NOTAS DE MATEMATICAS

Nº 49

ANILLOS CON ALGORITMO DEBIL

POR

FRANCISCO RIVERO

UNIVERSIDAD DE LOS ANDES

FACULTAD DE CIENCIAS

DEPARTAMENTO DE MATEMATICA

MERIDA-VENEZUELA

1982

UNIVERSIDAD DE LOS ANDES
FACULTAD DE CIENCIAS
DEPARTAMENTO DE MATEMATICA

"ANILLOS CON ALGORITMO DEBIL"

TESIS DE GRADO PRESENTADO POR EL LIC. FRANCISCO RIVERO M. PARA OPTAR AL EL TITULO DE MAGISTER SICIENTIARUM EN MATEMATICA DIRIGIDA POR EL DR. RAJ MARKANDA.

AGRADECIMIENTO

Al Profesor Raj Markanda por su valiosa ayuda en la elaboración de este trabajo.

A todos los profesores de la Maestría por haberme enseñado los conocimientos necesarios, para poder alcanzar esta etapa de mi formación.

A la señora Elide Ramírez y a la señorita Eunice Nava, por su paciencia y dedicación mostradas en el mecanografiado de esta tesis.

Finalmente al Consejo de Desarrollo Científico y Humanístico, por encargarse de financiar este trabajo.

INTRODUCCION

El objeto de este trabajo, consiste en estudiar los anillos con algoritmo de división.

En el capítulo 1, se estudia el algoritmo clásico de la división, el cual aparece por vez primera en "Los Elementos " de Euclides. Más adelante se obtiene el Algoritmo Mínimo con respecto a un algoritmo de división, y posteriormente se estudian aquellos anillos en donde el resto de la división es único. La última parte está dedicada a las funciones de grado y su relación con los anillos Euclideanos de restos - únicos (Corolario 22).

En el capítulo 2, se da una generalización de Dominio de - Ideales Principales, como lo son los Anillos de Ideales Libres. La manera de obtener este tipo de anillos, es por medio de la noción de Algoritmo Débil, que aparece por primera vez en Cohn [7].

El ejemplo clásico de Anillo de Ideales Libres, lo constituye el algebra libre asociativa $k < x_1,\ldots,x_n)$, (pág. 110).

El resultado principal de este capítulo viene dado en el Teorema 36, en donde se da una caracterización de los anillos con algoritmo débil.

El capítulo 3, consiste en resolver algunos problemas bastante relacionados con el capítulo anterior, como lo es la generalización para módulos, de el algoritmo débil.

CAPITULO 1

Este capítulo se divide en dos partes la primera trata del algoritmo de división sobre un anillo cualquiera y como se obtiene, a partir de éste, el algoritmo euclideano. Después se estudia algoritmo de división, en donde el resto es único y se obtienen una serie de propiedades.

La segunda parte toca otro tipo de función sobre un anillo, que es la función de grado. Después de estudiar sus propiedades y algunos ejemplos, como el anillo de división K y anillos de polinomio no conmutativo $K[x;\alpha\ \delta]$, se demuestra que estos son los únicos anillos que poseen función de grado.

Finalmente, se establece una relación entre las dos partes, al probar que (bajo ciertas condiciones) un anillo con algoritmo de división de restos únicos debe ser de la forma K o $K[x;\ \alpha,\ \delta]$.

ALGORITMO DE DIVISION

En esta sección, se expone el algoritmo clásico de la división y también se estudiarán aquelllos anillos en donde el resto de la división es único.

A lo largo de esta sección, R será un anillo unitario y $R^* = R - \{0\}$

DEFINICION 1: Una función $\phi: R^* \to \mathbb{N} \cup \{0\}$ se dice algoritmo del tipo 1, si para todo $a,b \in R$ con $b \neq 0$, existe $q,r \in R$ tal que:

$$a = bq + r \quad , \quad \text{con} \quad \phi(r) < \phi(b)$$

DEFINICION 2: Una función $\phi: R^* \to \mathbb{N} \cup \{0\}$ se dice algoritmo del tipo 2, si para todo $a,b \in R^*$ con $\phi(a) \geq \phi(b)$, existe $C \in R$ tal que:

$$\phi(a - bc) < \phi(a)$$

PROPOSICION: Todo algoritmo del tipo 1 es del tipo 2 y reciprocamente.

DEMOSTRACION: Un algoritmo del tipo 1, es del tipo 2. Reciprocamente, sea ϕ un algoritmo del tipo 2 entonces, sea $a,b \in R$ y $b \neq 0$, se tiene 3 casos:

i) Si $a = 0$, ponemos $a = b.0 + 0$ con $q = 0$, $r = 0$.

ii) Si $a \neq 0$ y $\phi(a) < \phi(b)$, podemos escribir

$a = b.0 + a$ con $q = 0$, $r = a$ y $\phi(r) = \phi(a) < \phi(b)$

iii) $a \neq 0$, $b \neq 0$ y $\phi(a) \geq \phi(b)$.

Se elije $q_1 \in R$ tal que $\phi(a - bq_1)$ sea mínimo. Entonces afirmamos que

$$\phi(a - bq_1) < \phi(b)$$

Supongamos que

$$\phi(a - bq_1) \geq \phi(b)$$

Luego, por la definición 2, existe un $C \in R$ tal que:

$$\phi(a - bq_1 - bc) < \phi(a - bq_1)$$

$$\phi(a - b(q_1 + c)) < \phi(a - bq_1)$$

lo cual es una contradicción, pues $\phi(a - bq_1)$ es mínimo.

NOTA: Un algoritmo del tipo 1 o equivalentemente del tipo 2, se llama ALGORITMO DE DIVISION.

DEFINICION 4: Un anillo R que satisface un algoritmo de división relativo a una función ϕ, se dice EUCLIDEANO si se tiene la propiedad

$$\phi(ab) \geq \phi(a) \qquad \forall\ a,b\ ,\ ab \in R^* .$$

A continuación, se demuestra que si se tiene un algoritmo de división sobre un anillo R, se puede construir un nuevo algoritmo de manera que R sea EUCLIDEANO.

DEFINICION 5: Sea R un anillo y $S \subset R^*$, definimos el CONJUNTO DERIVADO, como

$$S' = \{s \in S \mid a + s\,R \subset S \text{ para algún } a \in R\} .$$

TEOREMA 6: Sea R un anillo con algoritmo de división y $\{S_n\}$ la siguiente sucesión definida por recurrencia

$$S_o = R^*$$
$$S_1 = S_o'$$
$$\vdots$$
$$S_{n+1} = S_n'$$

Entonces

$$\bigcap_{n=0}^{\infty} S_n = \phi$$

DEMOSTRACION: Afirmamos que $\theta(x) \geq n \quad \forall\, x \in S_n$ (por inducción).

Para $n = 0$ es cierto $\theta(x) \geq 0 \quad \forall\, x \in R^* = S_o$.

Sea

$$x \in S_n = S_{n-1}'$$

Luego

$$a + x\,R \subset S_{n-1} \qquad \text{para algún } a \in R.$$

De donde,

$$a + xq \in S_{n-1} \qquad \forall\, q \in R\ .$$

Así

$$\theta(a + xq) \geq n-1 \qquad \text{(por hipótesis de inducción).}$$

Por la definición 2 $\exists\, q \in R$ tal que

$$\theta(a + xq) < \theta(x).$$

Por lo tanto

$$\theta(x) \geq n\ .$$

Ahora bien, sea $x \in \bigcap_{n=0}^{\infty} S_n$.

Por lo tanto

$$x \in S_n \qquad \forall\ n\ .$$

Luego

$$\theta(x) \geq n \qquad \forall\ n$$

Pero $\theta(x) \in \mathbb{N} \cup \{0\}$. Hemos llegado a una contradicción.

