \in k^*$. De manera que si deshacemos el cambio $U = Z_1/T_1$, tenemos que

$$H(Z_1,T_1) = T_1^n \prod_{l\in\Lambda}(Z_1/T_1 - \mu_l) = T_1^{n-1}\prod_{l\in\Lambda}(Z_1 - \mu_l T_1)$$

donde $H(Z_1,T_1)$ sigue siendo producto de factores irreducibles. Concluimos por tanto que

$$H\left(z^{p^{e-r}}, t^q\right) = t^{q(n-1)} \prod_{l\in\Lambda}\left(z^{p^{e-r}} - \mu_l t^q\right)$$

Luego, la factorización de $\overline{h(z,t)}$ en factores irreducibles es la siguiente:

$$\overline{h(z,t)} = \theta_0 t^{j_0+q(n-1)} z^{i_0 - np^{e-r}} \prod_{l\in\Lambda}\left(z^{p^{e-r}} - \mu_l t^q\right)$$

Renombrando por $i := i_0 - np^{e-r}$ y $j := j_0 + q(n-1)$, tenemos que

$$\overline{h(z,t)} = \theta_0 z^i t^j \prod_{l\in\Lambda}\left(z^{p^{e-r}} + \mu_l t^q\right) \tag{2.2}$$

para $\theta_0, \mu_l \in k^*$.

Como $\overline{h(z,t)} \notin k$, existe un factor irreducible ω de $\overline{h(z,t)}$ en $k[z,t]$. Debido a que $k[z,t]$ es un D.F.U., ω es un factor primo de $\overline{h(z,t)}$. Por la igualdad (2.2), podemos asumir que o bien $\omega = z$, ó $\omega = t$ ó $\omega = z^{p^{e-r}} + \mu t^q$ para algún $\mu \in k^*$. Gracias a que $\overline{h(z,t)}$ pertenece a $B^{\overline{\phi}}$, por el lema 1.2.6 a., $\omega \in B^{\overline{\phi}}$ y por tanto $k[y,\omega] \subseteq B^{\overline{\phi}}$.

Primero probaremos que $\omega \neq z^{p^{e-r}} + t^q$. Si $\omega = z^{p^{e-r}} + t^q$, entonces

$$x^m y = -(z^{p^e} + t^s) = -(z^{p^{e-r}} + t^q)^{p^r} = -\omega^{p^r} \in B^{\overline{\phi}}$$

lo que implica que $x \in B^{\overline{\phi}}$ (1.2.6 a).

Sea L el cuerpo de fracciones de $C := k[x,y,\omega] (\hookrightarrow B^{\overline{\phi}})$ y consideramos $S = C \setminus \{0\}$. Por el lema 1.2.9, $\overline{\phi}$ induce una aplicación exponencial no trivial en $S^{-1}B \cong B \otimes_C S^{-1}C = B \otimes_C L \cong L[z,t]$. Consideremos

$$\begin{array}{rccc} \varphi: & L[Z,T] & \twoheadrightarrow & L[z,t] \\ & f(Z,T) & \mapsto & f(z,t) \end{array}$$

Entonces, por el primer teorema de isomorfía, $L[z,t] \cong L[Z,T]/\ker\varphi$. Queremos averigüar que elementos forman el $\ker\varphi$. Así pues, sea $H \in L[Z,T]$ tal que $H(z,t) = 0$. Podemos multiplicar H por el producto de todos los denominadores de los coeficientes, dando lugar a $H' \in k[x,y,\omega][Z,T]$. Además, $H'(z,t) = 0$ si y sólo si $H(z,t) = 0$ en $B = k[x,y,z,t] = k[x,y,\omega,z,t]$. Luego basta conocer a los elementos $H \in B$ tales que $H(z,t) = 0$.

Consideramos por tanto, $H \in k[X,Y,W,Z,T]$, es decir, un polinomio en X,Y,W,Z,T con $\overline{W} = \omega$, tal que $H(x,y,\omega,z,t) = 0$. Dividimos H por el polinomio $Z^{p^{e-r}} + T^q - W$, de manera que

$$H = h(X,Y,W,Z,T)\left(Z^{p^{e-r}} + T^q - W\right) + \widetilde{H}(X,Y,Z,T)$$

tal que

$$h(x,y,\omega,z,t)\left(z^{p^{e-r}} + t^q - \omega\right) + \widetilde{H}(x,y,z,t) = \widetilde{H}(x,y,z,t) = 0 \text{ en } B$$

