

Ideales primos en extensiones PBW torcidas

JUAN PABLO ACOSTA LÓPEZ

UNIVERSIDAD NACIONAL DE COLOMBIA
FACULTAD DE CIENCIAS
DEPARTAMENTO DE MATEMÁTICAS
BOGOTÁ, D.C.
ENERO DE 2014

Ideales primos en extensiones PBW torcidas

JUAN PABLO ACOSTA LÓPEZ

DIRECTOR
OSWALDO LEZAMA
PROFESOR TITULAR

UNIVERSIDAD NACIONAL DE COLOMBIA
FACULTAD DE CIENCIAS
DEPARTAMENTO DE MATEMÁTICAS
BOGOTÁ, D.C.
ENERO DE 2014

Título en español

Ideales primos en extensiones PBW torcidas

Title in English

Prime ideals in skew PBW extensions

Resumen: En el trabajo estudiamos algunas propiedades de extensiones PBW torcidas, realizamos la construcción y caracterización por propiedad universal, describimos el proceso de extensión de ideales del anillo de coeficientes a ideales primos de una extensión PBW torcida biyectiva, y relacionamos los ideales primos de la extensión con una órbita de un ideal primo del anillo de coeficientes bajo los automorfismos que definen la extensión.

Abstract: In this work we study some properties of skew PBW extensions, we make the construction and characterization by universal property, we describe the extension process from an ideal in the coefficient ring to bijective skew PBW extension, and we associate with each prime ideal of the extension an orbit of a prime ideal of the coefficient ring under the automorphisms that define the extension.

Palabras clave: Extensiones PBW torcidas, propiedad universal, localización, propiedad de Jacobson, ideales primos.

Keywords: Skew PBW extensions, universal property, localization, Jacobson property, prime ideals.

Agradecimientos

Agradezco a el profesor Oswaldo Lezama, por guiarme en el proceso de la producción de este trabajo.

Agradezco a mis padres por todo el apoyo que me han dados durante muchos años, y que han hecho posible que me concentre en mis estudios.

Índice general

Índice general	I
Introducción	II
1. Preliminares	1
1.1. Teoría general de anillos	1
1.2. Extensiones PBW torcidas generalizadas	4
2. Propiedad Universal	7
2.1. Construcción y caracterización de las extensiones PBW torcidas generalizadas	7
2.2. Extensión del anillo de coeficientes	15
2.3. Aplicaciones	18
3. Ideales primos	23
3.1. Extensión a ideales primos	23
3.2. A cada ideal primo de la extensión se le asocia una órbita en $\text{Spec}(R)$	27
3.3. Propiedad de Jacobson	30
Bibliografía	34

Introducción

En este trabajo se estudian los ideales primos de las llamadas extensiones PBW torcidas introducidas en [5] y ampliamente estudiadas en [6].

En el transcurso del trabajo realizamos la construcción fundamental y caracterización por propiedad universal de estas extensiones, este resultado se encuentra en la sección 2.1 teorema 4. En el contexto de este teorema resulta natural generalizar las extensiones PBW torcidas originales, estas extensiones se llaman aquí extensiones PBW torcidas generalizadas, véase la sección 1.2 definición 7, estos objetos incluyen en particular los anillos de polinomios torcidos $R[x, \sigma, \delta]$ (incluso si σ es un endomorfismo no inyectivo) y las álgebras envolventes de álgebras de Lie libres sobre un anillo k conmutativo (incluso si el álgebra de Lie es infinito dimensional). En la sección 2.1 ejemplo 1 vimos que la construcción y caracterización en el teorema 4 de la sección 2.1, aplicada a las álgebras de Lie libres sobre un anillo k conmutativo produce el teorema de Poincaré-Birkhoff-Witt.

Las extensiones PBW torcidas generalizadas más frecuentes en la teoría son las finitas y biyectivas, véase la sección 1.2, estas extensiones coinciden con las extensiones PBW torcidas biyectivas definidas anteriormente, por ejemplo en [5], y por lo tanto para estas extensiones abandonamos el calificativo de generalizada, en particular este tipo de extensiones es la que se considera en el capítulo 3, donde se lleva a cabo un primer estudio de los ideales primos en estas extensiones con la hipótesis adicional de la Noetherianidad del anillo de coeficientes.

Resumimos a continuación los principales resultados de este trabajo

En la sección 1.1 reunimos algunos resultados estándar de la teoría general de anillos, principalmente algunas nociones relacionadas con localización en anillos no conmutativos. En la sección 1.2 damos la definición de extensión PBW torcida generalizada y algunas consecuencias sencillas de la definición.

En la sección 2.1 el resultado principal es el teorema 4 como ya se mencionó antes. En la sección 2.2 consideramos un anillo A , un homomorfismo de anillos $\varphi : A \rightarrow B$ y una extensión PBW torcida $\sigma(A)[X]$, y abordamos el problema de construir $\sigma(A)[X] \rightarrow \sigma(B)[X]$ que extienda a φ . Esto se hace en dos pasos, primero se extienden derivaciones de A a B en el corolario 2, y segundo se aplica el teorema 4 de la sección 2.1, para construir $\sigma(B)[X]$ en la proposición 6. En la sección 2.3 probamos algunas proposiciones conocidas sobre extensiones PBW generalizadas quasiconmutativas y finitas, que permiten simplificar algunas pruebas usando el método de graduación, como ejemplo se prueba el teorema conocido de la base de Hilbert para extensiones PBW generalizadas finitas y biyectivas. Se prueba además un resultado nuevo sobre localización por sistemas multiplicativos del

anillo de coeficientes invariantes por los endomorfismos asociados a la extensión, que se obtiene como corolario de la sección 2.2.

El capítulo 3, como ya se dijo antes, es un primer estudio de los ideales primos en una extensión PBW torcida biyectiva.

En la sección 3.1 se extienden ideales del anillo de coeficientes a la extensión, aquí seguimos parte de lo que se hizo en el artículo [2] para anillos de polinomios torcidos, los resultados principales son las proposiciones 12 y 15. En la sección 3.2 se modifica la técnica clásica de contracción y se le asocia a cada ideal primo de la extensión una órbita, por los automorfismos asociados a la extensión, de ideales primos en el anillo de coeficientes, el resultado principal es la proposición 18, aquí seguimos parte de los que se hizo en el artículo [4] para anillos de polinomios torcidos.

Finalmente en la sección 3.3 presentamos como tópico adicional la propiedad de Jacobson para extensiones PBW torcidas biyectivas sobre un cuerpo, el resultado principal es la proposición 22, aquí seguimos los resultados relevantes de [1], donde se prueba esto para álgebras envolventes de álgebras de Lie.

La mayor parte de los resultados son nuevos, exceptuando la sección 1.1 y parte de la sección 2.3.

Preliminares

En este capítulo se describen algunas definiciones, construcciones y propiedades de la teoría general de anillos en la primera sección; y de las extensiones PBW torcidas generalizadas en la segunda sección.

En todo el trabajo consideramos sólo anillos asociativos con unidad, pero no necesariamente conmutativos.

1.1. Teoría general de anillos

Empezamos describiendo la teoría de localización por sistemas multiplicativos de Ore.

Definición 1. Sea R un anillo y $S \subseteq R$; decimos que S es un subconjunto multiplicativo de R si $s_1 \in S$ y $s_2 \in S$ implican $s_1 s_2 \in S$.

Decimos que S es un conjunto de Ore a izquierda si además se tiene

1. Si $r \in R$ y $s \in S$ cumplen $rs = 0$ entonces existe $s_1 \in S$ con $s_1 r = 0$.
2. Para $r \in R$ y $s \in S$ existen $r_1 \in R$ y $s_1 \in S$ tales que $s_1 r = r_1 s$.

Observamos que cualquier subconjunto multiplicativo de un anillo conmutativo es de Ore (por ambos lados).

Definición 2. Sea R un anillo y $S \subseteq R$ un subconjunto multiplicativo. Sea A un anillo, y $\phi : R \rightarrow A$ un morfismo de anillos.

Entonces (A, ϕ) es una localización de Ore de R con respecto a S por la izquierda si, y sólo si,

1. $\phi(s)$ es invertible en A para todo $s \in S$.
2. $\text{Ker}(\phi) = \{r \in R \mid \text{existe } s \in S, \text{ tal que } sr = 0\}$.
3. Todo elemento en A es de la forma $\phi(s)^{-1} \phi(r)$, con $r \in R$ y $s \in S$.

Notamos que S es un subconjunto multiplicativo de R si, y sólo si, $S' = S \cup \{1\}$ es un subconjunto multiplicativo de R ; además S es de Ore a izquierda si, y sólo si, S' es de Ore a izquierda y (A, ϕ) es una localización de Ore por la izquierda de R con respecto a S si, y sólo si, es una localización de Ore por la izquierda de R con respecto a S' .

Por esta razón generalmente se asume que $1 \in S$.

Notamos también que para (A, ϕ) una localización de Ore por la izquierda de R con respecto a S , $A = 0$ si, y sólo si, $0 \in S$.

Finalmente ϕ es inyectivo si, y sólo si, los elementos de S son regulares, es decir para $s \in S$ y $r \in R$, $sr = 0$ o $rs = 0$ implica $r = 0$. El teorema principal es el siguiente.

Teorema 1. *Sea R un anillo y S un subconjunto multiplicativo de R . Entonces una localización de Ore por la izquierda de R con respecto a S , (A, ϕ) existe, si, y sólo si, S es de Ore a izquierda.*

En este caso (A, ϕ) cumple la siguiente propiedad universal:

1. $\phi(s)$ es invertible en A para todo $s \in S$.
2. Si $\tau : R \rightarrow B$ es un morfismo de anillos con $\tau(s)$ invertible en B para todo $s \in S$, existe un único morfismo de anillos $T : A \rightarrow B$ tal que $T\phi = \tau$.

Vemos entonces que el par (A, ϕ) , cuando existe, es único salvo isomorfismo, cuando existe se denota $S^{-1}R$.

También se tienen las definiciones simétricas de un conjunto de Ore a derecha y de RS^{-1} , y la simetría de la propiedad universal implica que $S^{-1}R \cong RS^{-1}$ cuando ambos existen. Hay también una teoría similar para módulos.

Definición 3. *Sea R un anillo y $S \subseteq R$ un subconjunto multiplicativo de Ore a izquierda. Sea M un R -módulo izquierdo y N un $S^{-1}R$ módulo izquierdo. Suponiendo $\phi : M \rightarrow N$ un morfismo de R -módulos.*

Entonces (N, ϕ) es una localización de Ore de M con respecto a S por la izquierda si, y sólo si,

1. $\text{Ker}(\phi) = \{m \in M \mid \text{existe } s \in S, \text{ tal que } sm = 0\}$.
2. Todo elemento en M es de la forma $s^{-1}\phi(m)$, con $m \in M$ y $s \in S$.

Tenemos la siguiente propiedad universal.

Teorema 2. *Sea R un anillo y S un subconjunto multiplicativo de Ore a izquierda de R . Sea M un R -módulo izquierdo. Entonces una localización de Ore por la izquierda de M con respecto a S , (N, ϕ) existe y cumple la propiedad universal:*

- Si B es un $S^{-1}R$ módulo izquierdo y $\tau : R \rightarrow B$ es un morfismo de R -módulos, entonces existe un único morfismo de $S^{-1}R$ -módulos $T : N \rightarrow B$ tal que $T\phi = \tau$.

Se tiene también el isomorfismo de $S^{-1}R$ -módulos $N \cong S^{-1}R \otimes_R M$.

Podemos denotar la localización del módulo M con respecto al sistema multiplicativo S , por $S^{-1}M$. Esta notación es consistente con la introducida para anillos antes (la localización de R es $S^{-1}R$).

Proposición 1. *Sea R un anillo y S un sistema multiplicativo de Ore a izquierda en R . Si $M_1 \rightarrow M_2 \rightarrow M_3$ es una sucesión exacta de R -módulos izquierdos, entonces $S^{-1}M_1 \rightarrow S^{-1}M_2 \rightarrow S^{-1}M_3$ (con morfismos naturales) es una sucesión exacta de $S^{-1}R$ -módulos izquierdos, en otras palabras $S^{-1}R$ es un R -módulo derecho plano. Si $N \subset S^{-1}M$ es un $S^{-1}R$ -submódulo de $S^{-1}M$, entonces existe $N_1 \subset M$ un R -submódulo de M tal que $N = S^{-1}N_1$.*

Concluimos con una especificación del teorema de Goldie (suficiente para los propósitos de este trabajo).

Teorema 3. *Si R es un anillo Noetheriano y semiprimo, entonces existe el anillo total de fracciones de R , es decir, existe $D = S^{-1}R$ con S el conjunto de elementos regulares de R . Además D es semisimple; y D es simple si, y sólo si, R es primo.*

Estos teoremas se pueden encontrar por ejemplo en [4] capítulo 6 (teorema de Goldie) y capítulo 10 (anillo de fracciones).

Definición 4. *Dado R un anillo definimos $C_R(0)$ como el conjunto de elementos regulares de R . Para un ideal $I \subseteq R$ definimos $C_R(I)$ como el conjunto de elementos de R cuya imagen en R/I es regular en R/I .*

Definición 5. *Sean R un anillo, S un conjunto multiplicativo de R y M un R -módulo izquierdo. Se dice que M es libre de S -torsión si $sm = 0$ implica $m = 0$ para todo $m \in M$ y $s \in S$.*

Se dice que M es libre de torsión si M es libre de $C_R(0)$ -torsión.

Los siguientes dos lemas se usan en la sección 3.2

Lema 1. *Sea R es un anillo noetheriano, P es un ideal primo de R y σ es un automorfismo de R . Sea D el anillo total de fracciones de R/P . Sea D^σ el D - R -módulo definido como: por grupo abeliano se toma el mismo D , y la multiplicación se define como $d \cdot a \cdot r = da\sigma(r)$ para $d, a \in D$ y $r \in R$. Entonces D^σ es simple.*

Demostración. El látice de sub-bimódulos en D^σ es el mismo que en D , luego basta tomar σ la identidad.

Reemplazando R por R/P vemos que se puede tomar sin pérdida de generalidad $P = 0$. En este caso tomemos S el conjunto de elementos regulares de R , de forma que $D = S^{-1}R$, y tomemos $E \subseteq D$ un $D - R$ -sub-bimódulo.

Recordamos que D es simple y artiniano; vamos a ver que $Es^{-1} = E$ para $s \in S$ esto es suficiente porque entonces E es un ideal de D y D es simple.

Para ver que $Es^{-1} = E$, tomamos

$$\dots \subseteq Es^2 \subseteq Es \subseteq E$$

una cadena descendente de ideales izquierdos en D , como D es artiniano se concluye que $Es^{n+1} = Es^n$ y multiplicando por la derecha por s^{-n-1} se concluye lo que se busca. \square

Lema 2. Sean R un anillo Noetheriano y P es un ideal primo de R . Sea ${}_R M$ un R -módulo izquierdo con $\text{ann}_R M = P$ y libre de torsión como R/P módulo. Entonces $\text{ann}_R N = P$ y N es libre de torsión como R/P -módulo, para N un submódulo no nulo de M .

Demostración. $P \subseteq \text{ann}_R N$ y N es claramente libre de torsión como R/P -módulo.

Reemplazando R por R/P suponemos sin pérdida de generalidad que $P = 0$. De forma que R es primo y noetheriano.

Tenemos entonces que el anillo total de fracciones $D = S^{-1}R$ existe, (recordando que aquí S es igual a el conjunto de elementos regulares de R) y D es una extensión de R , simple y artiniana.

Como M es libre de torsión, podemos identificar $N \subseteq M \subseteq S^{-1}M$, luego $E = \text{ann}_D(N)$ es un $D - R$ -sub-bimódulo de D , y concluimos por el lema 1 que $E = 0$ o $E = D$. Si $E = D$ entonces $N = 0$, si $E = 0$ entonces $\text{ann}_R(N) = 0$ como se quiere. \square

1.2. Extensiones PBW torcidas generalizadas

En esta sección se definen las extensiones PBW torcidas generalizadas y se dan algunas de sus propiedades.

Primero recordamos la definición original de una extensión PBW torcida que aparece en [5].

Definición 6. Sea A un anillo y R un subanillo de A . Entonces A se dice una extensión PBW torcida de R con indeterminadas X si

1. Existen $x_1, \dots, x_n \in A$ tales que $\{x_1^{a_1} \cdots x_n^{a_n} \mid a_k \in \mathbb{N} \text{ para } 1 \leq k \leq n\}$ es una base de ${}_R A$.
2. Para $1 \leq k \leq n$ y $0 \neq r \in R$, existe $0 \neq c_{ir} \in R$ con $x_i r - c_{ir} x_i \in R$.
3. Para $1 \leq i, j \leq n$, existe $0 \neq c_{ij} \in R$ con $x_j x_i - c_{ij} x_i x_j \in \sum_{1 \leq k \leq n} R x_k + R$.