Por lo tanto

$$\bigcap_{n=0}^{\infty} S_n = \phi$$

TEOREMA 7: Sea R un anillo que satisface un algoritmo de división relativo a una función ϕ. Entonces existe una función

$$\phi: R^* \longrightarrow \mathbb{N} \cup \{0\}$$

tal que

i) $\phi(a) \geq 0 \qquad \forall\, a \in R^*$,

ii) $\phi(1) = 0$

iii) $\phi(ab) \geq \phi(a) \qquad \forall\, a,b \in R^*$

iv) R es euclideano respecto de ϕ.

v) Además ϕ satisface.

$$\phi(a) \leq \theta(a) \qquad \forall\, a \in R^*$$

DEMOSTRACION:

Definimos $\phi: R^* \longrightarrow \mathbb{N} \cup \{0\}$

$$\phi(x) = \max \{ n \mid x \in S_n \}$$

ϕ está bien definida, pues

$$\bigcap_{n=0}^{\infty} S_n = \phi$$

(por teorema 6).

Además $S_o \supset S_1 \supset S_2 \supset \ldots \supset S_n \supset \ldots$

entonces $\phi(x) \geq n \iff x \in S_n$

i) Se verifica por definición

ii) No existe $a \in R$ tal que $a + R \subset R^*$ (puesto que $0 \in a + R$) luego $1 \notin S^1$ y como $1 \in S^\circ$, se tiene $\phi(1) = 0$.

iii) Sean $a,b \in R^*$. Supongamos $\phi(a) = n$. Entonces $a \in S_n$ y por lo tanto existe $c \in R$ tal que $c + aR \subset S'_{n-1}$.

Ahora

$$c + abR \subset C + aR \subset S'_{n-1}$$

luego

$$ab \in S_n \quad y \quad \phi(ab) \geq n = \phi(a)$$

iv) Sean $a,b \in R$, $b \neq 0$.

<u>CASO 1</u>: $a = 0$

$$a = 0b + a \quad y \quad \phi(a) < \phi(b)$$

<u>CASO 2</u>: $\phi(a) \geq \phi(b)$.

Sea

$$\phi(b) = n .$$

Afirmamos que existe $q \in R$ tal que

$$\phi(a + bq) < \phi(b).$$

Si esto no es cierto,

$$\phi(a + bq) \geq \phi(b) = n \qquad \forall\, q \in R$$

luego

$$a + bq \in S_n \qquad \forall q \in R .$$

así

$$a + bR \subset S_n$$

y en consecuencia $b \in S_{n+1} = S_n'$. Entonces $\theta(b) \geq n+1$, lo cual es una contradicción.

v) Sea $a \in R^*$ tal que $\phi(a) = n$, entonces

$$a \in S_n \quad y \quad a \notin S_m \qquad m \geq n + 1$$

Pero

$$a \in S_n \text{ , por lo tanto } \theta(a) \geq n$$

Luego

$$\theta(a) \geq \phi(a) \qquad \forall\, a \in R^* .$$

ALGORITMO MINIMO

DEFINICION 8: Sea R un anillo y Φ una familia de algoritmos de división sobre R, entonces

$$\theta(x) = \min\{\phi(x) \mid \phi \in \Phi\}$$

define un algoritmo de división sobre R y se llama ALGORITMO MINIMO, relativo a la familia Φ .

Para verificar que θ es un algoritmo, sean $a,b \in R^*$ y sea $\phi \in \Phi$ tal que $\phi(b) = \theta(b)$. Como ϕ es un algoritmo, existen $q,r \in R$ tales que:

$$a = bq + r \quad \text{con} \quad r = 0 \quad \text{ó} \quad \phi(r) < \phi(b)$$

Por lo tanto se tiene $r = 0$ ó

$$\theta(r) \leq \phi(r) < \phi(b) = \theta(b)$$

y esto demuestra la hipótesis.

NOTA: Si Φ es la familia de todos los algoritmos definidos sobre R, entonces el algoritmo mínimo θ relativo a Φ es precisamente la función ϕ del teorema 7, ϕ se llama algoritmo mínimo sobre R y se denota por θ_R .

Una caracterización de θ_R viene dada en el teorema siguiente.

TEOREMA 9: Sea ψ: $R^* \longrightarrow \mathbb{N} \cup \{0\}$ un algoritmo. Entonces ψ es el algoritmo mínimo si y sólo si para todo $b \in R$ y $n \in \mathbb{N}$ tal que $n < \psi(b)$ $\}$ $a \in R - Rb$ que cumple

$$\psi(c) \geq n \qquad \forall c \in a + Rb \qquad (*)$$

DEMOSTRACION: Sea ψ: $R \longrightarrow \mathbb{N} \cup \{0\}$ algoritmo mínimo. Sea

$$b \in R \quad y \quad n < \psi(b)$$

Se define

$$\theta: R \longrightarrow \mathbb{N} \cup \{0\}$$

por

$$\theta(x) = \psi(x) \quad \text{si} \quad x \neq b$$

$$\theta(b) = n$$

Entonces $\theta(b) < \psi(b)$ y luego θ no es un algoritmo.

Existen $a, b' \in R$ con $a \notin R\,b'$, tal que:

$$\theta(c) \geq \theta(b') \qquad \forall\, c \in a + Rb' \ .$$

Si $b \neq b'$, se tiene $\theta(b') = \psi(b')$ y $\psi(c) \geq \psi(b')$. Luego ψ no es un algoritmo.

Por lo tanto $b = b'$ y

$$\psi(c) = \theta(c) \geq n = \theta(b) \qquad \forall\, c \in a + Rb \ .$$

Recíprocamente, sea ψ un algoritmo que satisface (*).

Demostraremos que para todo algoritmo

$$\theta: R \longrightarrow \mathbb{N} \cup \{0\}$$

se debe tener

$$\psi(b) \leq \theta(b) \qquad \forall\, b \in R - \{0\}$$

Procediendo por inducción, se asume que

$$\psi(x) \leq \theta(x) \qquad \forall\, x \in R, \quad \text{con } \theta(x) < \theta(b)$$

Si $\theta(b) < \psi(b)$, podemos usar (*) haciendo $n = \theta(b)$ y

luego existe $a \in R-Rb$ tal que

$$\psi(c) \geq n = \theta(b) \qquad \forall c \in a + Rb$$

Ahora bien como θ es algoritmo, existe $c \in a + Rb$ tal que

$$\theta(c) < \theta(b) \leq \psi(c) \qquad (**) .$$

Pero

$\theta(c) < \theta(b)$ implica

$$\psi(c) \leq \theta(c)$$

(por hipótesis de inducción) lo cual contradice (**).

Luego se tiene $\psi(b) \leq \theta(b)$ y esto termina la demostración.

LEMA 10: Sea R euclideano con respecto a un algoritmo ϕ, y sea

$$\phi_*(x) = \min\{\phi(y) \mid y \in Rx\} .$$

Entonces ϕ_* es un algoritmo sobre R y

i) $\phi_*(x) \leq \phi_*(yx) \qquad \forall x,y \in R$

ii) $\phi_*(x) = \phi_*(yx) \iff Rx = Ryx$

DEMOSTRACION: Para demostrar que ϕ_* es un algoritmo, sean $a,b \in R^*$.

Por definición, existe $c \in Rb$ tal que

$$\phi_*(b) = \phi(c)$$

y como ϕ es un algoritmo, existen $r, q_1 \in R$ tales que

$$a = q_1 c + r \quad \text{con} \quad r = 0 \quad \text{ó} \quad \psi(r) < \phi(c).$$

Pero $c \in Rb$ implica $a = bqq_1 + r$ para algún $q \in R$ y $r = 0$ ó $\phi_*(r) \leq \phi(r) < \phi(c) = \phi_*(b)$. La prueba de i) y ii) es trivial.

TEOREMA 11: Sea R un anillo con algoritmo ϕ. Sea $b \in R$ que satisface $\phi(b) = \phi_*(b)$ y $A_{nn}(b) = \{x \in R \mid xb = 0\}$. Entonces $R/A_{nn}(b)$ es euclideano y

$$\phi(qb) \geq \phi(b) + \theta_{R/A_{nn}(b)}\,(q + A_{nn}(b))$$

para todo $q \in R$.

DEMOSTRACION: Tenemos

$$\phi(qb) \geq \phi_*(b) = \phi(b) \qquad \forall\ q \in R\ .$$

Definimos

$$\mu: R^* \longrightarrow \mathbb{N} \cup \{0\}$$

$$\mu(q) = \phi(qb) - \phi(b)$$

Así μ está bien definida, y además, si $q-q' \in A_{nn}(b)$.