Luego $\widetilde{H}(X,Y,Z,T) = h'(X,Y,Z,T)\left(X^mY + Z^{p^e} + T^q\right)$. Entonces, en $k[X,Y,W,Z,T]$,

$$H(X,Y,W,Z,T) \in \left\langle Z^{p^{e-r}} + T^q - W, X^mY + T^s + Z^{p^e}\right\rangle$$

Para verlo en $L[Z,T]$, tenemos que sustituir X,Y,W por x,y,ω de manera que

$$H(x,y,\omega,T,Z) \in \left\langle Z^{p^{e-r}} + T^q - \omega, x^my + T^s + Z^{p^e}\right\rangle$$

Recordemos que $x^my = -\omega^{p^r}$ y que $T^s + Z^{p^e} = \left(T^q + Z^{p^{e-r}}\right)^{p^r}$, de lo que podemos deducir que $\left(-\omega + T^q + Z^{p^{e-r}}\right)^{p^r} = x^my + T^s + Z^{p^e}$ y por tanto

$$\left\langle Z^{p^{e-r}} + T^q - \omega, x^my + T^s + Z^{p^e}\right\rangle = \left\langle Z^{p^{e-r}} + T^q - \omega\right\rangle$$

Luego $\ker\varphi$ es $\left\langle Z^{p^{e-r}} + T^q - \omega\right\rangle$ y podemos concluir entonces

$$S^{-1}B = L[z,t] \cong L[Z,T]\Big/\left\langle Z^{p^{e-r}} + T^q - \omega\right\rangle$$

Observar que L es un cuerpo de característica $p > 0$ pues k lo es. Además, Z,T son dos indeterminadas sobre L y tenemos un polinomio $Z^{p^{e-r}} + T^q - \omega$, donde $0 \neq \omega \in L$, con $e - r \geq 1$, $q > 1$ y $p \nmid q$, es decir, son coprimos. Entonces podemos aplicar el lema 2.5, que nos dice que $L[Z,T]/\langle Z^{p^{e-r}} + T^q - \omega\rangle$ no admite ninguna aplicación exponencial no trivial, lo cual es una contradicción. Por tanto, asumimos que o bien $\omega = z$ ó $\omega = t$ ó $\omega = z^{p^{e-r}} + \mu t^q$ para algún $\mu \in k^*$ con $\mu \neq 1$.

Notar que para todo $\lambda \in k^*$, $\omega - \lambda$ es un elemento primo de $k[z,t]$. Basta ver que si $\omega = z$ ó $\omega = t$, entonces $\omega - \lambda$ es irreducible en un D.F.U. y por tanto es un elemento primo. Supongamos ahora que $\omega = z^{p^{e-r}} + \mu t^q - \lambda$. Entonces $\mu t^q - \lambda$ es libre de cuadrado, ya que $m.c.d(\mu q t^{q-1}, \mu t^q - \lambda) = 1$. Por el criterio de Einstein, $z^{p^{e-r}} + \mu t^q - \lambda$ es un elemento irreducible en $k[z,t]$, luego es un elemento primo.

Queremos que estos elementos $\omega - \lambda$ sean primos en B, por lo que aplicaremos el lema 2.8 a. Tenemos que probar que $z^{p^e} + t^{qp^r} \notin (\omega - \lambda)k[z,t]$.

Supongamos que $\omega - \lambda = z - \lambda$. Si $z^{p^e} + t^{qp^r} = f(z,t)(z - \lambda)$ entonces $f(z,t)$ tiene una expresión de la forma

$$f(z,t) = \sum_{i=0}^{p^e-1} \alpha_i z^i + \sum_{\substack{j>0\\ i\geq 0}} \alpha_{ij} z^i t^j$$

Multiplicando por $z - \lambda$ tenemos que

$$z^{p^e} + t^{qp^r} = \sum_{i=0}^{p^e-1} \alpha_i z^{i+1} - \sum_{i=0}^{p^e-1} \lambda\alpha_i z^i + \sum_{\substack{j>0\\ i\geq 0}} \alpha_{ij} z^i t^j (z - \lambda)$$

Veamos los coeficientes de $f(z,0)(z - \lambda)$, los cuales deben ser todos cero expecto el coeficiente del término z^{p^e}, que debe ser uno.

El término independiente es $\alpha_0 = 0$, el de grado uno es $\alpha_0 - \alpha_1\lambda = 0$, como $\lambda \neq 0$, entonces $\alpha_1 = 0$. De manera general, el término de grado k es $(\alpha_{k-1} - \alpha_k\lambda)z^k$. Por inducción, llegamos a que $\alpha_k = 0$ para todo $0 \leq k \leq p^e - 1$. Veamos el coeficiente de z^{p^e}, éste es $1 = \alpha_{p^e-1} = 0$, lo que nos da una contradicción y por tanto $z^{p^e} + t^{qp^r} \notin \langle z - \lambda\rangle$.