Ahora definimos la generalización que proponemos en este trabajo.

Definición 7. Sea R un anillo. Sea A un anillo y $\phi : R \rightarrow A$ un homomorfismo de anillos. Tomemos $X = \{x_i \mid i \in I\} \subseteq A$ un conjunto indexado por un conjunto totalmente ordenado I .

Denotamos $\text{Mon}(X) = \{x_{i_1} \cdots x_{i_n} \mid n \geq 0, i_k \in I \text{ para } 1 \leq k \leq n, \text{ y } i_1 \leq \cdots \leq i_n\} \subseteq A$.

Se dice que A es una extensión PBW torcida generalizada de R con indeterminadas X si

1. $\text{Mon}(X)$ es una base del módulo ${}_R A$.
2. Para $i \in I$ y $r \in R$ se tiene $x_i r \in R x_i + R1$.
3. Para $i \in I$ y $j \in I$ con $i < j$, se tiene

$$x_j x_i \in R x_i x_j + \sum_{i \in I} R x_i + R1$$

En este caso se denota $A = \sigma(R)[X]$.

En la definición de $\text{Mon}(X)$ tomando $n = 0$ se observa que $1 \in \text{Mon}(X)$ y por lo tanto ϕ es inyectivo, por el ítem 1 en la definición 7.

También se ve que para $i \in I$ y $r \in R$ existen únicos $\sigma_i(r) \in R$ y $\delta_i(r) \in R$ con

$$x_i r = \sigma_i(r)x_i + \delta_i(r)$$

por 1 y 2 en la definición 7.

Definición 8. Si σ es un endomorfismo del anillo R , $\delta : R \rightarrow R$ es una σ derivación si es un morfismo del grupo aditivo de R y se tiene

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b.$$

También se dice que (σ, δ) es una derivación.

Nótese que esto implica $\delta(1) = 0$, de aplicar la fórmula en la definición a la identidad $1 \cdot 1 = 1$

Proposición 2. Sea A es una extensión PBW torcida generalizada de R . Sean $\sigma_i : R \rightarrow R$ y $\delta_i : R \rightarrow R$ determinados por

$$x_i r = \sigma_i(r)x_i + \delta_i(r),$$

entonces σ_i es un endomorfismo del anillo R y δ_i es una σ_i derivación.

Demostración. Si $i \in I, a, b \in R$, $x_i ab = \sigma_i(a)x_i b + \delta_i(a)b = \sigma_i(a)\sigma_i(b)x_i + \sigma_i(a)\delta_i(b) + \delta_i(a)b$, por otro lado $x_i ab = \sigma_i(ab)x_i + \delta_i(ab)$, notamos que $x_i, 1$ son elementos de una base de ${}_R A$ luego se concluye $\sigma_i(ab) = \sigma_i(a)\sigma_i(b)$ y $\delta_i(ab) = \sigma_i(a)\delta_i(b) + \delta_i(a)b$. También se tiene $x_i(a+b) = x_i a + x_i b = \sigma_i(a)x_i + \delta_i(a) + \sigma_i(b)x_i + \delta_i(b)$, y por otro lado $x_i(a+b) = \sigma_i(a+b)x_i + \delta_i(a+b)$, de aquí se sigue $\sigma_i(a+b) = \sigma_i(a) + \sigma_i(b)$ y $\delta_i(a+b) = \delta_i(a) + \delta_i(b)$. Finalmente $x_i 1 = 1x_i$ luego $\sigma_i(1) = 1, \delta_i(1) = 0$ \square

En el caso particular en el que hay una sola variable $X = \{x\}$ la extensión se denota $A = R[x, \sigma, \delta]$ y se va a probar que siempre existe cuando (σ, δ) es una derivación, y es única salvo isomorfismo. Esto se va a ver en el siguiente capítulo.

Definición 9. Una extensión PBW torcida generalizada $A = \sigma(R)[X]$ se dice

1. finita si I es finito.
2. quasi conmutativa si para $i \in I$ y $r \in R$ se cumple $x_i r \in R x_i$. Y para $i \in I$ y $j \in I$ con $i < j$ se cumple $x_j x_i \in R x_i x_j$.
3. biyectiva si σ_i es un automorfismo y

$$x_j x_i - c_{ij} x_i x_j \in \sum_{i \in I} R x_i + R$$

con $c_{ij} \in R$ invertible.

Vemos que $\sigma(R)[X]$ está siempre dotado de la filtración estándar. En general si R, A son anillos, $\phi : R \rightarrow A$ es un homomorfismo de anillos y $X \subseteq A$ es un subconjunto tal que $\phi(R) \cup X$ generan a A como anillo, se define la filtración estándar en A como, para $n \in \mathbb{N}$ elementos en A_n son sumas de elementos de A de la forma $\phi(r_0)x_1\phi(r_1)\cdots x_m\phi(r_m)$ con $m \leq n$ y $x_i \in X$.

Propiedad Universal

En este capítulo se da la construcción fundamental de las extensiones PBW torcidas generalizadas que motivó la definición 7, y se da su caracterización por propiedad universal, esto se hace en la primera sección. En la segunda sección estudiamos la posibilidad de extender el anillo de coeficientes de una extensión PBW torcida generalizada, aquí usamos el resultado de la primera sección, junto con una manera muy general de extender derivaciones. En la tercera sección vemos unas consecuencias sencillas de las dos secciones anteriores, el comportamiento de una extensión PBW torcida generalizada al hacer la graduación por la filtración estándar; y al hacer la localización por un sistema multiplicativo del anillo de coeficientes invariante por los endomorfismos del anillo.

2.1. Construcción y caracterización de las extensiones PBW torcidas generalizadas

Dada una extensión PBW torcida generalizada $A = \sigma(R)[X]$, se tienen las siguientes identidades

1. Para $i < j$ en I y k en I existen únicos $c_{ij}, a_{ij}^k, d_{ij} \in R$ tales que $x_j x_i = c_{ij} x_i x_j + \sum_k a_{ij}^k x_k + d_{ij}$.
2. Para $i \in I$ y $r \in R$ existen únicos $\sigma_i(r) \in R$ y $\delta_i(r) \in R$ tales que $x_i r = \sigma_i(r) x_i + \delta_i(r)$.

Intuitivamente los parámetros $c_{ij}, a_{ij}^k, d_{ij}, \sigma_i$ y δ_i determinan por completo la extensión A , en lo que sigue se prueba esta afirmación y se encuentran condiciones necesarias y suficientes sobre estos parámetros que garantizan la existencia de una extensión PBW torcida generalizada A de R que cumple (1) y (2). Esto se consigue con una construcción explícita. Para enunciar las condiciones y para la prueba del teorema es conveniente introducir algunas definiciones.

Definición 10. *R un anillo y X un conjunto, al módulo libre con base las palabras en X (es decir sucesiones finitas de elementos de X) se le puede dar una estructura de anillo por concatenación y extensión R -bilinear, el anillo resultante se denomina extensión libre*

de R con coeficientes en X y con coeficientes que conmutan con variables y se denota $A = R \langle X \rangle$.

Definición 11. R un anillo, I un conjunto totalmente ordenado y w una palabra en $\{x_i : i \in I\} \cup R$ (es decir una sucesión finita de elementos en el conjunto $\{x_i : i \in I\} \cup R$) la complejidad de w denotada $c(w)$ es la tripla de números no negativos (a, b, c) donde $a = \text{card}\{s : w_s = x_i\}$ número de x 's en w , $b = \text{card}\{(s, r) : s < r, x_j = w(s), x_i = w_r, i < j\}$ es el número de inversiones que involucran sólo x 's y $c = \text{card}\{(s, r) : s < rw_s = x_i, w_r \in R\}$ el número de inversiones del tipo (x_i, r) .

Las triplas se ordenan con orden lexicográfico $(a, b, c) \leq (d, e, f)$ ssi $a < d$ o $a = d, b < e$ o $a = d, b = e, c \leq f$, se sabe que es un buen orden.

La complejidad es una medida de que tan lejos está una palabra de ser ordenada en el sentido: w como en la definición y de longitud $n + m$ es ordenada si $w = r_1 \cdots r_n x_{i_1} \cdots x_{i_m}$ con $n, m \geq 0$, $r_l \in R$ y $i_k \in I$ para $1 \leq l \leq n$ y $1 \leq k \leq m$; y además $i_1 \leq \cdots \leq i_m$.

Denotamos T el conjunto de palabras en $\{x_i : i \in I\} \cup R$ ordenadas y $\mathbb{Z}T$ el grupo aditivo en $\mathbb{Z} \langle \{x_i : i \in I\} \cup R \rangle$ generado por T .

Observamos que para cualquier palabra w de longitud m en $\{x_i : i \in I\} \cup R$, podemos elegir el menor entero n tal que $w_n \cdots w_m$ es ordenado, y encontramos que $w \in T$ o existen únicas palabras v_1 y v_2 tales que $w = v_1 x_i s v_2$ con $s \in R$ o $s = x_j$ y $j < i$ y $sv_2 \in T$, en efecto $v_2 = w_{n+1} \cdots w_m$.

Definición 12. Sea R un anillo y I un conjunto totalmente ordenado. Sean $\{c_{ij}\}_{i < j}$, $\{d_{ij}\}_{i < j}$, $\{a_{ij}^k\}_{i < j, k}$ elementos de R los índices i, j, k en I ; tales que para $i < j$ en I a_{ij}^k es 0 para casi todo k . Sean $\sigma_i, \delta_i : R \rightarrow R$ un par de funciones para cada $i \in I$. Se define $p : \{\text{palabras en } \{x_i : i \in I\} \cup R\} \rightarrow \mathbb{Z} \langle \{x_i : i \in I\} \cup R \rangle$ por inducción en la complejidad

1. Si $w \in T$ entonces $p(w) = w$.
2. Si $w = v_1 x_i r v_2$ con $r \in R$, y $r v_2 \in T$ entonces $p(w) = p(v_1 \sigma_i(r) x_i v_2) + p(v_1 \delta_i(r) v_2)$.
3. Si $w = v_1 x_j x_i v_2$, $x_i v_2 \in T$, $i < j$ entonces $p(w) = p(v_1 c_{ij} x_i x_j v_2) + \sum_k p(v_1 a_{ij}^k x_k v_2) + p(v_1 d_{ij} v_2)$. La suma es sobre los k con $a_{ij}^k \neq 0$.

Esta definición tiene sentido pues los tres casos son disyuntos y exhaustivos. Y adicionalmente porque la complejidad de los términos en la derecha disminuye (incidentalmente esta es la única propiedad de la función de complejidad que se usa).

A la extensión lineal de p , $\mathbb{Z} \langle \{x_i : i \in I\} \cup R \rangle \rightarrow \mathbb{Z} \langle \{x_i : i \in I\} \cup R \rangle$ también la llamo p .

Vemos que la imagen de p está en $\mathbb{Z}T$.

$\text{Mon} = \{\prod_{k=1}^n x_{i_k} : i_1 \leq \cdots \leq i_n, n \geq 0\}$, y $F_R(\text{Mon})$ es el R -módulo libre con base Mon . Definimos también $q : \mathbb{Z}T \rightarrow F_R(\text{Mon})$ como la extensión lineal de $q(r_1 \cdots r_m x_{i_1} \cdots x_{i_n}) = (\prod_{k=1}^m r_k) x_{i_1} \cdots x_{i_n}$.

Finalmente definimos $h : \mathbb{Z} \langle \{x_i : i \in I\} \cup R \rangle \rightarrow F_R(\text{Mon})$ como $h = qp$ y se denomina función de reducción.

Se enuncia el teorema principal

Teorema 4. $R, I, a_{ij}^k, c_{ij}, \sigma_i, \delta_i, h, p, q$ como en la Definición 12, entonces existe A extensión PBW torcida generalizada de R con

1. $x_i r = \sigma_i(r)x_i + \delta_i(r)$.
2. $x_j x_i = c_{ij}x_i x_j + \sum_k a_{ij}^k x_k + d_{ij}$, para $i < j$ en I .

si, y sólo si,

1. σ_i es endomorfismo de anillos de R y δ_i es σ_i -derivación.
2. $h(x_j x_i a) = h(p(x_j x_i) a)$ para $i < j$ y $a \in R$.
3. $h(x_k x_j x_i) = h(p(x_k x_j) x_i)$ para $i < j < k$.

Y en este caso la inclusión $\iota : R \rightarrow A$ cumple la propiedad universal:

Si $f : R \rightarrow B$ es un morfismo de anillos, y $y_i \in B$ son elementos de B indexados por I tales que

1. $y_i f(r) = f(\sigma_i(r))y_i + f(\delta_i(r))$.
2. $y_j y_i = f(c_{ij})y_i y_j + \sum_k f(a_{ij}^k)y_k + f(d_{ij})$, para $i < j$ en I .

Entonces existe un único morfismo de anillos $F : A \rightarrow B$ tal que $F\iota = f$ y $F(x_i) = y_i$

Demostración. Llamamos $t : F_R(Mon) \rightarrow \mathbb{Z} \langle \{x_i \mid i \in I\} \cup R \rangle$ la siguiente función: un elemento de $F_R(Mon)$ se escribe de forma única como $\Sigma r_{\bar{x}} \bar{x}$ donde la suma es sobre un conjunto finito de $\bar{x} \in Mon$ y $r_{\bar{x}} \neq 0$ son elementos de R ; entonces $t(\Sigma r_{\bar{x}} \bar{x}) := \Sigma r_{\bar{x}} \bar{x} \in \mathbb{Z} \langle \{x_i \mid i \in I\} \cup R \rangle$.

Necesidad

Ya se vió que 1 es necesario, para 2 y 3 usamos la propiedad universal de $\mathbb{Z} \langle \{x_i : i \in I\} \cup R \rangle$ para encontrar un morfismo de anillos $k : \mathbb{Z} \langle \{x_i : i \in I\} \cup R \rangle \rightarrow A$ con $k(x_i) = x_i, k(r) = r; i \in I, r \in R$. Probamos ahora que $k(w) = h(w)$ como ambos son lineales basta tomar w palabra, procedemos por inducción en $c(w)$, sea $w = w_1 x_i r w_2$ con $r \in R, i \in I, c(r w_2) = (a, 0, 0)$; entonces $h(w) = h(w_1 \sigma_i(r) x_i w_2) + h(w_1 \delta_i(r) w_2) = k(w_1 \sigma_i(r) x_i w_2) + k(w_1 \delta_i(r) w_2) = k(w_1) \sigma_i(r) x_i k(w_2) + k(w_1) \delta_i(r) k(w_2) = k(w_1) (\sigma_i(r) x_i + \delta_i(r)) k(w_2) = k(w_1) (x_i r) k(w_2) = k(w_1 x_i r w_2) = k(w)$, primera igualdad es definición de h , segunda es inducción, tercera y sexta es porque k es morfismo de anillos que deja fijos x_i y R , quinta igualdad es hipótesis 1.

Ahora vemos que $h(p(x_j x_i) a) = h((c_{ij} x_i x_j + \sum_k a_{ij}^k x_k + d_{ij}) a) = (c_{ij} x_i x_j + \sum_k a_{ij}^k x_k + d_{ij}) a = x_j x_i a = h(x_j x_i a)$ tercera y quinta igualdad es porque h es un morfismo de anillos que deja fijos x_i, R , hipótesis 2 es la cuarta igualdad.

Reemplazando a por x_k con $k < i < j$ se tiene condición 3.

Suficiencia

Definimos ahora un producto en $F_R(Mon)$ como $a \star b = h(t(a)t(b))$, se prueba a continuación que $h(ab) = h(a) \star h(b)$, como además conocemos $h(a + b) = h(a) + h(b)$ y h es sobre entonces $A = (F_R(Mon), +, \star)$ es un anillo.

Veamos primero que A resulta una extensión PBW torcida generalizada de R .

Para esto hay que ver que $\iota : R \rightarrow A$ es un endomorfismo inyectivo y Mon es una base de ${}_R A$ estructura inducida por ι , aquí $\iota(r) = r$. Esto es claro si se prueba que $r \star p = rp$ en este caso se vé que la estructura de R módulo inducida por ι coincide con la original, si $p = \Sigma r_x \bar{x}$ como antes entonces $r \star p = h(rt(x)) = \Sigma rr_x \bar{x} = rp$. Además se requiere $x_i \star r = \sigma_i(r)x_i + \delta_i(r)$, si $r = 0$ ambos lados son 0, y si $r \neq 0$ entonces $x_i \star r = h(x_i r) = qp(x_i r) = q(\sigma_i(r)x_i + \delta_i(r)) = \sigma_i(r)x_i + \delta_i$, primera igualdad es definición de \star , tercera es definición de p .