Se tiene

$$qb = q'b$$

y esto implica

$$\mu(q) = \mu(q')$$

Por lo tanto μ induce una aplicación

$$\lambda: R/A_{nn}(b) \longrightarrow \mathbb{N} \cup \{0\}$$

$$\lambda(\bar{q}) = \phi(qb) - \phi(b)$$

Afirmamos que λ es un algoritmo de división. En efecto, sean $\bar{r}$, $\bar{s} \in R/A_{nn}(b)$, con $\bar{s} \neq 0$. Por ser ϕ algoritmo, existen q, $c \in R$ tales que

$$rb = qsb + c \quad \text{con} \quad c = 0 \ \text{ó} \ \phi(c) < \phi(sb).$$

Ahora bien,

$$\lambda(\overline{r - qs}) = \phi((r - qs)b) - \phi(b)$$

$$= \phi(c) - \phi(b)$$

$$\lambda(\bar{s}) = \phi(sb) - \phi(b) .$$

Restando se obtiene

$$\lambda(\overline{s - qs}) - \lambda(\bar{s}) = \phi(c) - \phi(sb) < 0$$

Por lo tanto

$$\lambda(\overline{r - qs}) < \lambda(\bar{s})$$

y esto implica $R/A_{nn}(b)$ es euclideano.

Finalmente

$$\phi(qb) = \phi(b) + \lambda(\bar{q})$$

$$\geq \phi(b) + \theta_{R/A_{nn}(b)}\ (q + {}^{R}/_{A_{nn}(b)})$$

lo cual da fin a la demostración.

COROLARIO 12: Sea R un anillo euclideano sin divisores de cero. Entonces

$$\theta_R(ab) \geq \theta_R(b) + \theta_R(a)$$

para todo $a,b \in R^*$.

DEMOSTRACION: En el teorema 11, tomamos $\phi = \theta_R$. Entonces

$$\theta_R(ab) \geq \theta_R(b) + \theta_{R/R_{nn}(b)}\ (a + A_{nn}(b)).$$

Pero R no tiene divisores de cero, y en consecuencia $A_{nn}(b) = (0)$, si $b \neq 0$. Luego $R/A_{nn}(b) = R$, y de aquí se obtiene el resultado.

ALGORITMO CON RESTO UNICO

DEFINICION 13: Sea R un anillo. Una función $\phi: R^* \to \mathbb{N} \cup \{0\}$

se llama un ALGORITMO CON RESTO UNICO, si para todo $a,b \in R$, existe un único elemento $\gamma \in a + Rb$ que satisface

$$\gamma = 0 \quad \text{ó} \quad \phi(\gamma) < \phi(b).$$

EJEMPLO: $R = k|x|$, con k un campo y ϕ la función de grado.

PROPOSICION 14: Un algoritmo $\phi: R^* \to \mathbb{N} \cup \{0\}$ es de resto único si y sólo si se cumple

i) $x, y \in R^*$ con $x \neq y$

$$\phi(x-y) \leq \max \{\phi(x), \phi(y)\}$$

ii) $x, y, yx \in R^*$.

$$\phi(x) \leq \phi(yx).$$

DEMOSTRACION:

i) Sea $a = x$, $b = x-y$. Luego $x,y \in a + Rb$ y por unicidad, no se puede tener al mismo tiempo

$$\phi(x) < \phi(b), \text{ y } \phi(y) < \phi(b),$$

entonces se cumple

$$\phi(x) \geq \phi(b) \quad \text{ó} \quad \phi(y) \geq \phi(b),$$

lo cual implica

$$\phi(x-y) \leq \max\{\phi(x), \phi(y)\}.$$

ii) Si se supone $\phi(yx) < \phi(x)$. Entonces $r = yx$ y $r = 0$ son dos elementos de $0 + Rx$ que satisfacen

$$r = 0 \quad \text{ó} \quad \phi(r) < \phi(x)$$

lo cual es una contradicción (ϕ es algoritmo de restos únicos).

Luego

$$\phi(yx) \geq \phi(x) \qquad \forall\ x,y,\ yx \in R^* .$$

Recíprocamente, supongamos que i) y ii) son válidos.

Sean $s,r \in a + Rb$, entonces si

$$r = 0 \quad \text{ó} \quad \phi(r) < \phi(b)$$

y

$$s = 0 \quad \text{ó} \quad \phi(s) < \phi(b)$$

Se debe probar $r = s$.

CASO 1: $r = 0$. Se tiene que $s-r \in Rb$, luego $s \in Rb$ y por la condición ii) se deduce $\phi(s) \geq \phi(b)$ y esto obliga a hacer $s = 0$.

Si $s = 0$ se procede de la misma forma.

CASO 2: $\phi(r) < \phi(b)$ y $\phi(s) < \phi(b)$ puesto que $s-r \in Rb$,

podemos hacer $s - r = qb$, para algún $q \in R^*$.

Entonces

$$\max\{\phi(r), \phi(s)\} < \phi(b) \leq \phi(qb) = \phi(r-s).$$

Ahora bien, si se supone $qb \neq 0$ se tiene la desigualdad

$$\phi(r-s) \leq \max\{\phi(r), \phi(s)\}.$$

Luego, se llega a una contradicción, y por lo tanto debe ser $qb = r-s = 0$. Con esto termina la demostración.

COROLARIO 15: Si ϕ es un algoritmo de restos únicos entonces ,

i) $\phi(x) = \phi(-x) \quad \forall\ x \in R.$

ii) $\phi(x+y) = \max\{\phi(x), \phi(y)\}$

Si $\phi(x) \neq \phi(y)$ y $x,y \in R^*$.

DEMOSTRACION:

i) $\phi(x) \leq \phi(-1x) = \phi(-x)$ por prop. 14,ii)

$\phi(-x) \leq \phi(-1(-x)) = \phi(x)$ igualmente.

De esto se sigue $\phi(x) = \phi(-x)$.

ii) Si $\phi(x) > \phi(y)$, se tiene

$$x = (x + y) - y$$

$$\phi(x) \leq \max\{\phi(x+y),\ \phi(y)\}$$

lo cual implica

$$\phi(x) \leq \phi(x + y)$$

y así

$$\max\{\phi(x),\ \phi(y)\} = \phi(x) \leq \phi(x + y). \qquad (*)$$

Por otro lado,

$$\phi(x + y) \leq \max\{\phi(x),\ \phi(-y)\}$$

por proposición 14 i).

Pero $\phi(-y) = \phi(y)$, y entonces se obtiene la desigualdad

$$\phi(x + y) \leq \max\{\phi(x),\ \phi(y)\}. \qquad (**)$$

Combinando las desigualdades (*) y (**) se obtiene el resultado deseado.

TEOREMA 16: Sea ϕ un algoritmo de restos únicos tal que sea sobreyectiva (es decir $\phi(R^*) = \mathbb{N} \cup \{0\}$). Entonces ϕ es el algoritmo mínimo θ_R sobre R. Además, para $b,q \in R$. Se tiene

$$\theta_R(qb) = \theta_R(b) + \theta_{R/A_{nn}}(b)\ (q + A_{nn}(b)).$$

DEMOSTRACION: Para demostrar que ϕ es igual a θ_R, nos basamos en el teorema 9. Para ello, sea $b \in R$ y $n \in \mathbb{N}$ tal que $n < \phi(b)$. Puesto que ϕ es sobreyectiva, existe $a \in R^*$ que satisface

$$\phi(a) = n .$$

Además

$$\phi(xb) \geq \phi(b) > n \qquad \forall\ x \in R^*$$

y de esto se sigue $a \notin Rb$ ó equivalentemente

$$0 \notin a + Rb.$$

Luego el único elemento r de $a + Rb$ que satisface $\phi(r) < \phi(b)$ es a. Por lo tanto $\phi(r) \geq n$ para todo $r \in a + Rb$ y en consecuencia $\phi = \theta_R$.

Para demostrar la segunda afirmación, se sabe (por el Teorema 11) que existe un algoritmo

$$\lambda: R/A_{nn}(b) \to \mathbb{N} \cup \{0\}$$

para $b,q \in R^*$, definido por

$$\lambda(\bar{q}) = \theta_R(qb) - \theta_R(b).$$

Probaremos que $\lambda = \theta_{R/A_{nn}(b)}$ en dos partes:

i) λ es un algoritmo de restos únicos.

ii) λ es sobreyectiva.

i) Sean $\bar{q},\bar{p} \in R/_{A_{nn}(b)}$, con $\bar{p} \neq \bar{q}$.