Análogamente, se tiene para $\omega = t$. Supongamos por último que $\omega = z^{p^{e-r}} + \mu t^q$ con $\mu \neq 1$ y supongamos además que $z^{p^e} + t^{qp^e} \in \langle \omega - \lambda\rangle$. Como este ideal es primo y $z^{p^e} + t^{qp^r} = (z^{p^{e-r}} + t^q)^{p^r}$, se debe cumplir que $z^{p^{e-r}} + t^q \in \langle \omega - \lambda\rangle$, es decir,

$$z^{p^{e-r}} + t^q = f(z,t)\left(z^{p^{e-r}} + \mu t^q - \lambda\right)$$

como $\lambda \neq 0$ y $\mu \neq 1$, entonces esto no puede ocurrir y por tanto $z^{p^e} + t^{qp^e} \notin \langle \omega - \lambda \rangle$.

En resumen, en cualquiera de los tres casos, $z^{p^e} + t^{qp^e} \notin (\omega - \lambda)k[z,t]$. Gracias a lo cual estamos bajo las hipótesis del lema 2.8 a. y por tanto $B/(\omega - \lambda)B$ es un dominio de integridad, es decir $\langle \omega - \lambda \rangle$ es un elemento primo en B.

Observar que k es un cuerpo infinito, tal que $\omega - \lambda$ es un elemento primo de B para infinitos elementos $\lambda \in k^*$ y que tenemos una aplicación exponencial en B tal que $\omega \in B^{\overline{\phi}}$. Por el lema 2.6, existe un $\beta \in k^*$ tal que $\overline{\phi}$ induce una aplicación exponencial ϕ_1 en $B/\langle \omega - \beta \rangle$ la cual bien definida por:

Dado $[b] \in B/\langle \omega - \beta \rangle$, si denotamos por $\overline{D}_n$ a las aplicaciones que definen $\overline{\phi}$, $\phi_1([b]) = \sum_{n \geq 0} \left[\overline{D}_n(b)\right] U^n$

Notar que $y \in B^{\overline{\phi}}$ y entonces $\phi_1([y]) = [y]$. Por tanto y pertenece al anillo de ϕ_1-invariantes.

Pongamos $f := \omega - \beta$, $g_0 := z^{p^{e-r}} + t^q$ y $g := g_0^{p^r} = z^{p^e} + t^{qp^r}$. Como $\mu \neq 1$, afirmamos que f y g_0 no son comaximales en $k[z,t]$. Supongamos que lo fueran, entonces deberían existir $h_1(z,t), h_2(z,t) \in k[z,t]$ tales que

$$1 = h_1(z,t)\left(z^{p^{e-r}} + t^q\right) + h_2(z,t)\left(z^{p^{e-r}} + \mu t^q - \beta\right)$$

Consideremos $h_3(t) = -t^{q/p^{e-r}} \in k\left[z, t, t^{q/p^{e-r}}\right]$, entonces

$$h_3(t)^{p^{e-r}} + t^q = -t^q + t^q = 0$$

luego si sustituimos $z = h_3(t)$, tenemos que

$$1 = h_1(h_3(t), t)\left(h_3(t)^{p^{e-r}} + t^q\right) + h_2(h_3(t), t)\left(h_3(t)^{p^{e-r}} + \mu t^q - \beta\right) = h_2(h_3(t), t)\left((\mu - 1)t^q - \beta\right)$$

es decir,

$$1 = (\mu - 1)h_2(h_3(t), t)t^q - h_2(h_3(t), t)\beta$$

Ya que $\mu - 1 \neq 0$ y $q > 0$, se tiene que $h_2(h_3(t), t) = 0$, pero entonces $1 = 0$ dando una contradicción. Luego, efectivamente f y g_0 son no comaximales.

Sea M un ideal maximal de $k[z,t]$ conteniendo a f y g_0. Entonces $g = g_0^{p^r} \in M^2$ pues $r \geq 1$ y por tanto $g \in fk[z,t] + M^2$. Es decir, podemos aplicar el lema 2.8 b. llegando a una contradicción. Luego, no existe ninguna aplicación exponencial no trivial ϕ en B tal que $y \in B^{\phi}$.

□

Lema 2.10 *Sea k un cuerpo infinito de característica positiva p y*

$$A = k[X,Y,Z,T] \Big/ \left\langle X^m Y + Z^{p^e} + T + T^{sp} \right\rangle$$

donde m, e, s son enteros positivos tales que $p^e \nmid sp$, $sp \nmid p^e$ y $m > 1$. Entonces A posee al menos una aplicación exponencial no trivial.