Similarmente si $i < j$, $x_j \star x_i = h(x_j x_i) = c_{ij}x_i x_j + \Sigma_k a_{ij}^k x_k + d_{ij} = c_{ij}x_i \star x_j + \Sigma_k a_{ij}^k x_k + d_{ij}$. Así que para terminar se prueba \square

Lema 3. $h(ab) = h(a) \star h(b)$, para $a, b \in \mathbb{Z} \langle \{x_i \mid i \in I\} \cup R \rangle$.

Para este fin se enuncian

Lema 4. 1. $h(a0b) = 0$.

2. $h(a(-r)b) = -h(arb)$.

3. $h(a(r+s)b) = h(arb + asb)$.

4. $h(a1b) = h(ab)$.

5. $h(a(rs)b) = h(arsb)$.

a, b palabras $r, s \in R$

Nota: La suma, resta, producto 1 y 0 en el lado izquierdo se refieren a las operaciones del anillo R , en el lado derecho suma, resta, 0 se refieren a $\mathbb{Z} \langle \{x_i \mid i \in I\} \cup R \rangle$ y $F_R(Mon)$ si no se indica con paréntesis se entiende producto en $\mathbb{Z} \langle \{x_i \mid i \in I\} \cup R \rangle$ (concatenación), el lema ayuda a evitar ambigüedad (módulo h).

Lema 5. $x, y \in \mathbb{Z} \langle \{x_i \mid i \in I\} \cup R \rangle$, $a, b \in \mathbb{Z}T$.

Si $q(a) = q(b)$ entonces $h(xay) = h(xby)$.

Lema 6. Si $x, y, z \in \mathbb{Z} \langle \{x_i \mid i \in I\} \cup R \rangle$ entonces $h(xp(y)z) = h(xyz)$.

Demostración. Lema 4.

Parte 1 y 2 son consecuencia de 3 pues $r \mapsto h(arb)$ resulta un morfismo del grupo aditivo de R en el grupo aditivo de $F_R(Mon)$.

Se procede a probar 3 por inducción en $c(a(r+s)b)$. Supongamos primero que la primera inversión de $a(r+s)b$ está contenida en b , entonces $b = w_1 x_i t w_2$ con $t \in R$ o $t = x_j$, $i > j$; en este caso $h(a(r+s)b) = h(a(r+s)w_1 p(x_i t) w_2) = h(arw_1 p(x_i t) w_2) + h(arw_1 p(x_i t) w_2) = h(arb) + h(asb)$, primera y tercera igualdad es definición de p y h , y la segunda es inducción. El caso en el que la primera inversión de $a(r+s)b$ está contenida en a es análogo, el caso restante es $a = a'x_i$ y $x_i(r+s)$ es la primera inversión; en este caso $h(a(r+s)b) = h(a'\sigma_i(r+s)x_i b) + h(a'\delta_i(r+s)b) = h(a'(\sigma_i r + \sigma_i s)x_i b) + h(a'(\delta_i r + \delta_i s)b) = h(a'\sigma_i(r)x_i b) + h(a'\delta_i(r)b) + h(a'\sigma_i(s)x_i b) + h(a'\delta_i(s)b) = h(a'x_i r b) + h(a'x_i s b) = h(arb) + h(asb)$ primera y cuarta igualdad es por definición de h , segunda es porque σ_i, δ_i son aditivos en R por hipótesis, y tercera es por inducción y reordenando la suma.

Falta el caso base cuando $a(r+s)b$ no tiene inversiones, en este caso $a = r_1 \dots r_m$, $b = s_1 \dots s_n \bar{x}$ donde $r_k, s_k \in R$ y $\bar{x} \in Mon$, por definición p deja fijos a $a(r+s)b$, arb , y asb ;

y $h(a(r+s)b) = (\prod r_k(r+s)\prod s_k)\bar{x} = (\prod r_k r \prod s_k)\bar{x} + (\prod r_k s \prod s_k)\bar{x} = h(arb) + h(asb)$.

El caso base en 4 y 5 son similares y también los casos en el que la primera inversión está en a o b . Solo hago el caso $a = a'x_i$, $x_i(rs)$ o x_i1 es la primera inversión: $h(a1b) = h(a'\sigma_i(1)x_ib) + h(a'\delta_i(1)b) = h(a'1x_ib) + h(a'0b) = h(a'x_ib) = h(ab)$, aquí usamos definición de h , inducción y parte 1 ya probadas, además se usa $\sigma_i(1) = 1$ por hipótesis en σ_i y que $\delta_i(1) = 0$, ver la discusión despues de la definición 8.

Finalmente

$$\begin{aligned} h(a'x_i(rs)b) &= h(a'\sigma_i(rs)x_ib) + h(a'\delta_i(rs)b) = h(a'(\sigma_i(r)\sigma_i(s))x_ib) + h(a'(\sigma_i(r)\delta_i(s) + \\ &\delta_i(r)s)b) = h(a'\sigma_i(r)\sigma_i(s)x_ib) + h(a'\sigma_i(r)\delta_i(s)b) + h(a'\delta_i(r)sb) = \\ &h(a'\sigma_i(r)x_isb) + h(a'\delta_i(r)sb) = h(a'x_i rsb) = h(arsb) \end{aligned}$$

Primera, cuarta y quinta igualdad es definición de h , segunda igualdad son las hipótesis en σ_i y δ_i y tercera igualdad es la parte 3 ya probada e inducción (3 veces). \square

Demostración. El lema 4 implica el lema 5.

$a = \sum_k z_k r_{k1} \dots r_{km(k)} x_{i_{k1}} \dots x_{i_{kn(k)}}$ suma es sobre k finito, z_k es entero, $m(k), n(k) \geq 0$ son enteros, $r_{kn} \in R$ para todo k y $1 \leq n \leq m(k)$, $i_{kn} \in I$ para todo k y $1 \leq n \leq n(k)$.

Escribamos $tq(a) = \sum_{\bar{i} \in A} (\sum_{k \in L_{\bar{i}}} s_k) x_{i_1} \dots x_{i_n}$, donde se denota $\bar{i} = (i_1, \dots, i_n)$ con $i_1, \dots, i_n \in I$, $L_{\bar{i}} = \{k : (i_{k1} \dots i_{kn(k)}) = \bar{i}\}$, $s_k = z_k \prod_{s=1}^{m(k)} r_{ks} \in R$ y $A = \{\bar{i} \mid \sum_{k \in L_{\bar{i}}} s_k \neq 0\}$.

Es claro que existe una sucesión finita $a = a_0, a_1, \dots, a_n = tq(a)$ de elementos en $\mathbb{Z}T$ que cumple $a_l = w + (rs)f$, $a_{l-1} = w + rsf$; o $a_l = w + 1f$, $a_{l-1} = w + f$; o $a_l = w + (r+s)f$, $a_{l-1} = w + rf + sf$; o $a_l = w + (-r)f$, $a_{l-1} = w - rf$; o $a_l = w$, $a_{l-1} = w + 0f$. Aquí f es una palabra $w \in \mathbb{Z}T$ y r y s pertenecen a R ; x, r, s, w dependen de l .

Vemos ahora que $h(xa_l y) = h(x(w + (rs)f)y) = h(xwy) + h(x(rs)f y) = h(xwy) + h(xrsf y) = h(x(w + rsf)y) = h(xa_{l-1} y)$ aquí x, y son palabras; se usa que h es lineal por definición y el lema 4. Los otros casos para a_l, a_{l-1} corresponden a los otros puntos del lema 4.

Se concluye $h(xay) = h(xa_0 y) = h(xa_1 y) = \dots = h(xa_n y) = h(xtq(a)y)$, para x, y palabras; pero como la identidad es lineal en x, y , esto es cierto para $x, y \in \mathbb{Z} < \{x_i \mid i \in I\} \cup R >$, de aquí es claro el lema 5. \square

Demostración. El lema 5 implica el lema 6.

Empezamos notando que la identidad es lineal en x, y, z luego se pueden asumir que son palabras.

A continuación procedemos por inducción en $c(xyz)$.

Supongamos primero que la primera inversión (de derecha a izquierda) en xyz está contenida en z , $z = w_1 x_j s w_2$ con $s \in R$, o, $s = x_i$ y $i < j$; entonces por definición $p(xyz) = p(xy w_1 p(x_j s) w_2)$ inducción aplica en (x, y, z') , z' es palabra en $w_1 p(x_j s) w_2$, así que $h(xyz) = h(xp(y) w_1 p(x_j s) w_2) = h(xp(y) z)$, la segunda igualdad es por la definición de h .

Supongamos ahora que la primera inversion de xyz está contenida por completo en y , $y = w_1 x_j s w_2$, s como antes; $h(xyz) = h(xw_1 p(x_j s) w_2 z) = h(xp(w_1 p(x_j s) w_2) z) = h(xp(y) z)$ primera y tercera igualdad es definición de h , segunda es inducción para (x, y', z) con y' palabra en $w_1 p(x_j s) w_2$.

Si no hay inversiones, o tienen parte en x entonces y es ordenado y $p(y) = y$.

Finalmente se tiene el caso $y = y'x_j$, $z = sz'$, j, s como antes. Suponemos primero que la primera inversión de y está contenida en y' , de forma que $y' = w_1x_k s'w_2$, en este caso se tiene

$$\begin{aligned} h(xyz) &= h(xy'p(x_j s)z') = h(xp(y')p(x_j s)z') = h(xp(w_1p(x_k s')w_2)p(x_j s)z') = \\ &h(xw_1p(x_k s')w_2p(x_j s)z') = h(xw_1p(x_k s')w_2x_jsz') = h(xp(w_1p(x_k s')w_2)z) = h(xp(y)z), \end{aligned}$$

la primera, tercera, quinta y séptima igualdad son de la definición de p . La segunda igualdad es inducción en (x, y', z_1) z_1 es palabra en $p(x_j s)z'$, la cuarta igualdad es inducción en (x, y_1, z_1) , y_1 es palabra en $w_1p(x_k s')w_2$, la sexta igualdad es inducción en (x, y_1, z) . El último caso es $y = y'x_kx_j$, $z = sz'$, (x_j, s) como antes (una inversión). En este caso

$$\begin{aligned} h(xyz) &= h(xy'x_kp(x_j s)z') = h(xy'p(x_kp(x_j s))z') = h(xy'p(p(x_kx_j)s)z') = \\ &h(xy'p(x_kx_j)sz') = h(xp(y'p(x_kx_j))z) = h(xp(y)z). \end{aligned}$$

Aquí la primera y sexta igualdad son de la definición de p , la segunda igualdad es inducción en (xy', y_1, z') , y_1 una palabra en $x_kp(x_j s)$, la cuarta igualdad es inducción en (xy', y_2, z') , y_2 palabra en $p(x_kx_j)s$, la quinta es inducción en (x, y_3, z) , y_3 palabra en $y'p(x_kx_j)$, y la tercera igualdad es gracias al lema 5, pues

$$qp(x_kp(x_j s)) = h(x_kp(x_j s)) = h(p(x_kx_j)s) = qp(p(x_kx_j)s)$$

la segunda igualdad aquí son las hipótesis 2 y 3 en el teorema 4. \square

Para terminar la parte de suficiencia en el teorema:

Demostración. Lema 5 y lema 6 implica lema 3.

$h(a) \star h(b) = h(tpp(a)tpp(b)) = h(p(a)p(b)) = h(ab)$, primera igualdad es definición de \star , segunda igualdad es lema 5 dos veces ($qtqp(a) = qp(a)$ pues qt es identidad, igual con b), y tercera igualdad es lema 6 aplicado dos veces. \square

Demostración. Universalidad en el teorema 4.

Llamamos $B = \mathbb{Z} \langle \{x_i \mid i \in I\} \cup R \rangle / G$ donde G es el ideal bilátero generado por:

1. para $r, s \in R$
 - (a) $(rs) - (r)(s)$.
 - (b) $(r) + (s) - (r + s)$.
 - (c) $1 - (1)$.
2. $x_i r - \sigma_i(r)x_i + \delta_i(r)$, para $r \in R, i \in I$.
3. $x_j x_i - c_{ij}x_i x_j - \sum_k a_{ij}^k x_k - d_{ij}$, para $i < j$ en I .

$R \rightarrow B$ claramente cumple la propiedad universal deseada, nótese que los generadores en 1 de G son exactamente los que hacen que esta función sea un morfismo de anillos. Probamos ahora que $\bar{h} : B \rightarrow A$ es biyección, notar primero que \bar{h} es la factorización de h a travez

del mapa cociente $\pi : \mathbb{Z} \langle \{x_i \mid i \in I\} \cup R \rangle \rightarrow B$ y está bien definida pues h anula los generadores de G .

\bar{h} tiene inverso por derecha πt , $\bar{h}\pi t = ht = 1$. Vemos que πt es inverso por izquierda, es decir $x = th(x) \pmod{G}$ para $x \in \mathbb{Z} \langle \{x_i \mid i \in I\} \cup R \rangle$, esto se hace en dos pasos:

Primero ver que $x = p(x) \pmod{G}$ para $x \in \mathbb{Z} \langle \{x_i \mid i \in I\} \cup R \rangle$, como esto es lineal en x basta para x palabra, y se usa inducción en $c(x)$: si x no tiene inversiones $p(x) = x$ es inmediato, si $x = w_1 x_i r w_2$, $x_i r$ la primera inversión de x , $r \in R$, se tiene $p(x) = p(w_1 \sigma_i(r) x_i w_2) + p(w_1 \delta_i(r) w_2) = w_1 \sigma_i(r) x_i w_2 + w_1 \delta_i(r) w_2 = w_1 x_i r w_2 = x \pmod{G}$, primera igualdad es definición de p , segunda es inducción, y tercera es por el numeral 2 en la definición de G . Similarmente si $x = w_1 x_j x_i w_2$ la conclusión se obtiene del numeral 3 en definición de G .

El segundo paso es ver $a = tq(a) \pmod{G}$ si $a \in \mathbb{Z}T$, si esto se tiene entonces $x = p(x) = tqp(x) = th(x) \pmod{G}$ como se requiere. Para ver $y = tq(y) \pmod{G}$, se recuerda la discusión de la prueba del lema 5, $a = a_0 = \dots = a_n = tq(a) \pmod{G}$ basta ver por ejemplo $a_k = r + (a + b)x = r + ax + bx = a_{k-1} \pmod{G}$ que se obtiene de multiplicar el numeral 1.b en la definición de G por x y sumar r , similarmente $(-r) = -(r) \pmod{G}$, $(0) = 0 \pmod{G}$, $(ab) = (a)(b) \pmod{G}$, $(1) = 1 \pmod{G}$, prueba los otros casos, las dos primeras identidades son consecuencia de 1.b pues bajo esta condición $R \rightarrow B$ es un morfismo de los grupos aditivos. □

Notamos que en la prueba de suficiencia las condiciones 2 y 3 solo se usan en la parte final de la prueba del lema 6, la condición 1 solo se usa en la prueba del lema 4.

De aquí se puede obtener un refinamiento que consiste en considerar las palabras en x_i y M , M un conjunto que genere a R como anillo, la complejidad $d(w) = (a, b, c)$, a, b como en la definición 11 pero $c = (c_1, \dots, c_a) \in \mathbb{N}^a$ definido por: si x_i es el k -ésimo objeto de la forma x_j , de derecha a izquierda en w , $x_i = w_s$ entonces $c_k = \text{card}\{r : w_r \in M, r > s\}$, estas tuplas ordenadas lexicográficamente forman un buen orden como antes. En lugar de d se puede tomar cualquier función con valores en un conjunto bien ordenado que disminuya al permutar una inversión de acuerdo con las reglas de conmutación.

La inducción en el lema 6 es igual reemplazando $r \in R$ por $r \in M$ y haciendo uso del lema 4.

Se obtiene:

Corolario 1. *Si M genera a R como anillo y con la notación del teorema 4 una condición suficiente para la existencia de una extensión PBW torcida generalizada como en el teorema son las condiciones 1 y 3 allí descritas junto con*

$$2' \quad h(x_j x_i a) = h(p(x_j x_i) a) \text{ para } i < j \text{ y } a \in M.$$

Vemos que el teorema 4 generaliza la construcción usual del anillo de polinomios torcidos $R[x, \sigma, \delta]$, en seguida se ve también que generaliza el teorema de Poincare-Birkhoff-Witt.

Ejemplo 1. Tomemos k un anillo conmutativo y V un k -módulo equipado con una función $[\cdot, \cdot] : V \times V \rightarrow V$, bilineal, que a un par $v_1, v_2 \in V$ le asocia $[v_1, v_2] \in V$. $(V, [\cdot, \cdot])$ se llama una k -álgebra de Lie si

1. $[v, v] = 0$ para todo $v \in V$.
2. $[v_1, [v_2, v_3]] + [v_2, [v_3, v_1]] + [v_3, [v_1, v_2]] = 0$ para cualesquiera v_1, v_2 y v_3 elementos de V .

A toda k -álgebra asociativa A se le puede asociar una k -álgebra de Lie dada por $[a, b] = ab - ba$.