Entonces

$$\lambda(\bar{p} - \bar{q}) = \theta_R((p - q)b) - \theta_R(b)$$

$$= \theta_R(qb - pb) - \theta_R(b)$$

$$\leq \max\{\theta_R(qb), \theta_R(pb)\} - \theta_R(b)$$

$$= \max\{\lambda(\bar{q}), \lambda(\bar{p})\}$$

$$\lambda(\bar{p}\,\bar{q}) = \theta_R(pqb) - \theta_R(b)$$

$$\geq \theta_R(qb) - \theta_R(b)$$

$$= \lambda(\bar{q}) \ .$$

Entonces por la proposición 14 λ es un algoritmo de restos únicos, y i) queda demostrado.

ii) Sea $n \in \mathbb{N} \cup \{0\}$. Por la sobreyectividad de θ_R , existe $c \in R$ tal que

$$\theta_R(c) = \theta_R(b) + n \ . \qquad (*)$$

Si $c \in Rb$, entonces $c = rb$ y se tiene

$$\mu(\bar{r}) = n$$

y en este caso, queda probado.

Si c no está en Rb, entonces $c = rb + d$ y además se tiene

$$\theta_R(d) < \theta_R(b)$$

(θ_R es algoritmo de restos únicos).

Luego

$$\theta_R(c) \leq \max\{\theta_R(rb), \theta_R(d)\} .$$

Pero

$$\theta_R(rb) \geq \theta_R(b) > \theta_R(d).$$

Y usando el corolario 15 ii) se tiene

$$\theta_R(c) = \max\{\theta_R(rb), \theta_R(d)\} = \theta_R(rb).$$

Así de nuevo $\mu(\bar{r}) = n$.

<u>COROLARIO 17</u>: Sea R un anillo sin divisores de cero y con algoritmo de restos únicos sobreyectiva, entonces

$$\theta_R(ab) = \theta_R(a) + \theta_R(b) \qquad \forall\, a,b \in R^*$$

DEMOSTRACION: Consecuencia directa del teorema anterior.

FUNCION DE GRADO

DEFINICION 18: Sea R un anillo. Una función

$$d: R \to \mathbb{N} \cup \{0\}$$

se dice función de grado sobre R, si

D.1. $\forall a \in R^*$, $d(a) \geq 0$, y $d(0) = -\infty$

D.2. $d(a-b) \leq \max\{d(a), d(b)\}$

D.3. $d(ab) = d(a) + d(b)$.

NOTA: De esta definición se derivan los siguientes hechos:

i) $d(1) = 0 = d(-1)$ (por D.3).

ii) $d(a) = d(-a)$ (por D.2).

iii) $d(a + b) \leq \max\{d(a), d(b)\}$ y si $d(a) \neq d(b)$ entonces

$$d(a + b) = \max\{d(a), d(b)\}$$

Véase la demostración en el COROLARIO 15 ii).

iv) R es un dominio de integridad.

EJEMPLO: $R = k[x]$, el anillo de polinomios sobre un cuerpo k, ó mas generalmente, k un anillo de división.

Si

$$f = a_o + xa_1 + \ldots + x^n a_n \quad (a_i \in k)$$

entonces

$$d(f) = \max\{i \mid a_i \neq 0\}$$

es la función de grado.

A continuación, se estudia un ejemplo de anillo, que es una generalización de $k[x]$, en donde la indeterminada x no conmuta con los elementos de k.

DEFINICION 19: Sea R,S anillos, tal que R es subanillo de S. Sea $x \in S$. El anillo de polinomio no conmutativo A, es aquel generado por R y x, en donde todo elemento $f \in A$, se expresa de manera única

$$f = a_o + xa_1 + \ldots + x^n a_n \qquad (a_i \in R) \qquad (*)$$

y además

i) la función

$$d(f) = \max\{i \mid a_i \neq 0\}$$

es una función de grado.

ii) Para todo $a \in R$, existe a^α, $a^\delta \in R$ tal que

$$ax = xa^\alpha + a^\delta .$$

NOTA: Puesto que la representación (*) es única se tiene lo siguiente:

1) a^α, a^δ están unicamente determinados por a.

2) $a^{\alpha} = 0 \quad <=> \quad \alpha = 0$.

3) Usando la ley distributiva en A se tiene

$$(a+b)x = x(a+b)^{\alpha} + (a+b)^{\delta}$$

$$ax + bx = x(a^{\alpha} + b^{\alpha}) + a^{\delta} + b^{\delta}$$

igualando ambos términos queda

$$(a+b)^{\alpha} = a^{\alpha} + b^{\alpha}$$

$$(a+b)^{\beta} = a^{\beta} + b^{\beta}$$

4) Usando la ley asociativa para el producto en A, se deduce:

$$\begin{aligned} a(bx) &= a(xb^{\alpha} + b^{\delta}) \\ &= a(xb^{\alpha}) + ab^{\delta} \\ &= (ax)b^{\alpha} + ab^{\delta} \\ &= xa^{\alpha} b^{\alpha} + a^{\delta} b^{\delta} + ab^{\delta} \end{aligned}$$

$$(ab)x = x(ab)^{\alpha} + (ab)^{\delta}$$

igualando queda

$$(ab)^{\alpha} = a^{\alpha} b^{\alpha}$$

$$(ab)^{\delta} = a^{\delta} b^{\alpha} + ab^{\delta}$$

5) Finalmente, haciendo a = b = 1, y usando la ley de

cancelación, ya que R es dominio de integridad se concluye

$$1^{\alpha} = 1^{\alpha}\, 1^{\alpha} \quad \Rightarrow \quad 1^{\alpha} = 1$$

$$1^{\delta} = 1^{\delta} + 1^{\delta} \quad \Rightarrow \quad 1^{\delta} = 0 \ .$$

Entonces queda demostrado que la aplicación

$$\alpha: R \to R$$

es un endomorfismo, y δ una α-derivación.

El anillo A queda completamente determinado cuando R, α y δ estan dudas.

En lo sucesivo, A se denota por

$$A = R[x;\ \alpha,\ \delta] \ .$$

TEOREMA 20: El anillo de polinomio no conmutativo $k[x;\ \alpha,\ \delta]$, donde k = anillo de división, satisface el algoritmo de división relativo a la función de grado usual.

DEMOSTRACION: Sean $a,b \in k[x;\ \alpha,\ \delta]$, entonces

$$a = a_o + xa_1 + \ldots + x^n a_n$$

$$b = b_o + xb_1 + \ldots + x^m b_m$$

$$(a_n \neq 0,\ b_m \neq 0 \ ,\ y \ \ n \geq m) \ .$$

Entonces

$$d(a-b\ b_m^{-1}\ x^{n-m}a_n) < n = d(a)$$

y en virtud de esto, d es un algoritmo de división (POR DEFINICION 2).

Estamos en condiciones de demostrar el siguiente.

TEOREMA 21: Sea R un anillo con algoritmo de división relativo a una función de grado. Entonces R es un cuerpo (ó anillo de división) k, ó $R = k[x; \alpha, \delta]$.

Reciprocamente todo anillo de división o cuerpo k, o anillo $k[x; \alpha, \delta]$ tal que $d(x) > 0$ para alguna función de grado, satisface el algoritmo de división.

DEMOSTRACION: (=>) Sea d la función de grado definida sobre R, la cual satisface el algoritmo de división. Consideremos

$$k = \{a \in R \mid d(a) \leq 0\} .$$

k es un subanillo de R.

En efecto, sean $a,b \in k$. Luego

$$d(a-b) \leq \max\{d(a), d(b)\} \leq 0$$

$$d(ab) = d(a) + d(b) \leq 0 .$$

Entonces $a - b \in k$, y $ab \in k$ con lo cual queda probado.

Además, dado $a \in k^*$, se tiene $d(a) = 0$. Por ser d algoritmo de división, existe $b \in k$ tal que

$$d(ab - 1) < d(a) = 0.$$

luego

$$ab - 1 = 0$$

ó $$ab = 1$$

y

$$d(b) = 0 \Rightarrow b \in k^* .$$

Hemos demostrado que todo elemento no cero de k tiene inverso, bajo el producto. Luego k es un anillo de división, o k es un cuerpo, si R es conmutativo.