Demostración.

El polinomio $f = X^m Y + Z^{p^e} + T + T^{sp}$ es un polinomio irreducible en $k^{[4]}$ y por tanto $\langle f \rangle$ genera un ideal primo en $k^{[4]}$. Consideremos la aplicación exponencial no trivial $\phi : k^{[4]} \to k^{[5]}$ definida en el ejemplo 1.3.8. Recordemos que esta aplicación viene definida por

$$\phi_1(X) = X, \quad \phi_1(Y) = Y - X^{m(p^e-1)}U^{p^e}, \quad \phi_1(Z) = Z + X^m U, \quad \phi_1(T) = T$$

Notar que $f \in \left(k^{[4]}\right)^{\phi}$, ya que

$$\phi(f) = \phi(X)^m \phi(Y) + \phi(Z)^{p^e} + \phi(T) + \phi(T)^{sp} = X^m\left(Y - X^{m(p^e-1)}U^{p^e}\right) + (Z + X^m U) + T + T^{sp} = f$$

Por otro lado, $Z \in k^{[4]} \setminus \left(k^{[4]}\right)^{\phi}$, pero $D_1(Z) = X^m \notin \langle f \rangle$. Luego, por la nota 2.7 existe una aplicación exponencial no trivial en A.

□

Proposición 2.11 *Sea k un cuerpo infinito de característica $p > 0$ y*

$$A = k[X,Y,Z,T] \Big/ \left\langle X^m Y + Z^{p^e} + T + T^{sp} \right\rangle$$

donde m, e, s son enteros positivos tales que $p^e \nmid sp$, $sp \nmid p^e$ y $m > 1$. Sea ϕ una aplicación exponencial no trivial en A. Entonces $A^\phi \subseteq k[x,z,t]$, donde x,y,z,t denotan las imagenes de X,Y,Z,T en A. En particular, $DK(A) \subsetneq A$.

Demostración.

Por el lema 2.10 existe al menos una aplicación no trivial en A. Demos a x,y,z,t los siguientes pesos.

$$wt(x) = -1, \quad wt(y) = m, \quad wt(z) = 0, \quad wt(t) = 0$$

entonces el polinomio, $x^m y + z^{p^e} + t + t^{sp}$ es un polinomio homogéneo y podemos considerar una estructura de $\mathbb{Z}$-álgebra graduada de A con esos pesos.

Para cada $g \in A$, denotaremos por $\widehat{g}$ a la componente homogénea de g en A de grado máximo. Como en la prueba del lema 2.9, vemos que ϕ induce una aplicación exponencial no trivial $\widehat{\phi}$ en $A(\cong gr(A))$ tal que $\widehat{g} \in A^{\widehat{\phi}}$ mientras que $g \in A^\phi$.

También de manera análoga a la anterior prueba, usando la relación $x^m y = -(z^{p^e} + t + t^{sp})$ si fuera necesario, llegamos a que cada elemento $g \in A$, puede escribirse de forma única como

$$g = \sum_{n \geq 0} g_n(z,t) x^n + \sum_{j>0, 0 \leq i < m} g_{ij}(z,t) x^i y^j \tag{2.3}$$

donde $g_n(z,t), g_{ij}(z,t) \in k[z,t]$. Además, los elementos homogéneos son de la forma $g_1(z,t)x^i y^j$ con $0 \leq i < m$ y $j \geq 0$.

Probaremos el resultado por reducción a lo absurdo. Supongamos que $A^\phi \not\subseteq k[x,z,t]$. Entonces podemos considerar $f \in A^\phi \setminus k[x,z,t]$. Veamos la expresión de $\widehat{f} \in A^\phi$.

Como $f \in A$, entonces se puede expresar como en (2.3). Sabemos que f tiene un término que posee a y como factor. Este término debe pertencer al segundo sumatorio, es decir, tiene que ser uno de la forma $f_{ij}(z,t)x^i y^j$ con $j > 0$ y $0 \leq i < m$, y su grado es $-i + mj$. Como $i < m$, se tiene que $-i + mj > m(j-1) \geq 0$. Luego el grado de este término es positivo.

Por otro lado, los términos que se encuentran en el primer sumatorio tienen grado $-n \leq 0$. De aquí se deduce que el elemento homogéneo de mayor grado, $\widehat{f}$, tiene que ser de la forma $f_1(z,t)x^a y^b$ con $0 \leq a < m$, $b > 0$ y $f_1(z,t) \in k[z,t]$. Por el lema 1.2.6 a. A^ϕ es factorialmente cerrado en A, de lo que se sigue que $y \in A^\phi$.