A toda álgebra de Lie V se le puede asociar una única álgebra asociativa A y un morfismo de álgebras de Lie $\phi : V \rightarrow A$ (donde A se toma como álgebra de Lie con la estructura definida anteriormente) que cumple la propiedad universal:

Si B es un álgebra asociativa y $f : V \rightarrow B$ es un morfismo de álgebras de Lie (donde B se toma como álgebra de Lie con la estructura definida anteriormente) entonces existe un punico morfismo de álgebras $F : A \rightarrow B$ tal que $F\phi = f$.

Esta álgebra asociativa se denomina el álgebra envolvente del álgebra de Lie V .

El teorema de Poincare-Birkhoff-Witt dice que si V es un k -módulo libre con base $\{x_i \mid i \in I\}$ con I un conjunto totalmente ordenado entonces A es un k -módulo libre con base $\text{Mon}(\{\phi(x_i) \mid i \in I\})$.

Para ver esto como consecuencia del teorema 4 observamos que para $i < j$ y $r \in k$ se tiene $\phi(x_i)r = r\phi(x_i)$ y $\phi(x_j)\phi(x_i) = \phi(x_i)\phi(x_j) + \phi([x_j, x_i])$, así que la consecuencia del teorema PBW dice que A es una extensión PBW torcida generalizada de k .

Recíprocamente si una extensión PBW torcida generalizada A que cumple estas dos ecuaciones existe, entonces por la propiedad universal en el teorema 4 A es el álgebra envolvente de V .

Para terminar sólo hay que verificar las hipótesis del teorema con las dos ecuaciones:

La primera condición se tiene pues la identidad de k , id_k , es un endomorfismo de k y la función constante a cero es una id_k -derivación.

Para la segunda condición se calcula $h(x_j x_i r) = h(x_j r x_i) = h(r x_j x_i) = r x_i x_j + r[x_j, x_i]$ y por otro lado $h(p(x_j x_i) r) = h(x_i x_j r) + h([x_j, x_i] r) = h(x_i r x_j) + r[x_j, x_i] = r x_i x_j + r[x_j, x_i]$ y se verifica $h(x_j x_i r) = h(p(x_j, x_i) r)$.

Para la tercera condición se calcula

$$h(x_k x_j x_i) = h(x_k x_i x_j) + h(x_k [x_j, x_i]) = h(x_i x_k x_j) + h([x_k, x_i] x_j) + h(x_k [x_j, x_i]) = x_i x_j x_k + h(x_i [x_j, x_k]) + h([x_k, x_i] x_j) + h(x_k [x_j, x_i])$$

y por otro lado

$$\begin{aligned} h(p(x_k x_j) x_i) &= h(x_j x_k x_i) + h([x_j, x_k] x_i) = h(x_j x_i x_k) + h(x_j [x_i, x_k]) + h([x_j, x_k] x_i) = \\ &= x_i x_j x_k + h([x_j, x_i] x_k) + h(x_j [x_i, x_k]) + h([x_j, x_k] x_i) = x_i x_j x_k + (h(x_k [x_j, x_i]) + \\ &+ h([x_j, x_i], x_k)) + (h([x_i, x_k] x_j) + h([x_i, x_k], x_j)) + (h(x_i [x_j, x_k]) + h([x_j, x_k], x_i)) = \\ &= h(x_k x_j x_i) + h([x_j, x_i], x_k) + [[x_i, x_k], x_j] + [[x_j, x_k], x_i] = h(x_k x_j x_i) \end{aligned}$$

donde la última igualdad es consecuencia de la segunda condición en la definición de álgebra de Lie.

2.2. Extensión del anillo de coeficientes

En esta sección usamos el teorema 4 para examinar el caso en el que A es una extensión PBW torcida generalizada de R y B es una extensión de R , y dar una construcción general para extender A a una extensión PBW torcida generalizada de B .

Primero damos una definición que es útil para la construcción de anillos con propiedades universales prescritas.

Definición 13. Dado un anillo A y un conjunto X , $A_l \langle X \rangle := \mathbb{Z} \langle X \cup A \rangle / I$ donde I es el ideal bilátero generado por

1. $(rs) - (r)(s)$.
2. $(r) + (s) - (r + s)$.
3. $1 - (1)$.

Para $r, s \in A$. $A_l \langle X \rangle$ está caracterizado por la propiedad universal $\iota : A \rightarrow A_l \langle X \rangle$ es un morfismo de anillos y si $f : A \rightarrow B$ es un morfismo de anillos y $g : X \rightarrow B$ es una función entonces existe un único morfismo de anillos $F : A_l \langle X \rangle \rightarrow B$ con $F\iota = f$ y $Fx = gx$ para $x \in X$. $A_l \langle X \rangle$ se denomina la extensión libre de A por X .

Si $\{r_\alpha\} \subset \mathbb{Z} \langle X \cup A \rangle$ entonces $B = \mathbb{Z} \langle X \cup A \rangle / (I + J)$ con J el ideal bilátero generado por $\{r_\alpha\}$ se llama la extensión de A con generadores X y relaciones $\{r_\alpha\}$. Este anillo cumple una propiedad universal análoga.

Ya se vió un ejemplo en la demostración del teorema 4, presentamos un segundo ejemplo.

Ejemplo 2. R un anillo y $S \subset R$, se define $R(S^{-1})$ como la extensión libre de R con generadores x_s un símbolo para cada $s \in S$ y relaciones $x_s s = s x_s = 1$. Este anillo cumple la propiedad universal:

1. $\phi : R \rightarrow R(S^{-1})$ es un morfismo de anillos tal que $\phi(s)$ es invertible en $R(S^{-1})$ para todo $s \in S$.
2. Si $f : R \rightarrow B$ es un morfismo de anillos tal que $f(s)$ es invertible en B para todo $s \in S$, entonces existe un único $F : R(S^{-1}) \rightarrow B$ tal que $F\phi = f$.

En efecto la imagen de x_s en $R(S^{-1})$ denotada por abuso de notación x_s es un inverso multiplicativo de $\phi(s)$ en $R(S^{-1})$ luego el primer ítem es válido.

Para el segundo ítem observamos que la función F cumple necesariamente

$$F(x_s) = F(\phi(s))^{-1} = f(s)^{-1},$$

luego es única porque $\{x_s \mid s \in S\} \cup \phi(R)$ genera a $R(S^{-1})$ como anillo. Y F existe por que $f = H\iota$ donde $\iota : R \rightarrow R_l \langle \{x_s \mid s \in S\} \rangle$, $H : R_l \langle \{x_s \mid s \in S\} \rangle \rightarrow B$ y $H(x_s) = f(s)^{-1}$; observamos entonces que $H(x_s \iota(s) - 1) = 0$ y $H(\iota(s)x_s - 1) = 0$ luego $H(J) = 0$ donde I es el ideal de $R_l \langle \{x_s \mid s \in S\} \rangle$ tal que $R_l \langle \{x_s \mid s \in S\} \rangle / J = R(S^{-1})$ (véase la definición anterior), luego existe $F : R(S^{-1}) \rightarrow B$ tal que $F\pi = H$ donde

$\pi : R_l \langle \{x_s \mid s \in S\} \rangle \rightarrow R(S^{-1})$ es la proyección canónica; luego $H\iota = F\pi\iota = F\phi$ como se afirma.

Por supuesto cuando S es un conjunto de Ore de R por la izquierda se tiene $RS^{-1} \cong R(S^{-1})$.

Como otro ejemplo (sin detalles) mencionamos que con una construcción similar se puede probar la existencia del álgebra envolvente de Lie del ejemplo 1, en efecto para el álgebra de Lie V el álgebra envolvente asociada es la k -álgebra con generadores $\{x_v \mid v \in V\}$ y relaciones $x_{v+w} - x_v - x_w$, $x_{rv} - rx_v$ y $x_vx_w - x_wx_v - x_{[v,w]}$, para $v, w \in V$ y $r \in k$.

Proposición 3. *K es un anillo conmutativo, X un conjunto y $f : X \rightarrow K \langle X \rangle$ es una función entonces existe un único endomorfismo f_1 de $K \langle X \rangle$ tal que $f_1(ra) = rf_1(a)$ para $a \in K \langle X \rangle$, $r \in K$; y $f_1x = fx$ para $x \in X$.*

$h : X \rightarrow K \langle X \rangle$ es una función, entonces existe una única f_1 -derivación h_1 en $K \langle X \rangle$ tal que $h_1(ra) = rh_1(a)$ para $a \in K \langle X \rangle$ y $r \in K$; y $h_1x = hx$ para $x \in X$.

Demostración. La primera afirmación se obtiene tomando $f_1(x_{i_1} \cdots x_{i_n}) = f(x_{i_1}) \cdots f(x_{i_n})$ y extensión K -lineal.

Para la derivación se define $h_1(\bar{x})$ para \bar{x} una palabra en X por inducción en la longitud de la palabra:

$h_1(1) = 0$ para la palabra vacía. $h_1(\bar{x}y) := f_1(\bar{x})h(y) + h_1(\bar{x})y$ por inducción. Y $h_1 : K[X] \rightarrow K[X]$ es la extensión K -lineal, esto prueba incidentalmente unicidad.

Cuando $\bar{x} = 1$ es la palabra vacía entonces observamos $h_1y = hy$ para $y \in X$.

Falta probar que $h_1(xy) = f_1(x)h_1(y) + h_1(x)y$ como esto es K -lineal en x, y basta suponer x, y palabras.

Se procede por inducción en la longitud de y , si $y = 1$ esto es cierto; supongamos $y = y'z$ con $z \in X$, entonces $h_1(xy'z) = f_1(xy')h(z) + h_1(xy')z = f_1(x)f_1(y')h(z) + f_1(x)h_1(y')z + h_1(x)y'z = f_1(x)h_1(y) + h_1(x)y$ en la primera igualdad se usa la definición de h_1 en (xy', z) , en la segunda se usa inducción para (x, y') y en la tercera se usa la definición de h_1 en (y', z) . \square

Proposición 4. *Con la notación de la proposición 3 $\{r_\alpha\} \subset K \langle X \rangle$, I el ideal bilátero en $K \langle X \rangle$ generado por los r_α , $A = K \langle X \rangle / I$. Si $f_1(r_\alpha) = 0 \pmod I$ entonces existe un único K -endomorfismo f_2 de A con $f_2(x + I) = f(x) + I$ para $x \in X$.*

Si además $h_1(r_\alpha) = 0 \pmod I$ entonces existe una única f_2 -derivación h_2 en A tal que $h_2(x + I) = h(x) + I$ para $x \in X$.

Demostración. f_2 y h_2 son la factorización por el cociente $K \langle X \rangle \rightarrow A$ de f_1 y h_2 respectivamente. La ecuación $h_1(ab) = f_1(a)h_1(b) + h_1(a)b$ produce $h_2(\bar{a}\bar{b}) = f_2(\bar{a})h_2(\bar{b}) + h_2(\bar{a})\bar{b}$.

Para terminar hay que probar que f_2 y h_2 están bien definidas, como son aditivas basta ver que $f_1(I) \subset I$ y $h_1(I) \subset I$, pero $f_1^{-1}(I)$ es un ideal bilátero por ser f_1 un endomorfismo, y contiene a r_α por hipótesis, luego se concluye $I \subset f_1^{-1}(I)$ como se requiere. Similarmente se prueba que $J = h_1^{-1}(I) \cap f_1^{-1}(I) \cap I$ es un ideal bilátero: J es un subgrupo aditivo; y si $h_1(a) = 0 = f_1(a) = a \pmod I$ y $b \in A$ entonces $h_1(ab) = f_1(a)h_1(b) + h_1(a)b = 0 \pmod I$,

$f_1(ab) = f_1(a)f_1(b) = 0 \pmod I$ y $ab = 0 \pmod I$ entonces $ab \in J$. De la misma forma si $b \in J$ y $a \in A$ entonces $ab \in J$ y J es ideal bilátero. Como $r_\alpha \in J$ entonces $I \subset J$. \square

Proposición 5. *Si σ es un endomorfismo de A y $f : X \rightarrow A_l \langle X \rangle$ es una función entonces existe un único endomorfismo g de $A_l \langle X \rangle$ tal que $g\iota = \sigma$ y $gx = fx$ para $x \in X$.*

Si δ es una σ -derivación en A y $h : X \rightarrow A_l \langle X \rangle$ es una función, entonces existe una única g -derivación d en $A_l \langle X \rangle$ tal que $d\iota = \delta$ y $dx = hx$ para $x \in X$.

Demostración. Sean G como en la definición 13 y $\pi : \mathbb{Z} \langle X \cup A \rangle \rightarrow A_l \langle X \rangle$ la proyección canónica.

$\tilde{f} : A \cup X \rightarrow \mathbb{Z} \langle X \cup A \rangle$ es tal que $\pi\tilde{f}$ es f en X y es σ en A . $\tilde{h} : A \cup X \rightarrow \mathbb{Z} \langle X \cup A \rangle$ es tal que $\pi\tilde{h}$ es h en X y es δ en A . (\tilde{g}, \tilde{d}) es una derivación de $\mathbb{Z}[X \cup A]$ que extiende a (\tilde{f}, \tilde{h}) , como en la proposición 3 para terminar por el teorema se prueban las condiciones de la proposición 4: por ejemplo $\pi\tilde{g}((r)(s)) = \pi\tilde{g}(rs)$ para $r, s \in R$, en efecto $\pi\tilde{g}((r)(s)) = \pi\tilde{f}(r)\pi\tilde{f}(s) = \sigma(r)\sigma(s) = \sigma(rs) = \pi\tilde{g}(rs)$; σ aditivo y preserva el uno son las otras dos condiciones, y también es necesario $\pi\tilde{d}((r)(s)) = \pi\tilde{f}(r)\pi\tilde{h}(s) + \pi\tilde{h}(r)\pi(s) = \sigma(r)\delta(s) + \delta(r)s = \delta(rs) = \pi\tilde{d}(rs)$. que δ es aditivo y $\delta(1) = 0$ son las otras dos condiciones. \square

Corolario 2. *$A, X, \sigma, \delta, f, g, h, d$ como antes. $\{r_\alpha\} \subset A_l \langle X \rangle$, I el ideal bilátero en $A_l \langle X \rangle$ generado por los r_α , $B = A_l \langle X \rangle / I$, $\phi : R \rightarrow B$ canónico. Si $g(r_\alpha) = 0 = d(r_\alpha) \pmod I$ entonces existe una única derivación (σ_1, δ_1) en B tal que $\sigma_1\phi = \phi\sigma, \delta_1\phi = \phi\delta, \sigma_1(x + I) = f(x) + I$ y $\delta_1(x + I) = h(x) + I$ para $x \in X$*

Demostración. De las dos proposiciones anteriores. \square

Este último corolario es uno de los objetivos de la sección.

Ejemplo 3. Como un ejemplo que constituyó una de las motivaciones principales del último resultado mencionamos el caso $B = R[x, \sigma, \delta]$, por la propiedad universal de B observamos que B es la extensión de R con generador x y relación $xr = \sigma(r)x + \delta(r)$.

Dado una segunda derivación $(\sigma_1, \delta_1) : R \rightarrow R$, es común buscar extender a una derivación $(\sigma_2, \delta_2) : R[x, \sigma, \delta] \rightarrow R[x, \sigma, \delta]$ con valores prescritos $\sigma_2(x) = a \in R[x, \sigma, \delta]$ y $\delta_2(x) = b \in R[x, \sigma, \delta]$. Condiciones evidentes necesarias para la existencia de (σ_2, δ_2) pueden obtenerse de aplicar σ_2 y δ_2 a la identidad $xr = \sigma(r)x + \delta(r)$. El corolario implica que estas condiciones son suficientes y la derivación obtenida (σ_2, δ_2) es única.

Como una ilustración calculamos explícitamente las condiciones necesarias y suficientes para la existencia de (σ_2, δ_2) con $\sigma_2(x) = x$ y $\delta_2(x) = 0$. En este caso $\sigma_2(xr) = x\sigma_1(r) = \sigma(\sigma_1(r))x + \delta(\sigma_1(r))$ y por otro lado $\sigma_2(\sigma(r)x + \delta(r)) = \sigma_1(\sigma(r))x + \sigma_1(\delta(r))$ de donde obtenemos $\sigma\sigma_1 = \sigma_1\sigma$ y $\delta\sigma_1 = \sigma_1\delta$. Análogamente $\delta_2(xr) = \sigma_2(x)\delta_2(r) + \delta_2(x)r = x\delta_1(r) = \sigma(\delta_1(r))x + \delta(\delta_1(r))$ y por otro lado $\delta_2(\sigma(r)x + \delta(r)) = \sigma_2(\sigma(r))\delta_2(x) + \delta_2(\sigma(r))x + \delta_2(\delta(r)) = \delta_1(\sigma(r))x + \delta_1(\delta(r))$, de donde obtenemos $\sigma\delta_1 = \delta_1\sigma$ y $\delta\delta_1 = \delta_1\delta$. De forma que la derivación (σ_2, δ_2) que extiende a (σ_1, δ_1) y cumple $\sigma_2(x) = x$ y $\delta_2 = 0$ existe si, y sólo si, las dos funciones en (σ, δ) conmutan con las dos funciones en (σ_1, δ_1) .