Si R no tiene elementos de grado positivo $R = k$, y se sigue el resultado.

Si R tiene elementos de grado, positivo, sea $x \in R$, tal que $d(x)$ es mínimo. Entonces, afirmamos que todo elemento f de R se expresa de la forma

$$f = a_o + xa_1 + \ldots + x^n a_n \qquad (a_i \in k). \quad (*)$$

Supongamos que existe $b \in R$ que no se escribe de esta manera. Asumamos, de una vez, que $d(b)$ es mínimo. Entonces,

por el algoritmo de división, existe $q \in R$ tal que

$$d(b - xq) < d(x)$$

Por la elección de x, se sigue que

$$b - xq \in k \qquad (**)$$

y por lo tanto

$$b = xq + a \quad \text{con} \quad a \in k.$$

Se tiene

$$d(q) < d(x) + d(q) = d(xq)$$

y

$$d(xq) = d(b-a) \leq \max\{d(b), d(a)\} = d(b) .$$

Luego $d(q) < d(b)$, y por la elección de b, q es de la forma

$$q = \sum x^i a_i \qquad (a_i \in k).$$

Sustituyendo esto en (**) obtenemos

$$b = \sum x^{i+1} a_i + a .$$

Lo cual contradice la definición de b y por lo tanto todo elemento en R es de la forma (*). Además, esta representación es única, ya que si un elemento a tiene dos representaciones

por el algoritmo de división, existe $q \in R$ tal que

$$d(b - xq) < d(x)$$

Por la elección de x, se sigue que

$$b - xq \in k \qquad (**)$$

y por lo tanto

$$b = xq + a \quad \text{con} \quad a \in k.$$

Se tiene

$$d(q) < d(x) + d(q) = d(xq)$$

y

$$d(xq) = d(b-a) \leq \max\{d(b), d(a)\} = d(b) .$$

Luego $d(q) < d(b)$, y por la elección de b, q es de la forma

$$q = \sum x^i a_i \qquad (a_i \in k).$$

Sustituyendo esto en (**) obtenemos

$$b = \sum x^{i+1} a_i + a .$$

Lo cual contradice la definición de b y por lo tanto todo elemento en R es de la forma (*). Además, esta representación es única, ya que si un elemento a tiene dos representaciones

$$a = a_o + xa_1 + \ldots + x^n a_n$$

$$a = b_o + xb_1 + \ldots + x^n b_n$$

se tendría

$$(a_o - b_o) + x(a_1 - b_1) + \ldots + x^n(a_n - b_n) = 0 \ .$$

Usando propiedades de la función de grado d, obtenemos

$$d(x^n) = d(x^n(a_n - b_n)) \leq \max_{1 \leq i \leq n-1} \{d(x^i(a_i - b_i))\}$$

y luego

$$n\, d(x) \leq (n-1)\, d(x)$$

lo cual contradice el hecho de ser $d(x) > 0$. Entonces si R es un anillo conmutativo $R = k[x]$ y el teorema queda probado en este caso.

Si R no es conmutativo, sea $a \in k$ debemos tener

$$ax = xa_1 + a_2 \ . \qquad (***)$$

(Ambas expresiones tienen el mismo grado) de donde

$$d(a_2) \leq \max\{d(ax),\ d(xa_1)\} =$$

$$= \max\{d(x),\ d(xa_1)\}$$

y así

$$d(a_2) \leq d(x) \ .$$

Si $d(a_2) = d(x)$, entonces a_2 es de la forma(*) y por lo tanto se factoriza en (***).

Luego, debe ser $d(a_2) < d(x)$ y así $d(a_2) \leq 0$.

También,

$$d(ax) \geq d(x) + d(a_1).$$

Por lo tanto

$$d(a_1) \leq d(ax) - d(x) = 0 .$$

Y así

$$a_1, a_2 \in k .$$

Por la unicidad de la representación (***) se deduce (ver la nota de la definición 19) que la aplicación

$$\alpha: a \to a_1$$

es un endomorfismo.

Y

$$\delta: a \to a_2$$

es una α-derivación.

Luego $R = k[x; \alpha, \delta]$, como se esperaba.

(<=) Reciprocamente, si R es un anillo de división, con una función de grado, esta es un algoritmo de división.

Sea $R = k[x; \alpha, \delta]$ con una función de grado d, tal que

$d(x) = \lambda > 0$.

Entonces los grados de x^n son diferentes para cada n y por lo tanto, si se tiene un elemento

$$a = a_o + xa_1 + \ldots + x^n a_n$$

$$d(a) = d(a_o + xa_1 + \ldots + x^n a_n)$$

$$= \max_{1 \leq i \leq n} \{d(x^i a_i)\} = n\lambda .$$

(Véase la nota a la definición 18).

En virtud de esto, podemos dividir todos los grados entre λ, para obtener la función de grado usual. Después, la demostración se obtiene directamente del **TEOREMA** 20.

COROLARIO 22: Sea R un anillo sin divisores de cero, y con un algoritmo de restos únicos ϕ sobreyectivo.

Entonces

i) La función

$$d(x) = \begin{cases} \phi(x) , & \text{si } x \neq 0 \\ -\infty , & \text{si } x = 0 \end{cases}$$

es una función de grado sobre R.

ii) R es de la forma k ó $k[x; \alpha, \delta]$ (k - anillo de división o cuerpo).

DEMOSTRACION:

i) Ciertamente, d satisface las condiciones D.1, D.2 y D.3 de la definición 18.

D.1 es consecuencia de la definición, D.2 aparece en la PROPOSICION 14 i) y D.3 se demuestra en el COROLARIO 17.

ii) Consecuencia directa del teorema anterior.

CAPITULO 2

ALGORITMO DEBIL

En el capítulo 1, estudiamos los anillos en donde se define un algoritmo de división. Este tipo de anillos tiene propiedades bastante buenas como por ejemplo ser Dominio de Ideales principales, dominio de factorización única etc.

Una generalización de Dominio de Ideales principales, son los Anillos de Ideales Libres, en los cuales todo ideal es libre.

Para obtener este tipo de anillo, usamos una función con propiedades más "débiles" que la de división, como es una fitración.

Luego, definimos un algoritmo débil, (que es equivalente al algoritmo Euclideano en el caso conmutativo) y a partir de éste llegamos a los Anillos de Ideales Libres.

A continuación, se estudia el Anillo Graduado asociado a R y se expresa el algoritmo débil en estos anillos.

Finalmente, se da una caracterización de los anillos con algoritmo débil.

DEFINICION 1. Sea R un anillo con 1. Una filtración, es una función

$$v: R^* \longrightarrow \mathbb{N} \cup \{0\}, \quad R^* = R-\{0\}$$

con las siguientes propiedades:

v.1. $v(x) \geq 0 \quad \forall x \in R^*$, $v(0) = -\infty$,

v.2. $v(x-y) \leq \max\{v(x), v(y)\}$,

v.3. $v(x,y) \leq v(x) + v(y)$,

v.4. $v(1) = 0$.

Si bien una filtración no es una función de grado, por comodidad en el lenguaje, llamaremos grado de x a $v(x)$.

EJEMPLO. Todo anillo posee la filtración trivial

$$v(x) = \begin{cases} 0 & \text{si } x \neq 0, \\ -\infty & \text{si } x = 0. \end{cases}$$

NOTA: A partir de la definición 1, se tienen las siguientes propiedades:

a) $v(x) = v(-x)$

$v(0-x) \leq \max\{v(0), v(x)\} = v(x)$ (por v.2)

de donde

$$v(-x) \leq v(x).$$

En particular,

$$v(-1) \leq v(1) = 0 \quad ,$$

y por lo tanto,

$$v(-1) = 0.$$

Luego,

$$v(x) = v(-1.(-x))$$

$$\leq v(-1) + v(-x) \qquad \text{(por v.3)}$$

y de aquí se tiene la desigualdad

$$v(x) \leq v(-x)$$

con lo cual a) queda demostrado.

b) $v(x+y) \leq \max\{v(x), v(y)\}$.