Escribimos s como qp^r donde $p \nmid q$. Gracias a que $p^e \nmid sp = qp^{r+1}$, se tiene que $e > r+1$ y por tanto $e - r - 1 > 0$ y ya que $sp = qp^{r+1} \nmid p^e$, se tiene que $q > 1$, pues $r + 1 < e$.

Es fácil comprobar que $k[x, x^{-1}, z, t]$ tiene una estructura de $\mathbb{Z}$-álgebra graduada sobre k con los siguientes pesos en los generadores

$$wt(x) = 0, \quad wt(z) = q, \quad wt(t) = p^{e-r-1}$$

Basta tomar $C_i := \{f \in k\left[x, x^{-1}, z, t\right] \big| deg(f) = i\}$, entonces $f \in C_i$ si y sólo si $deg(f) = i$ y por tanto $C_i \cap C_j = \{0\}$ y $k[x, x^{-1}, z, t] = \bigoplus_{i \in \mathbb{Z}} C_i$. Además, $deg(fg) = deg(f) + deg(g)$ y por tanto se tiene que $C_i C_j \subseteq C_{i+j}$.

Observar que $A[x^{-1}] = k[x,y,z,t,x^{-1}]$ pero entonces la relación que existe entre x,y,z y t en A, se puede expresar de la siguiente manera:

$$y = -x^{-m}\left(z^{p^{e-r}} + t + t^{sp}\right)$$

y por tanto $k\left[x,y,z,t,x^{-1}\right] = k\left[x,z,t,x^{-1}\right]$. Podemos entonces considerar la $\mathbb{Z}$-filtración propia $\{A_n\}_{n\in\mathbb{Z}}$ en A definida por $A_n := A \cap \bigoplus_{i \leq n} C_i$. Veamos que efectivamente es una $\mathbb{Z}$-filtración propia probando para ello cada una las propiedades de la definición. Antes, recordar que $\{D_n\}_{n\in\mathbb{Z}}$ con $D_n := \bigoplus\limits_{i \leq n} C_i$, forman una $\mathbb{Z}$-filtración propia de $k[x, x^{-1}, t, z]$ (1.4.5).

i. $A_n \subseteq A_{n+1}$. Si $a \in A_n$ entonces $a \in A$ y $a \in D_n \subset D_{n+1}$ y por tanto $a \in A_{n+1}$.

ii. $A = \bigcup\limits_{n\in\mathbb{Z}} A_n$.

$$\bigcup_{n\in\mathbb{Z}} A_n = \bigcup_{n\in\mathbb{Z}} \left(A \bigcap D_n\right) = A \bigcap \left(\bigcup_{n\in\mathbb{Z}} D_n\right) = A \bigcap k\left[x, x^{-1}, t, z\right] = A \bigcap A\left[x^{-1}\right] = A$$

iii. $\bigcap\limits_{n\in\mathbb{Z}} A_n = \{0\}$.

$$\bigcap_{n\in\mathbb{Z}} A_n = \bigcap_{n\in\mathbb{Z}} \left(A \bigcap D_n\right) = A \bigcap \left(\bigcap_{n\in\mathbb{Z}} D_n\right) = A \bigcap \{0\} = \{0\}$$

iv. $(A_n \setminus A_{n-1}) \cdot (A_m \setminus A_{m-1}) \subseteq A_{n+m} \setminus A_{n+m-1}$. Teniendo en cuenta que $(B_1 \bigcap B_2) \setminus (B_1 \bigcap B_3) = B_1 \bigcap (B_2 \setminus B_2)$, consideremos $a_n \in A_n \setminus A_{n-1}$ y $a_m \in A_m \setminus A_{m-1}$. Es decir, $a_n \in A \bigcap D_n \setminus D_{n-1}$ y $a_m \in A \bigcap D_m \setminus D_{m-1}$, entonces

$$a_n a_m \in A \bigcap (D_{n+m} \setminus D_{n+m-1}) = A_{n+m} \setminus A_{n+m-1}$$

Denotemos por B al anillo graduado $gr(A)(:= \bigoplus_{n\in\mathbb{Z}} A_n/A_{n-1})$ con respecto a la filtración anterior. Demostraremos que

$$B \cong k[X, Y, Z, T] \Big/ \left\langle X^m Y + Z^{p^e} + T^{sp} \right\rangle \tag{2.4}$$

para poder aplicar el lema 2.9 a B.