Por supuesto se puede tomar en lugar de $R[x, \sigma, \delta]$ una extensión PBW torcida generalizada, con resultados similares.

Ejemplo 4. Tomemos $\phi : R \rightarrow R(S^{-1})$ como en el ejemplo 2, y tomemos (σ, δ) una derivación de R tal que $\sigma(S) \subseteq S$.

Entonces existen una única derivación (σ_1, δ_1) de $R(S^{-1})$ tal que $\sigma_1\phi = \phi\sigma$ y $\delta_1\phi = \phi\delta$. En efecto suponiendo que existen se tiene que $\sigma_1(x_s) = \sigma_1(\phi(s)^{-1}) = \sigma_1(\phi(s))^{-1} = \phi(\sigma(s))^{-1}$ y de aplicando δ_1 a la ecuación $x_s\phi(s) = 1$ se obtiene $\delta_1(x_s\phi(s)) = \sigma_1(x_s)\delta_1(\phi(s)) + \delta_1(x_s)s = \phi(\sigma(s))^{-1}\phi(\delta(s)) + \delta_1(x_s)\phi(s) = 0 = \delta_1(1)$ luego $\delta_1(x_s) = -\phi(\sigma(s))^{-1}\phi(\delta(s))\phi(s)^{-1}$ luego el corolario 2 garantiza unicidad.

Si ahora prescribimos los valores (con la notación de el corolario 2) $f(x_s) = \phi(\sigma(s))^{-1}$ y $h(x_s) = -\phi(\sigma(s))^{-1}\phi(\delta(s))\phi(s)^{-1}$ entonces se tiene $g(x_s\phi(s)) = g(\phi(s)x_s) = g(1)$ y $d(x_s\phi(s)) = d(\phi(s)x_s) = d(1)$ por un argumento esencialmente idéntico al del párrafo anterior.

Luego se tiene existencia por la misma proposición.

Nota: De la prueba observamos que es suficiente la hipótesis más débil $\phi(\sigma(s))$ es invertible en $R(S^{-1})$.

Proposición 6. B, R son anillos y $\phi : R \rightarrow B$ es un morfismo de anillos. $M \subset B$ es tal que $\phi(R) \cup M$ generan a B como anillo. Sea A es una extensión PBW torcida generalizada de R con

1. $x_i r = \sigma_i(r)x_i + \delta_i(r)$. Para $i \in I$ y $r \in R$
2. $x_j x_i = c_{ij}x_i x_j + \sum_k a_{ij}^k x_k + d_{ij}$, para $i < j$ en I .

h como en la definición 12.

Supongamos además (σ'_i, δ'_i) es una derivación de B con $\sigma'_i\phi = \phi\sigma_i$ y $\delta'_i\phi = \phi\delta_i$.

Entonces existe C extensión PBW torcida generalizada de B con

1. $x'_i r = \sigma'_i(r)x_i + \delta'_i(r)$. Para $i \in I$ y $r \in B$
2. $x'_j x'_i = \phi(c_{ij})x'_i x'_j + \sum_k \phi(a_{ij}^k)x'_k + \phi(d_{ij})$, para $i < j$ en I .

si, y sólo si,

a $h'(x_j x_i a) = h'(p'(x_j x_i) a)$ para $i < j$ y $a \in M$.

h' es la función en la definición 12 con parametros las imágenes por ϕ de los correspondientes parámetros de h .

Demostración. Es consecuencia del corolario 1, condicion 1 está en la hipótesis, condición 2 para $\phi(a) \in \phi(R)$ y condición 3 se heredan de A . \square

2.3. Aplicaciones

En esta sección presentamos dos aplicaciones de las dos secciones anteriores.

Proposición 7. *Si A es una extensión PBW generalizada de R entonces $Gr(A)$, el graduado de A respecto a la filtración estándar, es una extensión quasiconmutativa de R . $Gr(A)$ es finita si A es finita y biyectiva si A es biyectiva.*

Demostración. Dotamos a A de la filtración estándar, $\{A_n\}_{n \in \mathbb{N}}$ y vamos a ver que A_n es el conjunto de sumas de elementos de la forma $r\bar{x}$ donde $r \in A$ y \bar{x} es un monomio en X con m indeterminadas $m \leq n$. En efecto, llamemos B_n a el conjunto cuyos elementos son sumas de elementos de la forma $r\bar{x}$ donde $r \in A$ y \bar{x} es un monomio en X con m indeterminadas $m \leq n$. De la definición de la filtración estándar todo elemento en A_{n+1} es una suma de elementos de la forma rx_ia donde $a \in A_n$, si asumimos por inducción que $a \in B_n$ entonces como B_n es cerrado por sumas y multiplicación por elementos de R a izquierda, basta observar que $x_i r \bar{x} = \sigma_i(r)x_i \bar{x} + \delta_i(r)\bar{x} \in B_{n+1}$ para $r \in R$ y \bar{x} un monomio como en la definición de B_{n+1} . Finalmente observamos por inducción en el número de variables en \bar{x} que $x_i \bar{x} = c\bar{x}' + d$ donde $c \in R$, \bar{x}' es el único monomio que tiene exactamente las variables en \bar{x} y un x_i adicional, d es suma de elementos de la forma $t\bar{y}$ con $t \in R$ y \bar{y} con menos variables que \bar{x} .

De aquí se sigue fácilmente que ${}_R Gr(A)$ es libre con base los monomios estándar en x'_i , donde $x'_i \in A_1/A_0 \subseteq Gr(A)$ es la imagen de x_i . Las otras condiciones en la definición de extensión PBW torcida generalizada quasiconmutativa para $Gr(A)$ son inmediatas.

Es claro que si A es finita entonces $Gr(A)$ es finita y si A es biyectiva entonces $Gr(A)$ también es biyectiva (pues tiene los mismos endomorfismos asociados). \square

Proposición 8. *Sea $A = \sigma(R)[X]$ es una extensión PBW generalizada quasiconmutativa de R . Para $i \in I$ sean $X_i^- = \{x_j \mid j < i\}$ y $X_i = \{x_j \mid j \leq i\}$, entonces los R -submódulos de ${}_R A$ generados por $Mon(X_i^-)$ y $Mon(X_i)$ son subanillos de A , y si se denotan A_i^- y A_i , se tiene que existe una única extensión (σ'_i, δ'_i) de la derivación (σ_i, δ_i) a A_i^- tal que $A_i = A_i^-[x_i, \sigma'_i, \delta'_i]$. Adicionalmente si A es biyectiva entonces σ'_i es biyectiva. Si A es finita existe una sucesión finita $\phi(R) = A_0 \subseteq \dots \subseteq A_n = A$ tal que $A_i = A_{i-1}[x_i, \sigma'_i, \delta'_i]$. Si A es finita y biyectiva, entonces σ'_i es biyectiva.*

Demostración. Llamamos A_J el R -submódulo de ${}_R A$ generado por monomios de $X_J = \{x_j \mid j \in J\}$ donde $J \subseteq I$. Para ver que A_J es un subanillo basta ver que $r_1 \bar{x}_1 r_2 \bar{x}_2 \in A_J$ para $r_1, r_2 \in R$ y $\bar{x}_1, \bar{x}_2 \in Mon(X_J)$, multiplicando los términos en $r_2 \bar{x}_2$ con $r_1 \bar{x}_1$ y recordando que A_J es un R -módulo izquierdo vemos que basta observar $\bar{x}r \in A_J$ y $\bar{x}x_j \in A_J$ para $r \in R, j \in J$ y $\bar{x} \in Mon(X_J)$.

Pero observamos que $\bar{x}r = \sigma(r)\bar{x}$ con σ un endomorfismo y $\bar{x}x_j = \bar{x}'x_jx_j = \bar{x}'c_{ji}x_jx_i = \sigma'(c_{ji})\bar{x}'x_jx_i$ y se concluye por inducción en la longitud de \bar{x} que $\bar{x}x_i = r\bar{y}$ donde $r \in R$ y \bar{y} es el único monomio que contiene sólo a los términos de \bar{x} y a x_i .

Es claro que A_i es una extensión PBW torcida generalizada con una variable x_i de A_i^- . Falta por ver que es biyectiva si A es biyectiva.

Para ver esto se toma $\tau : A_i^- \rightarrow A_i^-$ el endomorfismo determinado por $\tau\phi = \sigma_i^{-1}$ y $\tau(x_j) = \sigma_i^{-1}(c_{ji}^{-1})x_j$, para se tiene que $\tau = \sigma_i'^{-1}$ pues $\tau\sigma'_i$ y $\sigma'_i\tau$ coinciden con la identidad en x_j y en $\phi(R)$.

Para ver que τ está bien definido solo hay que observar que la definición es compatible con las identidades $x_jr = \sigma_j(r)x_j$ y $x_jx_k = c_{kj}x_kx_j$ por el teorema 4 y el colorario 2, aplicando τ se obtienen las identidades equivalentes

$$\sigma_i^{-1}(c_{ij}^{-1})\sigma_j(\sigma_i^{-1}(r)) = \sigma_i^{-1}(\sigma_j(r))\sigma_i^{-1}(c_{ij}^{-1}) \quad (2.1)$$

$$\sigma_i^{-1}(c_{ij}^{-1})\sigma_j(\sigma_i^{-1}(c_{ik}^{-1}))c_{kj} = \sigma_i^{-1}(c_{kj})\sigma_i^{-1}(c_{ik}^{-1})\sigma_k(\sigma_i^{-1}(c_{ij}^{-1})) \quad (2.2)$$

Aplicación de σ_i' a $x_j r = \sigma_j(r)x_j$ y $x_j x_k = c_{kj}x_k x_j$ genera

$$c_{ij}\sigma_j(\sigma_i(r)) = \sigma_j(\sigma_i(r))c_{ij} \quad (2.3)$$

$$c_{ij}\sigma_j(c_{ik})c_{kj} = \sigma_i(c_{kj})c_{ik}\sigma_k(c_{ij}) \quad (2.4)$$

La ecuación (1) es la ecuación (3) en $r' = \sigma_i^{-1}(r)$, multiplicando por c_{ij}^{-1} a derecha y a izquierda; y aplicando σ_i^{-1} . Usando la ecuación (1) en la ecuación (2) para $r = c_{ik}^{-1}$ en la izquierda y $r = c_{ij}^{-1}$ en la derecha se obtiene la identidad que resulta de multiplicar (4) por constantes adecuadas y aplicar σ_i^{-1} . \square

Proposición 9. *Su A es una extensión PBW torcida generalizada finita biyectiva de R y ${}_R R$ es Noetheriano, entonces ${}_A A$ es Noetheriano.*

Demostración. Por las proposiciones 7 y 8 se reduce al caso $A = R[x, \sigma]$ con σ un automorfismo de R .

Este caso se prueba como el teorema de la base de Hilbert usual:

Si $I \subseteq A$ es un ideal izquierdo entonces el conjunto $J = \{r \in R \mid x^i r + \sum_{k < i} r_k x^k \in I \text{ para algunos } i \geq 0, r_k \in R\} \subseteq R$ es un ideal izquierdo de R y por lo tanto es finitamente generado $J = r_1 R + \dots + r_n R$, se eligen entonces polinomios $f_1, \dots, f_n \in I$ con términos principales $x^m r_1, \dots, x^m r_n$. Tomando ahora $J_l = \{r \in R \mid x^l r + \sum_{k < l} r_k x^k\}$ para $0 \leq l < m$, observamos de la misma forma que los J_l son ideales izquierdos de R y por lo tanto son finitamente generados, digamos por $r_{1l} \dots r_{Nl}$, y tomando polinomios $f_{il} \in I$ con término principal $x^l r_{il}$ observamos que ${}_A I$ es generado por $\{f_k \mid 1 \leq k \leq n\} \cup \{f_{il} \mid 1 \leq i \leq N, 0 \leq l < m\}$. \square

Proposición 10. *Sean R un anillo, A es extensión PBW torcida generalizada de R , y $S \subseteq R$ un subconjunto de R tal que $\sigma_i(S) \subseteq S$ para todo $i \in I$, entonces existe una única extensión PBW torcida generalizada de $R(S^{-1})$ como en la proposición 6, digamos B , y se tiene $B \cong A(S^{-1})$.*

Si A es biyectiva y $\sigma_i(S) = S$ entonces B es biyectiva.

Si S es un sistema multiplicativo de Ore a izquierda en R entonces también lo es en A .

Demostración. En el ejemplo 4 se ve que existen unicas extensiones de σ_i, δ_i a $R(S^{-1})$ se quiere aplicar la proposición 6.

Basta ver $h(x_j x_i s^{-1}) = h(p(x_j x_i) s^{-1})$. Se calcula

$$\begin{aligned} h(x_j x_i t) &= h(x_j \sigma_i(t) x_i) + h(x_j \delta_i(t)) = \\ &h(\sigma_j(\sigma_i(t)) x_j x_i) + h(\delta_j(\sigma_i(t)) x_i) + h(\sigma_j(\delta_i(t)) x_j) + h(\delta_j(\delta_i(t))) = \\ &\sigma_j(\sigma_i(t)) c_{ij} x_i x_j + \sum_k \sigma_j(\sigma_i(t)) a_{ij}^k x_k + \sigma_j(\sigma_i(t)) d_{ij} + \delta_j(\sigma_i(t)) x_i + \sigma_j(\delta_i(t)) x_j + \delta_j(\delta_i(t)) \end{aligned}$$

$$\begin{aligned} h(p(x_j x_i) t) &= h(c_{ij} x_i x_j t) + \sum_k h(a_{ij}^k x_k t) + h(d_{ij} t) = h(c_{ij} x_i \sigma_j(t) x_j) + h(c_{ij} x_i \delta_j(t)) + \\ &\sum_k h(a_{ij}^k \sigma_k(t) x_k) + \sum_k h(a_{ij}^k \delta_k(t)) + d_{ij} t = c_{ij} \sigma_i(\sigma_j(t)) x_i x_j + c_{ij} \delta_i(\sigma_j(t)) x_j + c_{ij} \sigma_i(\delta_j(t)) x_i + \\ &c_{ij} \delta_i(\delta_j(t)) + \sum_k a_{ij}^k \sigma_k(t) x_k + \sum_k a_{ij}^k \delta_k(t) + d_{ij} t. \end{aligned}$$

Igualando se obtiene

$$\mathbf{at} \quad \sigma_j(\sigma_i(t))c_{ij} = c_{ij}\sigma_i(\sigma_j(t)).$$

$$\mathbf{bt} \quad \sigma_j(\sigma_i(t))a_{ij}^i + \delta_j(\sigma_i(t)) = c_{ij}\sigma_i(\delta_j(t)) + a_{ij}^i\sigma_i(t).$$

$$\mathbf{ct} \quad \sigma_j(\sigma_i(t))a_{ij}^j + \sigma_j(\delta_i(t)) = c_{ij}\delta_i(\sigma_j(t)) + a_{ij}^j\sigma_j(t).$$

$$\mathbf{dt} \quad \sigma_j(\sigma_i(t))a_{ij}^k = a_{ij}^k\sigma_k(t), \quad k \neq i, j.$$

$$\mathbf{et} \quad \sigma_j(\sigma_i(t))d_{ij} + \delta_j(\delta_i(t)) = c_{ij}\delta_i(\delta_j(t)) + \sum_k a_{ij}^k\delta_k(t) + d_{ij}t.$$

En \mathbf{as}^{-1} multiplicamos por $\sigma_j(\sigma_i(s))$ a izquierda y por $\sigma_i(\sigma_j(s))$ a derecha y se obtiene ecuación equivalente \mathbf{as} que es cierta.

En \mathbf{bs}^{-1} se multiplica por $\sigma_j(\sigma_i(s))$ a izquierda y por $\sigma_i s$ a derecha, y teniendo en cuenta la fórmula para $\delta_j(s^{-1}) = -\sigma_j(s)^{-1}\delta_j(s)s^{-1}$ se tiene la ecuación equivalente $a_{ij}^i\sigma_i(s) - \delta_j(\sigma_i(s)) = -\sigma_j(\sigma_i(s))c_{ij}\sigma_i(\sigma_j(s))^{-1}\sigma_i(\delta_j(s)) + \sigma_j(\sigma_i(s))a_{ij}^i$, en presencia de \mathbf{as} , se reduce a \mathbf{bs} .

Análogamente multiplicando \mathbf{cs}^{-1} por $\sigma_j(\sigma_i(s))$ a izquierda y por $\sigma_j(s)$ a derecha y usa \mathbf{as} para reducir la ecuación a \mathbf{cs} .