Por v.2 se tiene

$$v(x-(-y)) \leq \max\{v(x), v(-y)\}$$

$$= \max\{v(x), v(y)\} \qquad \text{(por a))}$$

c) $v(x-y) = \max\{v(x), v(y)\}$.

Si

$$v(x) \neq v(y).$$

Supongamos

$$v(x) > v(y)$$

y además,

$$v(x-y) < \max\{v(x), v(y)\} = v(x) \ .$$

Utilizando la parte b), se obtiene:

$$v(x) = v(y + x-y)$$

$$\leq \max\{v(y), v(x-y)\} < v(x)$$

contradicción. Luego

$$v(x-y) = \max\{v(x), v(y)\} \ .$$

DEFINICION 2. Sea R un anillo filtrado con filtración v. Una familia de elementos de R. $(a_i)_{i\in I}$, es dependiente por la derecha relativa a la filtración v, o v-dependiente a la derecha; si existen elementos $b_i \in R$ casi todos nulos tales que:

$$v\left(\sum_i a_i\, b_i\right) < \max_i\{v(a_i) + v(b_i)\}$$

o algunos a_i son nulos.

Si esto no ocurre, se dice que la familia (a_i) es v-independiente a la derecha.

NOTA: Toda familia v-independiente a la derecha es linealmente independiente a la derecha.

El recíproco no es cierto en general.

DEFINICION 3. Sea R un anillo con filtración v, y $(a_i)_{i\in I}$, una familia de elementos de R. Diremos que un elemento $a \in R$ es v-dependiente a la derecha sobre la familia (a_i), si $a = 0$ o si existen $b_i \in R$ casi todos nulos, tales que,

$$v(a - \sum a_i b_i) < v(a),$$

donde

$$v(a_i) + v(b_i) \leq v(a)$$

para todo i.

En caso contrario, se dice que a, es v-independiente a la derecha de la familia (a_i).

NOTA:

1) Si a, es v-dependiente a la derecha sobre un conjunto B, entonces, a es v-dependiente sobre los miembros de grado menor o igual a v(a).

   En efecto, si $B = (a_i)_{i\in I}$, existen $b_i \in R$ casi todos nulos tales que,

$$v(a - \sum a_i b_i) < v(a) \qquad (*)$$

   y además

$$v(a_i) + v(b_i) \leq v(a) \qquad (**)$$

Luego, si $a_i \in B$ es tal que

$$v(a_i) > v(a),$$

por (**) $b_i = 0$.

Entonces en (*) aparecen justamente, aquellos términos a_i, de grado menor o igual a $v(a)$.

2) Si a es v-dependiente sobre un conjunto B, y cada elemento de B es v-dependiente sobre un conjunto C, entonces a es v-dependiente sobre C.

Para demostrar esto, sea $B = (a_i)_{i \in I}$ y cada a_i es v-dependiente de una familia $C = (x_{i_j})_{j \in J}$. Entonces, existen $b_i \in R$ que cumplen

$$v(a - \sum_i a_i b_i) < v(a)$$

con

$$v(a_i) + v(b_i) \leq v(a)$$

para todo i.

También para cada $i \in I$, existen $d_j \in R$ con la propiedad

$$v(a_i - \sum_j c_{i_j} d_{i_j}) < v(a_i)$$

con

$$v(c_{i_j}) + v(d_{i_j}) \leq v(a_i)$$

para todo j.

Luego, para cada $i \in I$ se tiene

$$v(a_i\, b_i - \sum c_{i_j}\, d_j\, b_i) \leq v(a_i - \sum c_{i_j}\, d_j) + v(b_i)$$

$$< v(a_i) + v(b_i) \leq v(a) \ .$$

Así,

$$v(a - \sum_{i,j} c_{i_j}\, d_j\, b_i) =$$

$$= v(a - \sum_i a_i\, b_i + \sum_i a_i\, b_i - \sum c_{i_j}\, d_j\, b_i) < v(a).$$

y además

$$v(c_{i_j}) + v(d_j\, b_i) \leq v(c_{i_j}) + v(v(d_j) + v(b_i)$$

$$\leq v(a_i) + v(b_i) \leq v(a) \ .$$

Por lo tanto, a es v-dependiente sobre $(c_{i_j})_{i,j}$.

DEFINICION 4: Sea R un anillo con filtración v. Diremos que R satisface el algoritmo débil de n términos, si dada cualquier familia v-dependiente $a_1, a_2, \ldots, a_m$ $(m \leq n)$ con

$$v(a_1) \leq \ldots \leq v(a_m)$$

algún a_i es v-dependiente sobre $a_1,\ldots,a_{i-1}$. Si R satisface el algoritmo débil de n términos para todo n, diremos que R satisface el algoritmo débil para v.

NOTA: En la definición anterior, se supone que estamos hablando de v-dependiente a la derecha. Sin embargo, como veremos más adelante, esta definición es simétrica en el sentido siguiente: Si R satisface el algoritmo débil de n terminos por la derecha entonces R satisface el algoritmo debil de n-términos por la izquierda y recíprocamente.

DEFINICION 5: Sea R un anillo con filtración v. Entonces el número de dependencia de R, relativo a la filtración v, que se simboliza por $\lambda_v(R)$, es el menos entero n, para el cual no hay algoritmo débil de n-términos y, $+\infty$ si R satisface el algoritmo débil de n-términos para todo n.

A continuación, estudiaremos el significado concreto de esta definición sobre un anillo conmutativo o más generalmente un anillo de ORE.

DEFINICION 6: Un anillo R se dice que es un anillo de ORE a la derecha si

$$aR \cap bR \neq 0 \qquad \forall\, a,b \in R-\{0\}$$

TEOREMA 7: Sea R un anillo de ORE a la derecha con filtración v. Entonces si:

i) $\lambda_v(R) = 1$ v no es una función de grado

ii) $\lambda_v(R) = 2$ v es una función de grado pero R no es Euclideano con respecto a v.

iii) $\lambda_v(R) = \infty$, v es una función de grado y R es Euclideano con respecto a v.

DEMOSTRACION:

i) Sea $\lambda_v(R) = 1$.

Si v es una función de grado, entonces se tiene

$$v(ab) = v(a) + v(b) \qquad \forall\ a,b \in R^* .$$

Entonces no existe $a \in R$ tal que a es v-dependiente y en virtud de esto, se cumple el algoritmo débil de 1 término (por vacuidad). Esto es una contradición, pues $\lambda_v(R) = 1$.

ii) Sea $\lambda_v(R) = 2$.

Si se supone que v no es una función de grado, se tiene

$$v(ab) < v(a) + v(b)$$

para algunos $a,b \in R - \{0\}$.

Luego a es v-dependiente, y R tiene algoritmo débil de 1-término y por lo tanto, existe $c \in R$ tal que,

$$v(a - ac) < v(a) \qquad (*)$$

y

$$v(a) + v(c) \leq v(a) .$$

Así, $c = 0$ (por la última desigualdad) lo cual contradice (*). En consecuencia se debe tener

$$v(ab) = v(a) + v(b) \qquad \forall a,b \in R - \{0\} .$$

Para demostrar que R no puede ser Euclideano, notemos primero, que cualquier par de elementos

$$a_1, a_2 \in R - \{0\}$$

son v-dependientes.

En efecto, ya que $a_1R \cap a_2R \neq 0$ existen $c_1, c_2 \in R$ tales que

$$a_1 c_1 = a_2 c_2$$

y entonces

$$v(a_1c_1 + a_2(-c_2)) = v(0) < \max_i \{v(a_i) + v(c_i)\}$$

Si v es un algoritmo de división, y suponemos

$$v(a_1) \leq v(a_2),$$

existen $q, r \in R$ tales que

$$v(a_1 - a_2q) < v(a_1)$$

y además

$$\begin{aligned} v(a_2) + v(q) &= v(a_2q) \\ &= v(a - r) \\ &\leq \max\{v(a), v(r)\} \\ &= v(a) \end{aligned}$$

donde

$$r = a_1 - a_2q .$$

Luego a_1 es v-dependiente de a_2 y $\{a_1, a_2\}$ es una familia v-dependiente.

Por lo tanto R tiene el algoritmo débil de 2-términos y así $\lambda_v(R) > 2$, lo cual es una contradicción.

iii) Sea $\lambda_v(R) = \infty$.