Para cada $g \in A$, denotaremos por $\overline{g}$ a la imagen de g en B. Por la expresión única de los elementos de A dada en (2.3), cualquiera de ellos puede ser escrito como un polinomio en las variables $\overline{x}, \overline{y}, \overline{z}$ y $\overline{t}$. Además, si $g \in A_n \setminus A_{n-1}$, entonces cada término de g pertenece a D_n, es decir, cada término pertenece a A_n luego la filtración definida en A es admisible con el conjunto de generadores $\Gamma := \{x, y, z, t\}$. De esta manera, B está generado por $\overline{x}, \overline{y}, \overline{z}$ y $\overline{t}$ (1.4.4).

Consideremos el anillo graduado de $k\left[x, x^{-1}, z, t\right]$ con la filtración propia definida por $\{D_n\}_{n\in\mathbb{Z}}$. Observar que el homomorfismo

$$\begin{array}{ccc} A_n/A_{n-1} & \longrightarrow & D_n/D_{n-1} \\ a_n + A_{n-1} & \longmapsto & a_n + D_{n-1} \end{array}$$

es inyectivo para todo n. Para verlo, tomamos un elemento $a_n + A_{n-1} \in A_n/A_{n-1}$ tal que $a_n \in D_{n-1}$. Como $a_n \in A_n = A \cap D_n$, podemos concluir que $a_n \in A \cap D_{n-1}$, pero entonces $a_n + A_{n-1} = 0$. De aquí, se tiene que B puede identificarse con un subanillo de $gr\left(k\left[x, x^{-1}, t, z\right]\right)$.

Recordar que por el lema 1.4.5, se tiene que $gr\left(k\left[x, x^{-1}, t, z\right]\right) \cong k\left[x, x^{-1}, t, z\right]$. Por tanto, B puede ser identificado con un subanillo de $k\left[x, x^{-1}, z, t\right]$. Gracias a esto, podemos ver que los elementos $\overline{x}, \overline{z}$ y $\overline{t}$ de B son algebraicamente independientes sobre k. Esto se debe a que $\overline{x}, \overline{z}$ y $\overline{t}$, bajo el isomorfismos $gr\left(k\left[x, x^{-1}, z, t\right]\right) \cong k\left[x, x^{-1}, z, t\right]$, se identifican con x, z, t en $k\left[x, x^{-1}, z, t\right]$, los cuales son algebraicamente independientes. Observar que gracias a la independencia, $\operatorname{tr.deg}_k(B) = 3$.

Como $y = -x^{-m}\left(z^{p^e} + t + t^{st}\right)$, entonces el grado $\deg(y) = \max\left\{qp^e, p^{e-r-1}, qp^{e-r}\right\} = qp^e$. Definimos $l_1 := qp^e$ y $l_2 := p^{e-r-1}$, con lo que $l_2 < l_1$. Entonces $x^m y, z^{p^e}$ y t^{sp} pertenecen a $A_{l_1} \setminus A_{l_1-1}$ y $t \in A_{l_2} \setminus A_{l_2-1}$. Como $x^m y + z^{p^e} + t^{sp} = -t \in A_{l_2} \subset A_{l_1-1}$, tenemos que $\overline{x}^m \overline{y} + \overline{z}^{p^e} + \overline{t}^{sp} = 0$ en B.

Ahora como $k[X, Y, Z, T]/\langle X^m Y + Z^{p^e} + T^{sp}\rangle$ es un dominio de integridad, afirmamos que el isomorfismo 2.4 se da. Probaremos esta afirmación.

Consideremos el siguiente homomorfismo sobreyectivo

$$\begin{array}{cccc} \varphi: & k[X, Y, Z, T] & \twoheadrightarrow & B \\ & f(X, Y, Z, T) & \mapsto & f(\overline{x}, \overline{y}, \overline{z}, \overline{t}) \end{array}$$

Observar que $\varphi\left(X^m Y + Z^{p^e} + T^{sp}\right) = \overline{x}^m \overline{y} + \overline{z}^{p^e} + \overline{t}^{sp} = 0$. Luego $\left\langle X^m Y + Z^{p^e} + T^{sp}\right\rangle \subseteq \ker\varphi$. Definimos entonces la aplicación

$$\varphi_1 : k[X, Y, Z, T] \Big/ \left\langle X^m Y + Z^{p^e} + T^{sp} \right\rangle \twoheadrightarrow B$$

inducida por φ que sigue siendo sobreyectiva y supongamos que $\ker\varphi_1 \neq 0$. Recordemos que B es un dominio de integridad (1.4.2) y que por tanto $\langle 0\rangle$ es un ideal primo en B cuyo ideal contraido es $\ker\varphi_1$, luego éste debe ser un ideal primo. Contrayendo este ideal en $k[X,Y,Z,T]$ y teniendo en cuenta que $k[X,Y,Z,T]$ es un dominio de integridad, obtenemos

$$\langle 0\rangle \subsetneq \left\langle X^mY + Z^{p^e} + T^{sp}\right\rangle \subsetneq \ker\varphi_1^c$$

Por tanto la altura de $\ker\varphi_1^c$ es mayor o igual que 2. Se tiene entonces que $\operatorname{tr.deg}_k\left(k[X,Y,Z,T]/\ker\varphi_1^c\right) \leq 2$.