Para \mathbf{ds}^{-1} se multiplica por $\sigma_j(\sigma_i(s))$ a izquierda y por $\sigma_k(s)$ a derecha y se obtiene \mathbf{ds} .

Finalmente hay que probar \mathbf{es}^{-1} , multiplicando por $\sigma_j(\sigma_i(s))$ a derecha y por s a izquierda se obtiene

$$\begin{aligned} d_{ij}s + \sigma_j(\sigma_i(s))\delta_j(\delta_i(s^{-1}))s = \\ \sigma_j(\sigma_i(s))c_{ij}\delta_i(\delta_j(s^{-1}))s + \sum_k \sigma_j(\sigma_i(s))a_{ij}^k\delta_k(s^{-1})s + \sigma_j(\sigma_i(s))d_{ij} \end{aligned}$$

y usando $\mathbf{as}, \mathbf{bs}, \mathbf{cs}, \mathbf{ds}$ se obtiene

$$\begin{aligned} d_{ij}s + \sigma_j(\sigma_i(s))\delta_j(\delta_i(s^{-1}))s = \\ c_{ij}\sigma_i(\sigma_j(s))\delta_i(\delta_j(s^{-1}))s + \sum_k a_{ij}^k\sigma_k(s)\delta_k(s^{-1})s - \sigma_j(\delta_i(s))\delta_j(s^{-1})s + c_{ij}\delta_i(\sigma_j(s))\delta_j(s^{-1})s - \\ \delta_j(\sigma_i(s))\delta_i(s^{-1})s + c_{ij}\sigma_i(\delta_j(s))\delta_i(s^{-1})s + \sigma_j(\sigma_i(s))d_{ij}. \end{aligned}$$

Ahora usamos las identidades

$$\delta(abc) = \sigma(a)\sigma(b)\delta(c) + \sigma(a)\delta(b)c + \delta(a)bc$$

y

$$\delta(s^{-1}) = -\sigma_k(s)^{-1}\delta_k(s)s^{-1}$$

para obtener

$$\begin{aligned} \delta_j\delta_i(s^{-1}) = -\delta_j(\sigma_i(s)^{-1}\delta_i(s)s^{-1}) = -\sigma_j(\sigma_i(s)^{-1})\sigma_j(\delta_i(s))\delta_j(s^{-1}) - \\ \sigma_j(\sigma_i(s)^{-1})\delta_j(\delta_i(s))s^{-1} - \delta_j(\sigma_i(s)^{-1})\delta_i(s)s^{-1} = \sigma_j(\sigma_i(s))^{-1}\sigma_j(\delta_i(s))\sigma_j(s)^{-1}\delta_j(s)s^{-1} - \\ \sigma_j(\sigma_i(s))^{-1}\delta_j(\delta_i(s))s^{-1} + \sigma_j(\sigma_i(s))^{-1}\delta_j(\sigma_i(s))\sigma_i(s)^{-1}\delta_i(s)s^{-1}. \end{aligned}$$

Y de aquí

$$\sigma_j(\sigma_i(s))\delta_j(\delta_i(s^{-1}))s = \sigma_j(\delta_i(s))\sigma_j(s)^{-1}\delta_j(s) - \delta_j(\delta_i(s)) + \delta_j(\sigma_i(s))\sigma_i(s)^{-1}\delta_i(s).$$

Intercambiar (i, j) produce otra identidad. Al reemplazar estas identidades y reordenar en la ecuación equivalente a \mathbf{es}^{-1} obtenida antes se obtiene

$$d_{ij}s + \sigma_j(\delta_i(s))\sigma_j(s)^{-1}\delta_j(s) - \delta_j(\delta_i(s)) + \delta_j(\sigma_i(s))\sigma_i(s)^{-1}\delta_i(s) = c_{ij}\sigma_i(\delta_j(s))\sigma_i(s)^{-1}\delta_i(s) - c_{ij}\delta_i(\delta_j(s)) + c_{ij}\delta_i(\sigma_j(s))\sigma_j(s)^{-1}\delta_j(s) - \sum_k a_{ij}^k \delta_k(s) + \sigma_j(\delta_i(s))\sigma_j(s)^{-1}\delta_j(s) - c_{ij}\delta_i(\sigma_j(s))\sigma_j(s)^{-1}\delta_j(s) + \delta_j(\sigma_i(s))\sigma_i(s)^{-1}\delta_i(s) - c_{ij}\sigma_i(\delta_j(s))\sigma_i(s)^{-1}\delta_i(s) + \sigma_j(\sigma_i(s))d_{ij}.$$

Y

$$0 = \sigma_j(\sigma_i(s))d_{ij} + \delta_j(\delta_i(s)) - c_{ij}\delta_i(\delta_j(s)) - \sum_k a_{ij}^k \delta_k(s) - d_{ij}s$$

Esto es **es**. Esto termina la prueba de existencia de B .

Por propiedades universales el isomorfismo es claro.

Si $\sigma_i(S) = S$ entonces σ_i^{-1} se extiende a $R(S^{-1})$ luego $\sigma_i : R(S^{-1}) \rightarrow R(S^{-1})$ es biyectivo y B es extensión PBW torcida generalizada biyectiva.

Ahora supongamos que $S \subset R$ es de Ore a izquierda y $\chi : A \rightarrow B$ es el morfismo canónico, basta ver que todo elemento $b \in B$ se expresa de la forma $\chi(s)^{-1}\chi(a)$, $s \in S$ y que $\chi(a) = 0$ implica $sa = 0$ para algún $s \in S$.

Tomemos $b = \Sigma r_{\bar{x}}\bar{x}$, suma es sobre $\bar{x} \in Mon$ y $r_x \in S^{-1}R$, como S es de Ore a izquierda existe un denominador común $r_{\bar{x}} = s^{-1}l_{\bar{x}}$ con $l_{\bar{x}} \in R$, así que $b = s^{-1}c$ con $c = \Sigma l_{\bar{x}}\bar{x}$.

Tomemos ahora $\chi(a) = 0$ en B , $a \in A$; se escribe $a = \Sigma r_{\bar{x}}\bar{x}$ la suma sobre un conjunto finito de $\bar{x} \in Mon$, $r_{\bar{x}} \neq 0$. De aquí se tiene $1^{-1}r_{\bar{x}} = 0$ en $S^{-1}R$ para todos los coeficientes que aparecen en la suma.

Por lo tanto existe $s_{\bar{x}} \in S$ con $s_{\bar{x}}r_{\bar{x}} = 0$, pero como S es de Ore a izquierda existe $s \in S$ y $t_{\bar{x}}$ con $s = t_{\bar{x}}s_{\bar{x}}$, es claro que $sr_{\bar{x}} = 0$ y $sa = 0$ como se busca. \square

Ideales primos

En este capítulo se hace un primer estudio de ideales primos en una extensión PBW torcida finita y biyectiva. El anillo de coeficientes se toma Noetheriano. En la primera sección se toma un ideal invariante en el anillo de coeficientes, se extiende a la extensión PBW torcida, y se dan resultados sobre la clase de ideales en el anillo de coeficientes que se extienden a ideales primos; los resultados en esta sección son adaptados del artículo [2]. En la segunda sección se empieza desde un ideal primo de la extensión y se le asocia una órbita de un ideal primo de el anillo de coeficientes bajo los automorfismos de la extensión, aquí seguimos el artículo [3].

Finalmente en la última sección cubrimos como un tema adicional la propiedad de Jacobson cuando el anillo de coeficientes es un cuerpo, aquí adaptamos resultados del libro [1].

En todo el capítulo todas las extensiones se asumen finitas.

3.1. Extensión a ideales primos

En esta sección damos algunos resultados parciales a la pregunta de para cuáles ideales I de R es IA un ideal primo de A . Empezamos con algunas definiciones.

Definición 14. *Dado un anillo R un sistema de automorfismos de R es un conjunto finito $\Sigma = \{\sigma_1, \dots, \sigma_n\}$ indexado por $\{1, \dots, n\}$ tal que σ_i es un automorfismo de R para todo i . Un sistema de Σ -derivaciones Δ es un conjunto finito $\Delta = \{\delta_1, \dots, \delta_n\}$ indexado por $\{1, \dots, n\}$ tal que δ_i es una σ_i derivación. También decimos que (Σ, Δ) es un sistema de derivaciones de R .*

Definición 15. *Dado un anillo R y un conjunto L de funciones de R es si mismo, decimos que un ideal $I \subseteq R$ es L -invariante si $f(I) \subseteq I$ para todo $f \in L$. Decimos que un ideal es f -invariante si es $\{f\}$ -invariante. Por ejemplo para (Σ, Δ) un sistema de derivaciones de R podemos hablar de ideales Σ -invariantes y Δ -invariantes.*

Un ideal se dice (Σ, Δ) -invariante si, y sólo si, es $\Sigma \cup \Delta$ -invariante (o equivalentemente si es Σ -invariante y Δ -invariante)

El siguiente lema se usa en lo que sigue sin mención explícita

Lema 7. Si R es Noetheriano, σ es un automorfismo e I es un ideal σ -invariante de R , entonces $\sigma(I) = I$.

Demostración. Tenemos $\sigma(I) \subseteq I$, aplicando σ^{-n} obtenemos

$$I \subseteq \sigma^{-1}(I) \subseteq \sigma^{-2}(I) \subseteq \dots$$

Por Noetherianidad concluimos $\sigma^{-n}(I) = \sigma^{-n-1}(I)$ y aplicando σ^{n+1} se obtiene $I = \sigma(I)$ \square

Definición 16. Dado un anillo R y un conjunto L de funciones de R es si mismo, decimos que un ideal $I \subset R$ es L -primo si $I \neq R$, I es L -invariante y para todo par J, K de ideales L -primos con $JK \subseteq I$ se tiene $J \subseteq I$ o $K \subseteq I$.

R se dice L -primo si 0 es L -primo.

Lema 8. Sea R es un anillo y A es una extensión PBW torcida biyectiva de R con sistema de derivaciones asociado (Σ, Δ) . Si I es un ideal de R (Σ, Δ) -invariante entonces IA es un ideal de A . Además A/IA es una extensión PBW torcida generalizada de R/I , y es biyectiva si R es Noetheriano.

Demostración. Para ver que IA es un ideal de A basta observar que $x_i I \subseteq IA$ para x_i una variable de A . Y en efecto $x_i a = \sigma_i(a)x_i + \delta_i(a) \in IA$ para $a \in I$, pues I es (Σ, Δ) -invariante.

Vemos que las condiciones $\sigma_i(I) \subseteq I$ y $\delta_i(I) \subseteq I$ son equivalentes a decir que existe una derivación (σ'_i, δ'_i) en R/I tal que $\sigma'_i(r+I) = \sigma_i(r) + I$ y $\delta'_i(r+I) = \delta_i(r) + I$, se puede ver directamente de la definición que A/IA es una extensión PBW torcida generalizada de R/I con estas derivaciones, pero también es consecuencia de la proposición 6 y la propiedad universal.

Finalmente σ'_i es biyectiva si $\sigma_i(I) = I$ (en este caso tiene inversa) y esta igualdad es válida si R es Noetheriano por el lema 7. \square

Proposición 11. Si R es un anillo Noetheriano, A es una extensión PBW torcida biyectiva de R y el conjunto de automorfismos y derivaciones de R asociados a A es (Σ, Δ) , si I es un ideal Σ -primo y Δ invariante de R entonces IA es un ideal primo de A .

Demostración. Reemplazando R por R/I podemos asumir sin pérdida de generalidad ue $I = 0$.

Reemplazando A por $Gr(A)$ (con la filtración estándar) podemos asumir que A es quasicommutativo, véase la sección 2.3, proposición 7 (y recordando que si $Gr(A)$ es primo entonces A es primo).

Recordando que $A = R[x_1, \sigma_1] \cdots [x_n, \sigma_n]$ (véase la sección 2.3, proposición 8), basta ver que si $A = R[x, \sigma]$ y R es $\Sigma \cup \{\sigma\}$ -primo donde $\Sigma = \{\sigma_1, \dots, \sigma_n\}$ y σ_i se extiende a A al hacer $\sigma_i(x) = c_i x$ con $c_i \in R$ invertible, entonces A es Σ -primo.

En este caso tomamos $I, J \subseteq A$ ideales Σ -invariantes con $IJ = 0$. Definimos $I_1 = \{r \in$

$R : rx^n + \sum_{k < n} r_k x^k \in I$ para algunos $n \geq 0, r_k \in R$ y $J_1 = \{r \in R : rx^n + \sum_{k < n} r_k x^k \in J$ para algunos $r_k \in R\}$. Para $r \in I_1$ elegimos $f = rx^n + \sum_{k < n} r_k x^k \in I$ con $r_k \in R$, para $a, b \in R$ multiplicando f por a a izquierda y por $\sigma^{-n}b$ a derecha observamos que $arb \in I_1$. Para $s \in I_1$ elegimos $g = sx^m + \sum_{k < m} s_k x^k \in I$ con $s_k \in R$, considerando $fx^m + gx^n$ vemos que $r + s \in I_1$. Calculando $\sigma_i(f) \in I$ observamos que $\sigma_i(r)c_i\sigma_i(c_i) \cdots \sigma_i^{n-1}(c_i) \in I_1$ y como $c_i\sigma_i(c_i) \cdots \sigma_i^{n-1}(c_i)$ es invertible entonces $\sigma_i(r) \in I_1$. Finalmente considerando xf observamos que $\sigma(r) \in I_1$. Concluimos que I_1 es un ideal $\Sigma \cup \{\sigma\}$ invariante de R . Por supuesto esto tambien es cierto para J_1 .

Ahora tomemos $t \in J_1$ elegimos $h = tx^l + \sum_{k < l} t_k x^k \in J$ con $t_k \in R$, haciendo el producto $fh = 0$ y viendo el coeficiente de x^{l+n} obtenemos $r\sigma^n(t) = 0$, como R es noetheriano y J_1 es σ invariante concluimos que $\sigma^{-n}(t) \in J_1$ y por lo tanto $rt = 0$, es decir $I_1J_1 = 0$. Como R es $\Sigma \cup \{\sigma\}$ primo concluimos $I_1 = 0$ o $J_1 = 0$ y de aquí $I = 0$ o $J = 0$ como se requiere. \square

Como ejemplo vemos un caso particular, en el que las derivaciones se toman como 0.

Proposición 12. *Sea R un anillo Noetheriano y A una extensión PBW-torcida biyectiva con automorfismos asociados Σ y derivaciones asociadas todas 0.*

Si I es un ideal de R Σ -invariante entonces IA es un ideal primo de A si, y sólo si, I es un ideal Σ -primo de R .

Demostración. Una dirección es la proposición anterior, para la otra asumimos que I es un ideal Σ -invariante pero no Σ -primo, entonces existen J, K ideales Σ -invariantes no contenidos en I con $JK \subseteq I$. Entonces JA y KA son ideales de A no contenidos en IA con $JAKA \subseteq IA$, y IA no es primo en A . \square

Proposición 13. *Sea R un anillo Noetheriano, y Σ un conjunto de automorfismos. Sea I un ideal de R Σ -primo, entonces I es semiprimo.*

Demostración. Reemplazando R por R/I podemos asumir sin pérdida de generalidad ue $I = 0$.

En este caso $J = Nil(R)$ es nilpotente pues R es Noetheriano, $J^n = 0$. Pero J es siempre Σ -invariante, luego $J = 0$, es decir R es semiprimo. \square

Denotemos las palabras finitas en el alfabeto $\{1, \dots, n\}$ por P_n , para cada elemento $t = (t_1, \dots, t_m) \in P_n$ definimos $\sigma_t = \sigma_{t_1} \cdots \sigma_{t_m}$ (como convención si $m = 0$ entonces $\sigma_t = id$).

Tomemos I un ideal de R un anillo y definimos para $k \geq 0$

$$I_k = \{a \in R : \sigma_{n_0} \delta_{i_1} \sigma_{n_1} \cdots \delta_{i_j} \sigma_{n_j}(a) \in I \text{ para } 0 \leq j < k, 1 \leq i_1, \dots, i_j \leq n, n_0, \dots, n_j \in P_n\}$$

Se tiene la siguiente identidad

$$\sigma_{n_0} \delta_{i_1} \sigma_{n_1} \cdots \delta_{i_j} \sigma_{n_j}(ab) = \sum_w \sigma_{n_0} \alpha_{i_1 w(1)} \sigma_{n_1} \cdots \alpha_{i_j w(j)} \sigma_{n_j}(a) \sigma_{n_0} \beta_{i_1 w(1)} \sigma_{n_1} \cdots \beta_{i_j w(j)} \sigma_{n_j}(b)$$

la suma en la derecha es sobre $w : \{1, \dots, j\} \rightarrow \{0, 1\}$, $\alpha_{r0} = \sigma_r$, $\beta_{r0} = \delta_r$, $\alpha_{r1} = \delta_r$, $\beta_{r1} = id$.

Esta identidad se prueba por inducción en j .