Sean $a_1, a_2 \in R$ con $v(a_1) \leq v(a_2)$. La familia $\{a_1, a_2\}$ es v-dependiente, pues R es anillo de ORE.

R satisface el algoritmo débil de 2 términos, por lo

tanto a_2 es v-dependiente de a_1 y $\exists\, q \in R$ tal que

$$v(a_2 - a_1 q) < v(a_2) .$$

Luego R es Euclideano con respecto a v.

TEOREMA 8: Sea R un anillo con algoritmo débil de 2-términos y

$$R_o = \{a \in R \mid v(a) \leq 0\} .$$

Entonces R_o es un cuerpo (o anillo de división si R no es conmutativo).

DEMOSTRACION: R_o es un subanillo de R, pues $a,b \in R_o$

$$v(a-b) \leq \max\{v(a), v(b)\} \leq 0 ,$$

$$v(ab) \leq v(a) + v(b) \leq 0 .$$

Además, sea $a \in R_o$. Entonces la familia $\{1,a\}$ es v-dependiente.

$$v(1.a - a.1) = v(0) < \max\{v(1)+ v(a)\}$$

y

$$v(a) \leq v(1).$$

R tiene algoritmo débil de 2-términos y esto implica 1 es v-dependiente de a.

Luego $\exists\, b \in R$ tal que,

$$v(1 - ab) < v(1) = 0$$

y

$$v(a) + v(b) \leq v(1) = 0 .$$

Esto implica

$$1 - ab = 0 \quad y \quad b \in R_o .$$

Así $ab = 1$, o sea, todo elemento en R_o posee un inverso.

DEFINICION 9: Sea R un anillo con filtración v, y un ideal de R. Diremos que un conjunto $B \subset \P$ es una v-base débil de $\P$ si:

i) Todo elemento de $\P$ es v-dependiente a la derecha de B.

ii) Ningún elemento $a \in B$ es v-dependiente de $B-\{a\}$.

PROPOSICION 10: Sea B una v-base débil de $\P$, entonces B genera a $\P$ como ideal derecho.

DEMOSTRACION: Sea $\P$ el ideal derecho generado por B. Sea $a \in \P - \P'$ tal que $v(a)$ es mínimo. Como a es v-dependiente de B, por definición, existen

$$b_1, \ldots, b_n \in B$$

y

$$c_1, \ldots, c_n \in R$$

tales que

$$v(a - \sum_{i=1}^{n} b_i c_i) < v(a) \ .$$

Luego,

$$c = \sum_{i=1}^{n} b_i c_i \in \P'$$

y

$$v(a - c) < v(a)$$

implica

$$a - c \in \P'$$

(pues v(a) es mínimo).

De esto se deduce que $a \in \P'$, lo cual es una contradicción.

TEOREMA 11: Sea R un anillo filtrado, tal que

$$K = \{a \in R \mid v(a) \leq 0\}$$

es un cuerpo.

Entonces, todo ideal derecho ¶ de R, posee una v-base débil.

DEMOSTRACION: Para cada $t \in \mathbb{N} \cup \{0\}$, sea

$$R_t = \{a \in R \mid v(a) \leq t\} \ .$$

Entonces $\mathfrak{P}_t = \mathfrak{P} \cap R_t$ es un K-espacio vectorial a la derecha $\forall\, t \in \mathbb{N} \cup \{0\}$. En efecto, si $a,b \in \mathfrak{P}_t$ y $x \in k$ se tiene

$$v(a-b) \leq t \ ,$$

y

$$v(ax) \leq t \ .$$

Consideremos los siguientes conjuntos definidos por recurrencia

$$\mathfrak{P}'_t = \{a \in \mathfrak{P}_t \mid a \text{ es v-dependiente de } \mathfrak{P}_{t-1}\} \ .$$

Afirmamos que para cada t, $\mathfrak{P}'_t$ es un subespacio de $\mathfrak{P}_t$.

Sean

$$a,b \in \mathfrak{P}'_t$$

i) Si $v(a - b) \leq t - 1$ entonces a-b es v-dependiente de $\mathfrak{P}_{t-1}$ y por lo tanto $a-b \in \mathfrak{P}_{t'}$.

ii) Si $v(a-b) = t$, entonces como $a \in \mathfrak{P}'_t$, a es v-dependiente de $\mathfrak{P}_{t-1}$. Luego, existen

$$a_1, a_2, \ldots, a_r \in \mathfrak{P}_{t-1}$$

y

$$c_1, c_2, \ldots, c_r \in R$$

tales que,

$$v(a - \sum a_i\, c_i) < v(a),$$

y

$$v(a_i) + v(c_i) \leq v(a).$$

Del mismo modo, $b \in \P'_t$, implica

$$v(b - \sum b_j\, d_j) < v(b)$$

con,

$$v(b_j) + v(d_j) \leq v(b)$$

donde,

$$b_j \in \P_{t-1} \quad y \quad d_j \in R$$

para todo j.

Utilizando ambos resultados, se obtiene

$$v((a-b) - (\sum a_i\, c_i - \sum b_j\, d_j))$$

$$\leq \max\{v(a - \sum a_i\, c_i),\ v(b - \sum b_j\, d_j)\}$$

$$< \max\{v(a),\ v(b)\} = t.$$

Además,

$$v(a_i) + v(c_i) \leq t = v(a-b)$$

$$v(b_j) + v(d_j) \leq t = v(a-b)\ .$$

Luego $a - b$ es v-dependiente de $\P_{t-1}$, y con esto se llega a que $a-b \in \P'_t$.

Entonces, una vez hecho esto, podemos escojer un conjunto minimal B_t ($\forall\, t \geq 0$) tal que genera $\P_t$ módulo $\P'_t$. Es decir representantes de la K-base de $\P_t / \P'_t$.

Tomemos ahora $B = \bigcup B_t$.

Afirmamos que B es una v-base débil de $\P$,

i) Todo $a \in \P$ es v-dependiente de B. La prueba es por inducción. Si $v(a) = 1$ entonces $a \in \P_1$.

Pero

$$\P_1 = \frac{\P_1}{\P'_1} \quad ,$$

pues

$$\P_o = \P \cap K = (0) \ ,$$

y

$$\P'_1 = \{a \in \P_1 \ / \ a \text{ es v-dependiente de } \P_o\} = (0) \ .$$

Luego B_1 es una base $\P_1$. Por lo tanto, a es una combinación lineal a la derecha de elementos de B_1 y así v-dependiente de B_1.

Supongamos que todo elemento de $\P_{t-1}$ es v-dependiente de B.

Sea,

$$v(a) = t.$$

Entonces,

$$a + \P'_t \varepsilon \frac{\P_t}{\P'_t} \quad ,$$

y luego,

$$a + \P'_t = \sum b_i \, k_i + \P'_t \, , \quad b_i \varepsilon B_t$$

o sea

$$a - \sum b_i \, k_i \varepsilon \P'_t \quad .$$

Luego $a - \sum b_i \, k_i$ es v-dependiente de $\P_{t-1}$. Pero por hipótesis de inducción, $\P_{t-1}$ es v-dependiente de B, y por la nota a la definición 3, se concluye que a es v-dependiente de B.

ii) Ningún $b \varepsilon B$ es v-dependiente de $B - \{b\}$.

Supongamos que $v(b) = t$ y además, b es v-dependiente de $B - \{b\}$.

Entonces,

$$\Big] \, b_i \varepsilon B, \quad c_i \varepsilon R$$

tales que

$$v(b - \sum b_i \, c_i) < v(b) = t$$

y

$$v(b_i) + v(c_i) \leq v(b) = t \ .$$

Luego

$$b - \sum b_i \, c_i \in \P'_t$$

y por lo tanto

$$b \equiv \sum b_i \, c_i \bmod \P'_t \qquad (*)$$

a) Si para algún i, $v(b_i) < t$, entonces $b_i \, c_i$ es v-dependiente de $\P_{t-1}$.

En efecto, se presentan dos posibilidades.

Si

$$v(b_i \, c_i) = t \ ,$$

se tiene

$$t = v(b_i \, c_i) \leq v(c_i) + v(b_i) \leq t$$

y por lo tanto

$$v(b_i \, c_i) = v(c_i) + v(b_i)$$

luego, se deduce fácilmente, que $b_i \, c_i$ es v-dependiente de b_i, y por ende de $\P_{t-1}$.