Además,

$$B \cong \left(k[X,Y,Z,T]/\langle g\rangle\right)/\ker\varphi \cong k[X,Y,Z,T]/\langle g, \ker\varphi_1^c\rangle = k[X,Y,Z,T]/\ker\varphi_1^c$$

llegando a una contradicción, pues $\operatorname{tr.deg}_k(B) = 3$. De aquí 2.4 es cierto.

Recordemos que $y \in A^{\widehat{\phi}}$ y que A tiene una $\mathbb{Z}$-filtración propia admisible. Por esta razón podemos aplicar el teorema 1.4.6, dando como resultado que $\widehat{\phi}$ induce una aplicación exponencial no trivial $\overline{\phi}$ en B e $\overline{y} \in B^{\overline{\phi}}$

Observar también que $B \cong k[X,Y,Z,T]\Big/\left\langle X^mY + Z^{p^e} + T^{sp}\right\rangle$ está en las condiciones del lema 2.9 pues k es un cuerpo de característica $p > 0$, m, e, sp son enteros positivos tales que $s = qp^r$ con $q > 1$ y $p \nmid q$. Además, $sp = qp^{r+1}$ y como $e - (r+1) > 0$, se tiene que $e > r+1 > 1$. Pero este lema nos dice que B no admite ninguna aplicación exponencial no trivial tal que y esté en su anillo de invariantes. Hemos llegado así a una contradicción, por lo que podemos concluir que $A^{\phi} \subseteq k[x,z,t]$. De manera obvia, podemos concluir que en particular $DK(A) \subsetneq A$, pues para todo aplicación exponencial no trivial de A, $A^{\phi} \in k[x,z,t]$.

□

Nota 2.12 *El lema 2.9 y la proposición 2.11 no se cumplen si $m = 1$, i.e si*

$$A = k[X,Y,Z,T]\Big/\left\langle XY + Z^{p^e} + T + T^{sp}\right\rangle$$

Para ello, consideremos $f(y,z) \in k[y,z] \setminus \{0\}$ y definamos $\phi_1 : A \to A[U]$ como

$$\phi_1(y) = y, \quad \phi_1(z) = z, \quad \phi_1(t) = t + yf(y,z)U$$
$$\phi_1(x) = x - f(y,z)U - y^{sp-1}(f(y,z)U)^{sp}$$

Observar que este homomorfismo está bien definido, pues

$$\begin{aligned} \phi_1\left(xy + z^{p^e} + t + t^{sp}\right) &= (x - f(y,z)U - y^{sp-1}(f(y,z)U)^{sp})y + z^{p^e} + t + yf(y,z)U + (t + yf(y,z)U)^{sp} \\ &= xy - yf(y,z)U - y^{sp}(f(y,z)U)^{sp} + z^{p^e} + t + yf(y,z)U + t^{sp} + (yf(y,z)U)^{sp} \\ &= xy - z^{p^e} + t + t^{sp} = 0 \end{aligned}$$

Además, cumple las condiciones para ser una aplicación exponencial. Para probarlo es suficiente con ver que estas condiciones se cumplen para los generadores.

1. Para probar que $\phi_1 = Id \mod U$, basta ver que se tiene para t y x, para y y z se tiene por definición. Pero es obvio que $\phi_1(t) = t \mod U$ y que $\phi_1(x) = x \mod U$.

2. La segunda propiedad nos dice que $\phi_{1_V}\phi_{1_U} = \phi_{1_{U+V}}$.

$$\begin{aligned} \phi_{1_V}\phi_{1_U}(y) &= y = \phi_{1_{U+V}}(y) \\ \phi_{1_V}\phi_{1_U}(z) &= z = \phi_{1_{U+V}}(z) \\ \phi_{1_V}\phi_{1_U}(t) &= t + yf(y,z)V + yf(y,z)U \\ &= t + yf(y,z)(U+V) = \phi_{1_{U+V}}(t) \\ \phi_{1_V}\phi_{1_U}(x) &= x - f(y,z)V - y^{sp-1}(f(y,z)V)^{sp} - f(y,z)U - y^{sp-1}(f(y,z)U)^{sp} \\ &= x - f(y,z)(U+V) - y^{sp-1}(f(y,z)(U+V))^{sp} = \phi_{1_{U+V}}(x) \end{aligned}$$

Esta aplicación exponencial es no trivial e $y, z \in A^{\phi_1}$. Consideremos en segundo lugar el homomorfismo definido por

$$\begin{aligned} \phi_2(y) = y, &\quad \phi_2(z) = z + yg(y,t)U \\ \phi_2(t) = t, &\quad \phi_2(x) = x - y^{p^e-1} g(y,t)^{p^e} U^{p^e} \end{aligned}$$

donde $g(y,t) \in k[y,t] \setminus 0$. Razonando como antes se prueba que este homomorfismo está bien definido y que además es una aplicación exponencial no trivial con $y, t \in A^{\phi_2}$.