Ahora si $a \in I_n$, $b \in I_m$ y $0 \leq j < n + m$ entonces para cada $w : \{1, \dots, j\} \rightarrow \{0, 1\}$, se tiene $\text{card}\{r : w(r) = 0\} < n$ o $\text{card}\{r : w(r) = 1\} < m$. En el primer caso $\sigma_{n_0} \beta_{i_1 w(1)} \sigma_{n_1} \cdots \beta_{i_j w(j)} \sigma_{n_j}(b) \in I$ y en el segundo $\sigma_{n_0} \alpha_{i_1 w(1)} \sigma_{n_1} \cdots \alpha_{i_j w(j)} \sigma_{n_j}(a) \in I$, concluimos que $\sigma_{n_0} \delta_{i_1} \sigma_{n_1} \cdots \delta_{i_j} \sigma_{n_j}(ab) \in I$ y $ab \in I_{n+m}$.

Es decir $I_n I_m \subseteq I_{n+m}$, en particular si $m = 0$, $I_0 = R$ y I_n es un ideal derecho, por simetría I_n es un ideal bilátero.

También podemos ver que

$$\prod_k I_{n_k} \subseteq I_{\sum_k n_k}$$

por inducción en el número de ks. En particular $I_1^m \subseteq I_m$.

Proposición 14. *Sea R un anillo Noetheriano, Σ un sistema de automorfismos de R y Δ un sistema de Σ -derivaciones de R . Si R es (Σ, Δ) -primo, entonces*

1. $\text{Nil}(R)$ es Σ -primo.
2. $C_R(0) = C_R(\text{Nil}(R))$.
3. El anillo total de fracciones de R existe y es artiniiano.

Demostración. 1) Tomamos un ideal $I \subseteq R$, Σ -invariante con $\text{rann}_R(I) \neq 0$ y maximal con esta propiedad.

Vemos primero que I es Σ -primo, en efecto si J, K son ideales Σ -invariantes con $JK \subseteq I$ y J, K no contenidos en I entonces reemplazando J, K por $J + I, K + I$ podemos suponer $I \subsetneq J, K$ y por maximalidad de I concluimos que $\text{rann}_R(J) = 0 = \text{rann}_R(K)$ y de aquí $\text{rann}_R(JK) = 0$ pues si $r \in R$ es tal que $rJK = 0$ entonces $rJ \subseteq \text{rann}_R(K) = 0$ y $r \in \text{rann}_R(J) = 0$. Esto contradice $0 \neq \text{rann}_R(I) \subseteq \text{rann}_R(JK)$.

Vemos entonces que I es semiprimo por la proposición 13 y por lo tanto $\text{Nil}(R) \subseteq I$.

Para la otra contención recordamos las convenciones de antes de esta proposición

$$\cdots \subseteq I_2 \subseteq I_1 = I$$

y

$$\text{rann}_R I_1 \subseteq \text{rann}_R I_2 \cdots$$

Por Noetherianidad tenemos que $J = \text{rann}_R I_m = \text{rann}_R I_{m+1} = \cdots$ para algún m . Vamos a ver que J es un ideal (Σ, Δ) -invariante, en efecto J es Σ -invariante porque I_m es Σ -invariante. Tomemos ahora $a \in J$ y $b \in I_{m+1}$ entonces $ab = 0$, $\sigma_i(a) \in J$ y $\delta_i(b) \in I_m$, luego $\sigma_i(a)\delta_i(b) = 0$, y de aquí

$$0 = \delta_i(ab) = \sigma_i(a)\delta_i(b) + \delta_i(a)b = \delta_i(a)b$$

concluimos que $\delta_i(a) \in J$, y J es (Σ, Δ) -invariante.

También tenemos que $L = \text{lann}_R J$ es un ideal (Σ, Δ) -invariante, en efecto L es Σ -invariante porque J es Σ -invariante; y si tomamos $a \in L$ y $b \in J$ entonces $ba = 0$, $\delta_i(b) \in J$, y por tanto $\delta_i(b)a = 0$, y de aquí

$$0 = \delta_i(ba) = \sigma_i(b)\delta_i(a) + \delta_i(b)a = \sigma_i(b)\delta_i(a)$$

es decir $0 = \sigma_i(J)\delta_i(a) = J\delta_i(a)$ y $\delta_i(a) \in L$.

De la definición de J y L tenemos $I_m \subseteq L$, $rann_R I \subseteq J$ y $JL = 0$. Por la elección de I , tenemos $rann_R I \neq 0$, de donde $J \neq 0$. R es (Σ, Δ) -invariante y $JL = 0$ implica $L = 0$. Finalmente por la discusión antes de la prueba $I^m \subseteq I_m \subseteq L$ implica $I_m = I^m = 0$ y $I \subseteq Nil(R)$.

2) La inclusión $C_R(0) \subseteq C_R(Nil(R))$ es cierta para anillos Noetherianos cualquiera, véase [7]4.1.3 (iii).

Tomamos $I = Nil(R)$ e I_n como en la prueba de 1, y observamos que

$$0 = I_m \subseteq \cdots \subseteq I_0 = R$$

de forma que sólo hay que probar que I_n/I_{n+1} es $C_R(I)$ -libre de torsión. Para esto tomamos $s \in C_R(I)$ y $r \in I_n$ con $sr \in I_{n+1}$. Y tomamos $j < n + 1$, recordamos la identidad

$$\sigma_{n_0}\delta_{i_1}\sigma_{n_1}\cdots\delta_{i_j}\sigma_{n_j}(sr) = \sum_w \sigma_{n_0}\alpha_{i_1w(1)}\sigma_{n_1}\cdots\alpha_{i_jw(j)}\sigma_{n_j}(s)\sigma_{n_0}\beta_{i_1w(1)}\sigma_{n_1}\cdots\beta_{i_jw(j)}\sigma_{n_j}(r)$$

con las convenciones de la discusión antes de esta proposición. Vemos que el término en la derecha pertenece a I (por definición de I_{n+1}) y $\sigma_{n_j}(s)\sigma_{n_0}\beta_{i_1w(1)}\sigma_{n_1}\cdots\beta_{i_jw(j)}\sigma_{n_j}(r) \in I$ siempre que w no sea constante a 0. Reduciendo módulo I obtenemos

$$\sigma_{\bar{f}}(s)\sigma_{n_0}\delta_{i_1}\sigma_{n_1}\cdots\delta_{i_j}\sigma_{n_j}(r) \in I$$

con $\sigma_{\bar{f}}$ una palabra en σ_i . Como I es Σ -invariante entonces $C_R(I)$ es Σ -invariante y $\sigma_{\bar{f}}(s) \in C_R(I)$, $\sigma_{n_0}\delta_{i_1}\sigma_{n_1}\cdots\delta_{i_j}\sigma_{n_j}(r) \in I$ y $r \in I_{n+1}$ como se requiere. Un argumento simétrico prueba que si $rs \in I_{n+1}$ entonces $r \in I_{n+1}$.

3) Esto es consecuencia de 2 por el teorema de Small, véase [7] 4.1.4. \square

En la siguiente proposición resolvemos la pregunta del principio de la sección para el caso mixto (es decir automorfismos y derivaciones no triviales) para el caso algo restrictivo de ideales semiprimos.

Proposición 15. *Sea R un anillo Noetheriano y A una extensión PBW-torcida biyectiva con derivaciones asociadas (Σ, Δ) . Si I es un ideal de R (Σ, Δ) -invariante y semiprimo, entonces IA es un ideal primo de A si, y sólo si, I es un ideal Σ -primo de R si, y sólo si, I es un ideal (Σ, Δ) -primo de R .*

Demostración. Una dirección es la proposición 11.

Ahora asumimos que I es un ideal (Σ, Δ) -invariante pero no (Σ, Δ) -primo, entonces existen J, K ideales (Σ, Δ) -invariantes no contenidos en I con $JK \subseteq I$. Entonces JA y KA son ideales de A no contenidos en IA con $JAKA \subseteq IA$, y IA no es primo en A . Esta es otra de las implicaciones.

Finalmente si I es (Σ, Δ) -primo y semiprimo entonces la parte 1 de la proposición anterior aplicada a R/I implica que $Nil(I) = I$ es Σ -primo. Esto termina la prueba. \square

3.2. A cada ideal primo de la extensión se le asocia una órbita en $\text{Spec}(R)$

En esta sección seguimos los resultados de [3] (especialmente la sección 4), en el contexto de extensiones PBW torcidas.

Proposición 16. *Sea T un anillo y ${}_T M$ un T módulo derecho. Si se tiene una susección de submódulos de ${}_T M$*

$$M_0 = 0 \subset M_1 \subset \dots$$

tales que M_i/M_{i-1} es simple y $M = \cup_i M_i$, y tomamos N un subfactor simple de M entonces existe i tal que $M_i/M_{i-1} \cong N$

Demostración. $N = N_1/N_2$ con $N_2 \subset N_1 \subset M$. Existe i tal que $M_i \cap N_1 \not\subseteq N_2$, de lo contrario como $M = \cup_i M_i$ se tendría $N_1 = N_2$; se elige i mínimo con esta propiedad, de forma que en particular $M_i \cap N_1/M_{i-1} \cap N_1 \neq 0$.

Tenemos morfismos inyectivos $M_i \cap N_1/M_{i-1} \cap N_1 \rightarrow M_i/M_{i-1}$ y

$M_i \cap N_1/M_i \cap N_2 \rightarrow N$; como tienen dominios no nulos y rangos simples son isomorfismos, en particular $M_i \cap N_1/M_{i-1} \cap N_1$ es simple y $M_{i-1} \cap N_1 \subseteq M_i \cap N_2 \subset M_i \cap N_1$ implica $M_{i-1} \cap N_1 = M_i \cap N_2$ y $N \cong M_i \cap N_1/M_{i-1} \cap N_1 \cong M_i/M_{i-1}$ que es el enunciado. \square

Lema 9. *Si R es un anillo Noetheriano y A es una extensión PBW-torcida biyectiva de R , si M es un subfactor de ${}_R A_R$, y $b \in M$ entonces el R - R bimódulo RbR es finitamente generado por cualquiera de los dos lados.*

Demostración. Como $M = B/C$ con $C \subset B \subset A$, entonces se observa que basta probar el lema para $M = A$.

En este caso si

$$b = \sum_{a \in J} r_a x^a$$

donde $J \subseteq \mathbb{N}^n$ es finito y $r_a \in R$, entonces RbR es un submódulo izquierdo de $\sum_{a \in J} R x^a$, como R es Noetheriano se concluye el resultado. (El lado derecho es por simetría). \square

Sea R un anillo Noetheriano por ambos lados y A una extensión de R , A un anillo Noetheriano, tomemos P un ideal primo de A .

Siguiendo las pruebas en [3], llamamos C el anillo total de fracciones de A/P , y tomamos una serie de descomposición de ${}_R C_C$, $0 = C_0 \subset C_1 \subset \dots \subset C_m = C$, llamamos $Q_i = \text{ann}_R(C_i/C_{i-1})$. Vemos que Q_i es primo de R . Más en general si A y B son anillos y ${}_A M_B$ es un bimódulo simple entonces $\text{ann}_A M = \{a \in A \mid am = 0 \text{ para todo } m \in M\}$ es un ideal primo de A . $P \cap R \subset Q_i$ y $Q_1 \dots Q_m \subset P \cap R$; en particular si Q es primo minimal con $P \cap R \subset Q$ entonces $Q \in \{Q_1, \dots, Q_m\}$.

Dado una tupla $a = (a_1, \dots, a_n) \in \mathbb{Z}$, denotamos $\sigma^a = \sigma_1^{a_1} \dots \sigma_n^{a_n}$.

Dados monomios estándar $\bar{x} = x_1^{a_1} \dots x_n^{a_n}$ y $\bar{y} = x_1^{b_1} \dots x_n^{b_n}$, decimos $\bar{x} \leq \bar{y}$ si

$$(\sum a_k, a_1, \dots, a_n) \leq (\sum b_k, b_1, \dots, b_n)$$

en el orden lexicográfico. Este orden es isomorfo a ω .

Proposición 17. *Dado R, A, C, P y Q_1, \dots, Q_m como antes existe un B , R - R bimódulo subfactor de $A/Q_m A$ con $\text{ann}_R B = Q_m$, $\text{ann} B_R = Q_i$ y B libre de torsión por ambos lados como R/Q_m - R/Q_i -bimódulo.*

Demostración. Se encuentra en el lemma 2 de [8] □

Proposición 18. *Tomando A una extensión PBW torcida biyectiva de R y con la notación de antes, para todo $1 \leq i \leq m$ existe $a \in \mathbb{N}$ tal que $\sigma^a(Q_i) = Q_m$*

Demostración. Se elige B un R - R bimódulo, subfactor del R - R bimódulo $A/Q_m A$ con $\text{ann}_R B = Q_m$ y $\text{ann}_R B = Q_i$, libre de torsión por ambos lados como R/Q_m - R/Q_i bimódulo, podemos reemplazar B por RbR con $b \in B$ no nulo para concluir que sin pérdida de generalidad B es finitamente generado como R módulo por cualquier lado (véase el lema 2 en la sección 1.1 y el lema 9).

D es el anillo de fracciones de R/Q_m , entonces $D \otimes_R B$ es un D - R bimódulo de longitud finita con $\text{ann}(D \otimes_R B)_R = Q_i$. En efecto $D \otimes_R B$ es finitamente generado como D -módulo izquierdo luego es artiniario y noetheriano como D - R -bimódulo, es decir es de longitud finita, y como B es libre de torsión como R/Q_m módulo se tiene también que el morfismo $B \rightarrow D \otimes_R B$ canónico es inyectivo luego $\text{ann}(D \otimes_R B)_R = Q_i$. Ahora elegimos $M \subseteq D \otimes_R B$ simple entonces $M = D \otimes_R B_1$ y reemplazando B por B_1 podemos suponer sin pérdida de generalidad que $D \otimes B$ es simple. En efecto $D \otimes_R B$ es la localización del módulo izquierdo B por el sistema multiplicativo de elementos regulares de R/Q_m , de forma que los submódulos de $D \otimes_R B$ son localizaciones de submódulos de B , luego $M = D \otimes B_1$ y aplicando de nuevo el lema 2 en la sección 1.1 obtenemos lo que mencionamos antes.

$D \otimes B$ es un subfactor de $V = D \otimes_R A = D \otimes_R A/Q_m A$, pues D es un R/Q_m módulo izquierdo plano.

${}_D(D \otimes_R A)$ es libre con base $\{1 \otimes \bar{x} \mid \bar{x} \text{ es un monomio estándar}\}$.

$V_{\bar{x}} = \Sigma_{\bar{y} \leq \bar{x}} D(1 \otimes \bar{y})$ es una filtración de ${}_D V_R$ con los cocientes consecutivos $G_{\bar{x}} = \Sigma_{\bar{y} \leq \bar{x}} D(1 \otimes \bar{y}) / \Sigma_{\bar{y} < \bar{x}} D(1 \otimes \bar{y})$, D - R bimódulos isomorfo to D^{σ^a} luego es simple (véase el lema 1 en la sección 1.1). Y se tiene con $\text{ann}(G_{\bar{x}})_R = (\sigma^a)^{-1}(Q_m)$.

Se concluye por la proposición 16 que $D \otimes_R B \cong G_{\bar{x}}$ para algún \bar{x} y tomando los anuladores derechos $Q_i = (\sigma^a)^{-1}(Q_m)$. □

Este resultado se puede interpretar como: a cada ideal primo de P de A la estrategia clásica es asociarle el ideal de R obtenido por contracción $P \cap R$, pero se observa en [3] que esta asociación no es adecuada en el caso $R[x, \sigma, \delta]$ con R no conmutativo y σ y δ no triviales, esta proposición se propone en ese artículo como una modificación del método clásico, que a un ideal primo P de A le asocia la órbita $\{\tau_{i_1} \cdots \tau_{i_n}(Q_1) \mid 1 \leq i_k \leq n, \tau_i = \sigma_i \text{ o } \tau_i = \sigma_i^{-1}\}$ que contiene a todos los primos minimales de R sobre $P \cap R$. Sigue un resultado de localización.

Lema 10. *Sea R un anillo Noetheriano y A un anillo Noetheriano con $R \subset A$, sea P un ideal primo de A . Sea C el anillo total de fracciones de A/P , y una serie de descomposición de ${}_R C_C$, $0 = C_0 \subset C_1 \subset \cdots \subset C_m = C$, llamamos $Q_i = \text{ann}_R(C_i/C_{i-1})$.*

Suponiendo que Q_1, \dots, Q_n son exactamente los primos minimales sobre $P \cap R$ y que RaR es noetheriano como R -módulo por ambos lados, se tiene entonces que para C el conjunto de elementos regulares de $R/P \cap R$, C es de Ore en $R/P \cap R$ y en A/P y que $C^{-1}(R/P \cap R)$ es artiniario.