Si además, intercambiamos los papeles de x e y en ϕ_1 y ϕ_2, tenemos dos aplicaciones exponenciales no triviales tales que x está en sus anillo de invariantes. De aquí, $DK(A) = A$. Luego la proposición 2.11 no se cumple.

Teorema 2.13 *Sea k un cuerpo infinito de característica $p > 0$ y*

$$A = k[X,Y,Z,T] \Big/ \left\langle X^m Y + Z^{p^e} + T + T^{sp} \right\rangle$$

donde m, e, s son enteros positivos tales que $p^e \nmid sp$ y $sp \nmid p^e$ y $m > 1$. Entonces $A \ncong_k k^{[3]}$.

Demostración.

Sabemos que para A existen aplicaciones exponenciales no triviales (2.10). Por la proposición 2.11, tenemos que $DK(A) \subsetneq A$. Además, $\operatorname{tr.deg}_k(A) = 3 > 1$ luego por el lema 1.2.10 se concluye que A no es un anillo de polinomios sobre k. En particular, $A \ncong_k k^{[3]}$.

□

Corolario 2.14 *La conjetura de la cancelación no se cumple para el anillo de polinomios $k[X,Y,Z]$, donde k es un cuerpo infinito de característica positiva.*

Demostración.

Consideremos el dominio afín

$$A = k[X,Y,Z,T] \Big/ \left\langle X^m Y + Z^{p^e} + T + T^{sp} \right\rangle$$

como en el teorema precedente (2.13). Por éste, se tiene que $A \ncong_k k^{[3]}$. Sin embargo, A cumple todas las hipótesis del corolario 1.1.6, de lo que se deduce que $A^{[1]} \cong_k k^{[4]}$.

□

Bibliografía

[AEH] S. Abhyankar, P. Eakin, W. Heinzer, *On the uniqueness of the coefficient ring in a polynomial ring*, J. Algebra 23: 310-342 (1972)

[As] T. Asanuma, *Polynomial fibre rings of algebras over Noetherian rings*, Invent. Math. 87: 101-127 (1987).

[Asa] T. Asanuma, *Non-linearizable algebraic group actions on* $\mathbb{A}^n$. J. Algebra 166: 72-79 (1994)

[Ba] H. Bass, E. Connel, D. Wright, *Locally polynomial algebras are symmetric algebras*, Invent. math. 38: 279-299 (1977)

[Cr] A. Crachiola, *The hypersurface* $x + x^2y + z^2 + t^3$ *over a field of arbitrary characteristic*, Proc. Am. Math. Soc. 134(5), 1289-1298 (2005).

[CM] A. Crachiola, L. Makar-Limanov, *On the rigidity of small domains*, J.Algebra, 284: 1,1-12 (2005).

[CML] A. Crachiola, L. Makar-Limanov, *An algebraic proof of a cancellation theorem for surfaces*, J. Algebra 320(8): 3113-3119 (2008)

[Fuj] T. Fujita, *On Zariski problem*, Proc. Jpn. Acad., 55A: 106-110 (1979)

[Fu] W. Fulton, *Algebraic curves: An introduction to algebraic geometry*,W.A. Benjamin, Inc.,1969, U.S.A.

[Gu] N. Gupta, *On the cancellation problem for the affine space* $\mathbb{A}^3$ *in characteristic* p, Invent. Math. 195: 279-288(2014).

[Gup] N. Gupta, *On Zariski's Cancellation Problem in positive characteristic*, preprint, 2013.

[Ma] H. Matsumara, *Commutative Algebra, Second Edition*, The Benjamin/Cummings publishing company, Inc., 1980, U.S.A.

[MS] M. Miyanishi, T. Sugie, *Affine surfaces containing cylinderlike open sets*, J. Math. Kyoto Univ. 20: 11-42 (1980)

[Is] I.M. Isaacs, *Algebra, a graduate course*, Brooks/Cole, Pacific Grove, 1994, U.S.A.

[Ru] P. Russell, *On affine-ruled rational surfaces*, Math. Ann. 255: 287-302 (1981)