Demostración. Es una especialización de [3] lema 4.5. □

Proposición 19. *R Noetheriano y A extensión PBW-torcida biyectiva de R , P un ideal primo de A . Y sea \mathcal{C} el conjunto de elementos regulares de $R/P \cap R$, entonces \mathcal{C} es un conjunto de Ore de elementos regulares en $R/P \cap R$ y en A/P , y $\mathcal{C}^{-1}(R/P \cap R)$ es artiniiano.*

Demostración. Hay que ver por el lema anterior que con la notación de la proposición 18 $\{Q_1, \dots, Q_n\}$ es exactamente el conjunto de primos minimales de $R/P \cap R$.

Pero por la proposición 18 $R/Q_i \cong R/Q_j$ y por lo tanto la dimensión de krull clásica de R/Q_i , $ckdim(R/Q_i)$ es un ordinal (pues R es Noetheriano) independiente de i .

En particular tomando Q_i cualquiera y $P \cap R \subseteq Q \subseteq Q_i$ con Q un primo minimal con estas condiciones, por la discusión antes de la proposición 18 se concluye que $Q \in \{Q_1 \dots Q_n\}$ luego $ckdim(R/Q) = ckdim(R/Q_i)$ y esto implica $Q_i = Q$ como se busca. \square

Proposición 20. *Sea R un anillo noetheriano, A un anillo y $\phi : R \rightarrow A$ un morfismo. Suponiendo que hay elementos $x_1, \dots, x_n \in A$ que junto con R generan a A como anillo y que cumplen $x_i R + R = R x_i + R$, y, $x_j x_i R + \Sigma R x_k + R = R x_i x_j + \Sigma R x_k + R$; se tiene entonces que $rkdim(A) \leq rkdim(R) + n$.*

Demostración. Dotamos a A de la filtración estándar dada por los x_i , como $rkdim(A) \leq rkdim(Gr(A))$ reemplazando A por $Gr(A)$ podemos suponer que $x_i R = R x_i$ y $x_j x_i R = x_i x_j R$.

Tomando $R_0 = \phi(R)$ y $R_k = \Sigma_n R_{k-1} x_k^n$ y reemplazando A por R_k y R por R_{k-1} se puede asumir además que solo hay una variable y R es un subanillo de A .

En este caso A es Noetheriano por [7] 1.2.10 y por [7] 6.3.8 hay un ideal primo de A tal que $rkdim(A/P) = rkdim(A)$, reemplazando A por A/P y R por $R/P \cap R$ suponemos también que A es primo.

En este caso x es un elemento normal en A , luego $x = 0$ o x es regular en A ; el primer caso es trivial y en el segundo $xr = \sigma(r)x$ con $\sigma : R \rightarrow R$ un automorfismo unívocamente determinado por esta ecuación, de aquí se concluye que $A = R[x, \sigma]$, y en este caso $rkdim(A) = rkdim(R) + 1$ por [7] 6.5.4. \square

3.3. Propiedad de Jacobson

En esta sección probamos que una extensión PBW torcida finita biyectiva sobre un cuerpo es de Jacobson.

Para las siguientes proposiciones seguimos las ideas de [1] 2.6.4 y 3.1.15. El orden total de \mathbb{N}^n es dado por $a \leq_t b$ si $a_k \leq b_k$ para todo k , esto es un orden parcial.

Lema 11. *Si $S \subset \mathbb{N}^n$ entonces el subconjunto de elementos minimales S_0 de S respecto al orden total es finito.*

Todo elemento en S es mayor o igual que un elemento en S_0

Demostración. El conjunto de elementos minimales con respecto a S es un conjunto de elementos incomparables en el orden total, si se elige $a = (a_1, \dots, a_n) \in S_0$ cualquiera entonces hay a lo más $\Sigma_k a_k + 2$ elementos en S_0 , en efecto $S_0 - a \subseteq \{0, \dots, a_1 - 1\} \times \mathbb{N}^{n-1} \cup \dots \cup \mathbb{N}^{n-1} \times \{0, \dots, a_n - 1\}$ si hubieran más elementos el principio de casillas permite encontrar dos elementos en $\mathbb{N}^i \times \{k\} \times \mathbb{N}^{n-1-i}$ que resultan comparables. \square

En la siguiente prueba usamos otro orden en \mathbb{N}^n , $a < b$ si

$$(|a|, a_1, \dots, a_n) < (|b|, b_1, \dots, b_n)$$

con el orden lexicográfico. Hemos denotado $|a| = a_1 + \dots + a_n$. Notamos que \mathbb{N}^n con este orden es isomorfo \mathbb{N} con el orden habitual.

Si A es un anillo conmutativo con un conjunto de automorfismos σ_i denotamos $A_{f,\sigma}$ la localización de A por el sistema multiplicativo $S_{f,\sigma} = \{\prod \sigma(f) : \sigma \text{ es palabra en } \sigma_i\}$, se usa varias veces sin mención explícita que $A_{f,\sigma}$ es un A -módulo derecho plano.

Usaremos también el siguiente lema elemental.

Lema 12. *Sea A es un anillo y ${}_A N$ es un A -módulo. Sea $\{M_\beta\}_{\beta < \alpha}$ una cadena de submódulos de N indexados por un ordinal α (es decir $M_\beta \subset M_\gamma$ para $\beta < \gamma$) tal que para $M_\beta^- = \sum_{\gamma < \beta} M_\gamma = \cup_{\gamma < \beta} M_\gamma$ se tiene que M_β/M_β^- es proyectivo para $\beta < \alpha$. Entonces $M_\alpha^- = \bigoplus_{\beta < \alpha} L_\beta$ con $L_\beta \cong M_\beta/M_\beta^-$. En particular si M_β/M_β^- es libre entonces M_α^- también es libre.*

La prueba es sencilla y se omite.

Lema 13. *Sea R un dominio conmutativo y B una imagen homomórfica de una extensión PBW-torcida biyectiva de R , entonces si ${}_B M$ es un B -módulo finitamente generado, existe $f \in R - 0$ tal que $R_{f,\sigma} \otimes_R M$ es un $R_{f,\sigma}$ -módulo libre.*

Demostración. Sin pérdida de generalidad B es una extensión PBW-torcida biyectiva de R en las variables x_1, \dots, x_n y ${}_B M = Bm$. En efecto, como M es finitamente generado, digamos con generadores m_1, \dots, m_l , entonces tomando $M_1 = \sum_{k < l} Bm_k$ y $M_2 = M/M_1$, tenemos la sucesión exacta $0 \rightarrow M_1 \rightarrow M \rightarrow M_2 \rightarrow 0$, como M_1 tiene menos generadores que M podemos asumir por inducción que existe $f \in R - 0$ tal que $R_{f,\sigma} \otimes_R M_1$ es libre, y como M_2 tiene un sólo generador, podemos suponer que $R_{g,\sigma} \otimes_R M_2$ es libre para algún $g \in R - 0$; entonces (por ejemplo por propiedad universal) $R_{fg,\sigma} \otimes_R M_1 = R_{fg,\sigma} \otimes_{R_{f,\sigma}} R_{f,\sigma} \otimes_R M_1$ es libre, y similarmente $R_{fg,\sigma} \otimes_R M_2$ es libre, tensorizando la sucesión exacta $0 \rightarrow M_1 \rightarrow M \rightarrow M_2 \rightarrow 0$ por $R_{fg,\sigma}$ observamos que $R_{fg,\sigma} \otimes_R M$ es libre y $fg \in R - 0$ pues R es un dominio.

Si $a = (a_1, \dots, a_n) \in \mathbb{N}^n$, denotamos $x^a = x_1^{a_1} \dots x_n^{a_n}$. Con el orden en \mathbb{N}^n de antes llamamos $N_a = \sum_{b \leq a} R x^b m$ y $N_a^- = \sum_{b < a} R x^b m$ ambos son R -módulos izquierdos; y denotamos $K_a = N_a/N_a^-$ y $I_a = \text{ann}_R(\overline{x^a m}) = \{r \in R \mid r \overline{x^a m} = 0\}$ donde $\overline{x^a m}$ es la imagen de $x^a m$ en K_a .

Si $a, b \in \mathbb{N}^n$ y $a \leq_t b$ en el orden total entonces $\sigma(I_a) \subset I_b$ con σ una concatenación de σ_i , en efecto sin pérdida de generalidad $b = (a_1, \dots, a_i + 1, \dots, a_n)$ y si $r \in I_a$ entonces $r x^a m \in N_a^-$, es decir $r x^a m = \sum_{c < a} r_c x^c m$, ahora observamos que $x_i r x^a = u \sigma_i(r) x^b + \sum_c l_c x^c$ donde la suma en la derecha involucra solo $c \in \mathbb{N}^n$ con $|c| < |b|$, (y por lo tanto $c < b$) y $u \in U(R)$. Multiplicando por $u^{-1} x_i$ la ecuación $r x^a m = \sum_{c < a} r_c x^c m$ y con un cálculo similar para los términos de la derecha se obtiene $\sigma_i(r) \in I_b$.

Tomamos $S = \{a \in \mathbb{N}^n \mid I_a \neq 0\}$, por el lema 11 hay un número finito de elementos minimales en S con el orden total $s_1 \dots s_n \in S$ y como R es un dominio conmutativo, elegimos $f \in I_{s_1} \cap \dots \cap I_{s_n}$ no nulo.

Si K_a es tal que $I_a \neq 0$ entonces $R_{f,\sigma} \otimes_R K_a$ es un $R_{f,\sigma}$ -módulo generado por $\overline{x^a m}$ pero

$\sigma(f)\overline{x^am} = 0$ y $\sigma(f)$ es invertible en $R_{f,\sigma}$, de aquí $R_{f,\sigma} \otimes_R K_a = 0$.

Si K_a es tal que $I_a = 0$ entonces $K_a \cong_R R$ en todo caso $R_{f,\sigma} \otimes_R K_a$ es libre y por lo tanto $R_{f,\sigma} \otimes_R M$ también lo es por el lema anterior. \square

En la siguiente prueba usamos el siguiente lema

Lema 14. *Supongamos R un dominio conmutativo con una colección de automorfismos σ_i , $i \in I$, y supongamos que $F \subset R$ es $\mathbb{Z}/p\mathbb{Z}$ con p primo o \mathbb{Z} dependiendo de la característica de R . σ_i se extienden a $R[x]$ haciendo $\sigma_i(x) = x$. Tomamos $f \in R[x] - 0$ arbitrario. Entonces existe $g \in T[x]$ que no divide a ningún polinomio en $S_{f,\sigma} \in R[x]$.*

Demostración. Podemos reemplazar R por la clausura algebraica k del cuerpo de fracciones de R (en efecto se sabe que σ_i se pueden extender a k).

Construimos $f_0 = x$ y $f_n = \prod_{k < n} f_k + 1$ polinomios no constantes en $T[x]$, y se observa que si $k \neq n$ entonces f_n y f_k no tienen raíces en común.

Suponemos por contradicción que $f_n \mid g_n$ con $g_n \in S_{f,\sigma}$, elegimos una raíz r de f_n entonces r es raíz de g_n y por lo tanto $r = \sigma(a_n)$ con a_n una raíz de f , como f_n es un polinomio en T y T es σ_i -invariante entonces a_n es raíz de f_n . El conjunto de raíces de f es finito luego para una subsucesión de f_n , $a_n = a$. Esto contradice la construcción de f_n . \square

Proposición 21. *Sea R un dominio conmutativo y B es una imagen homomórfica de una extensión PBW-torcida biyectiva de R , entonces para ${}_B M$ un módulo simple y $a \in \text{End}_B({}_B M)$ existe una única estructura de $R[x]$ -módulo derecho sobre M que extiende a la de B y tal que $xm = a(m)$. Con esta estructura existe un polinomio $f \in R[x]$ tal que para todo $m \in M$ existe $g \in S_{f,\sigma}$ con $g(m) = 0$.*

Demostración. $C = B[x]$ es la imagen homomórfica de una extensión PBW-torcida biyectiva sobre $R[x]$. Si $a \in \text{End}_B({}_B M)$ entonces hay una única estructura de C -módulo derecho sobre M que extiende la de ${}_B M$ y tal que $xm = a(m)$. Y por el lema 13 existe $f \in R[x]$ no nulo tal que $N = R[x]_{f,\sigma} \otimes_R M$ es libre. Tomemos $F = \mathbb{Z}/p\mathbb{Z}$ o $F = \mathbb{Z}$ con p primo dependiendo de la característica de R , tal que $F \subset R$ es el subgrupo aditivo generado por 1. Entonces existe $g \in F[x]$ tal que g no divide ningún polinomio en $S_{f,\sigma}$ por el lema anterior y por lo tanto $g \notin U(R[x]_{f,\sigma})$.

Ahora supongamos que $N \neq 0$ entonces el morfismo de $R[x]_{f,\sigma}$ -módulos $\beta(n) = gn$ no es sobreyectivo (pues N es libre). Y por otro lado para $h \in R[x]_{f,\sigma}$ y $m \in M$ se tiene $\beta(h \otimes m) = h \otimes gm$, como las imágenes de F en B pertenecen al centro entonces el mapa $m \mapsto gm$ es un morfismo de B -módulos, y como ${}_B M$ es simple entonces es 0 o invertible, no puede ser invertible pues se obtiene una contradicción, y si es 0 entonces $g \in R[x]$ cumple lo que se requiere.

Si suponemos ahora que $N = 0$ entonces es conocido que M es de $S_{f,\sigma}$ -torsión. Esto es precisamente la conclusión del teorema. \square

Proposición 22. *Sea k un cuerpo y B es una imagen homomórfica de una extensión PBW-torcida biyectiva de k , entonces $\text{Rad}(B) = \text{Nil}(B)$.*

Demostración. Tomamos $C = B[x]$ que es imagen homomórfica de una extensión PBW-torcida biyectiva de $k[x]$, y tomamos $a \in \text{Rad}(B)$.

Suponemos que $C(1 - ax) \neq C$, entonces hacemos ${}_C M = C/I$ donde I es un ideal derecho maximal de C que contiene a $C(1 - ax)$ entonces ${}_C M$ es simple y si m_1 es la imagen de 1 en M entonces $(1 - ax)m_1 = 0$.

Consideramos la función de M en si mismo $X : m \mapsto xm$ como $x \in Z(C)$ es un elemento del centro de C , se tiene que X es un C -endomorfismo y es distinto de 0 pues $X(am_1) = m_1$. Concluimos que tiene inverso Y , y se tiene que para algún polinomio $g \in k[x]$, $g(Y)m_1 = 0$ en el sentido de la proposición anterior. Observamos que sin pérdida de generalidad $g(0) = 1$ pues Y es inyectiva (y k es cuerpo).

Para un polinomio $f = \sum r_n x^n \in k[x]$ denotamos $f(a)m_1 = \sum r_n a^n m_1$ y observamos que $f(a)m_1 = f(Y)m_1$ para cualquier polinomio f . En efecto esta identidad es k -lineal en f luego basta verificarla para $f = x^n$ en este caso aplicando el morfismo X^n se obtiene m_1 en ambos lados, como X es inyectiva se tiene la identidad. En particular $g(a)m_1 = (1 + g_1(a)a)m_1 = g(Y)m_1 = 0$ esto contradice $a \in \text{Rad}(B)$.

Esta contradicción muestra $C(1 - ax) = C$, pero en este caso para un polinomio $h \in B[x]$, $h(x)(1 - ax) = 1$ e igualando los coeficientes se puede ver que $a^n = 0$. Es decir $\text{Rad}(B)$ es un ideal nil, y como B es noetheriano se obtiene $\text{Rad}(B) = \text{Nil}(B)$ como se busca. \square

Bibliografía

- [1] **Dixmier, J.** *Enveloping Algebras* North-Holland.(1977).
- [2] **Goodearl, K., R.** *Prime ideals in skew polynomial rings and quantized Weyl algebras*, J. of Algebra, 150, 1992, 324-377.
- [3] **Goodearl, K., R. & Letzter, S.**, *Prime Ideals in skew and q-skew polynomial rings*, Memoirs of American Mathematical Society 1994, American Mathematical Society.
- [4] **Goodearl, K., R. & Warfield JR., R., B.** *An Introduction to Noncommutative Noetherian Rings*. London Mathematical Society (2004).
- [5] **Lezama, O. & Gallego C.** *Gröbner bases for ideals of sigma-PBW extensions*, Communications in Algebra, 39 (1), 2011, 50-75.
- [6] **Lezama, O. & Reyes, M.**, *Some homological properties of skew PBW extensions*, Communications in Algebra, 42, 2014, 1200-1230.
- [7] **McConnell, J. & Robson, J.**, *Noncommutative Noetherian Rings*, Graduate Studies in Mathematics 2001, American Mathematical Society.
- [8] **Warfield, R., B. Jr.**, *Prime ideals in ring extensions*, J. London Mathematical Society 28 (1983).