Si

$$v(b_i \, c_i) < t,$$

entonces

$$b_i\ c_i \in \P_{t-1}\ ,$$

y esto implica que $b_i\ c_i$ es v-dependiente de $\P_{t-1}$.

b) Si $v(b_i) = t$ para algún i, se deduce que $v(c_i) = 0$, y $c_i \in k$.

Eliminando términos superfluos en (*) se obtiene

$$b \equiv \sum b_i\ c_i \mod \P'_t \quad \text{con} \quad c_i \in k\ .$$

Pero $b, b_1, \ldots, b_n$ son linealmente independientes módulo $\P'_t$, y esto es una contradicción. Luego ii) queda demostrado.

El teorema que acabamos de demostrar, también es cierto en sentido contrario como veremos a continuación.

<u>TEOREMA 12</u>: Sea R un anillo filtrado, $\P$ un ideal de R y sea B una v-base débil de $\P$. Entonces los elementos de grado t de B, forman la k-base de $\P_t \pmod{\P'_t}$.

<u>DEMOSTRACION</u>: Por inducción.

Sea

$$B_i = \{b \in B \ /\ v(b) = i\} \qquad i = 0,1,\ldots$$

Entonces B_1 es una k-base de $\dfrac{\P_1}{\P'_1} = \P_1$.

En efecto, B_1 es un conjunto v-independiente y por lo tanto linealmente independiente. (Véase la nota a la definición 2).

Además, si $x \in \P_1$, entonces x es v-dependiente de B_1.

Luego

$$\exists\, b_i \in B_1 , \quad c_i \in R \qquad (i=1,2,\ldots,n)$$

tales que

$$v(x - \sum b_i c_i) < v(x) = 1 \qquad (*)$$

con

$$v(b_i) + v(c_i) \leq v(x) = 1 .$$

Debemos tener entonces,

$$v(b_i) = 1 \quad y \quad v(c_i) = 0.$$

Luego

$$c_i \in k \qquad \forall\, i=1,2,\ldots,n$$

De la desigualdad (*) se originan dos posibilidades:

i) $v(x - \sum b_i c_i) = 0.$

Con lo cual $x - \sum b_i c_i$ es una unidad, y por lo tanto $\P = R$.

ii) $v(x - \sum b_i c_i) = -\infty$

y entonces

$$x - \sum b_i c_i = 0$$

y

$$x = \sum b_i\, c_i \quad \text{con} \quad b_i \in B \quad \text{y} \quad c_i \in k$$

Con esto termina el primer paso de la inducción.

Supongamos ahora, que el resultado es válido para t-1. Sea

$$x \in \P_t \quad , \quad \text{con} \quad v(x) = t.$$

Entonces x es v-dependiente de B y así, existen $b_j \in B$, $c_j \in R$ $j = 1,\ldots,n$ tales que

$$v(x - \sum b_j\, c_j) < v(x) = t$$

con

$$v(b_j) + v(c_j) \leq v(x) = t \ .$$

Razonando como en la prueba del teorema anterior, llegamos a $x \equiv \sum b_j\, c_j (\text{mod } \P'_t)$ con $v(b_j) = t$, $c_j \in k$. Luego x es combinación lineal de elementos de B_t módulo $\P'_t$. Con esto termina la prueba.

NOTA: Si R es un anillo que satisface las hipótesis del TEOREMA 11, entonces dos v-bases débiles de un ideal derecho ¶, deben tener las mismas cardinalidades. Más precisamente, si B y B' son dos v-bases débiles para ¶, entonces

$$B = \bigcup B_t \quad , \quad B' = \bigcup B'_t$$

$$\text{card}(B_t) = \text{card}(B'_t) = \dim_k \P_t / \P'_t$$

y $\text{card}(B) = \text{card}(B')$.

A partir de estas ideas, tenemos la siguiente.

DEFINICION 13: Sea R un anillo filtrado. Sea $\P$ un ideal derecho con v-base débil B. Entonces el NUMERO DE V-GENERADORES DE $\P$ DE GRADO t, denotado por $\gamma_t(\P)$ es igual al cardinal de B_t, donde

$$B_t = \{a \in B \mid v(a) = t\} .$$

Además, se define el NUMERO DE V-GENERADORES DE $\P$, como

$$\gamma(\P) = \sum \gamma_t(\P) .$$

PROPOSICION 14: Sea R un anillo con algoritmo débil. Sea $\P$ un ideal de R, con base débil B. Entonces si $\{a_i\} \subset \P$ es una familia linealmente independiente ningún a_i es v-dependiente del resto.

DEMOSTRACION: Razonando por el absurdo, supongamos que a_n es v-dependiente de $a_1,\ldots,a_{n-1}$.

O sea existen $c_i \in R$ tales que

$$v(a_n - \sum_{i=1}^{n} a_i\, c_i) < v(a_n) .$$

Además

$$a_n - \sum_{i=1}^{n} a_i\, c_i \neq 0$$

pués $\{a_1,\ldots,a_n\}$ es un conjunto linealmente independiente.

Para cada a_i, existen $b_j \in B$ tales que

$$a_i = \sum_{j=1}^{m} b_j\, d_{i_j} \qquad \text{con} \qquad d_{ij} \in R\ .$$

Esto, en virtud de la PROPOSICION 10. Luego, podemos escribir

$$v\Big(\sum_j b_j\, d_{nj} - \sum_i \sum_j b_j\, d_{ij}\, c_i\Big) < v\Big(\sum_j b_j\, d_{nj}\Big)$$

$$\leq \max_j \{b_j + d_{nj}\}\ .$$

Entonces la familia $\{b_j\}$ es v-dependiente y por tener R el algoritmo débil, algún b_i es v-dependiente de $b_1,\ldots,b_{i-1}$. Hemos llegado asi a una contradicción, ya que B es una v-base débil.

Luego, se verifica la tesis de la PROPOSICION.

COROLARIO 15: Sea R un anillo con algoritmo débil, y ¶ un ideal de R. Entonces, toda base B de ¶ es una v-base débil.

DEMOSTRACION: Probaremos que B satisface las dos condiciones

de la DEFINICION 9.

i) Sea $a \in \P$, $a \neq 0$.

Entonces existen $b_i \in B$ tales que,

$$a = \sum_{i=1}^{n} b_i \, c_i \quad , \quad \text{con} \quad c_i \in R \ .$$

Luego

$$v(a - \sum_{i=1}^{n} b_i \, c_i) < v(a) \ .$$

Además los $\{b_i\}$ son linealmente independientes, y por lo tanto v-independientes (por el TEOREMA 14) . Así

$$v(a) = v(\sum b_i \, c_i) = \max_i \{v(b_i) + v(c_i)\} \ .$$

Entonces a es v-dependiente de B.

ii) Ningún $b_i \in B$ es v-dependiente de $B - \{b_i\}$, en vista del TEOREMA 14.

ANILLO DE IDEALES LIBRES

DEFINICION 16: Un anillo R se dice ANILLO DE IDEALES LIBRES, si todo ideal a la derecha es libre, como R módulo, y de rango único.

NOTA: Un ideal libre es de rango único, si dos bases cualesquiera tienen la misma cardinalidad.

Si F es un módulo libre sobre un anillo conmutativo R, con unidad, entonces esta condición se satisface. (Ver [2]).

En caso de no ser el anillo conmutativo, el teorema no es cierto. Un ejemplo se encuentra en [1], pag. 6.

TEOREMA 17: Sea R un anillo con algoritmo débil. Entonces R es un anillo de ideales libres.

DEMOSTRACION: Sea $\P$ un ideal de R.

Hemos demostrado en el TEOREMA 11, la existencia de una v-base débil B, para $\P$.

Afirmamos que B es una base de $\P$.

i) B genera a $\P$ como R-módulo.

Consecuencia de la PROPOSICION 10.

ii) B es un conjunto linealmente independiente.

Supongamos que se tiene

$$\sum_{i=1}^{n} b_i c_i = 0 \quad , \quad b_i \in B \qquad 1 \leq j \leq n$$

con

$$v(b_1) \leq v(b_2) \leq \ldots \leq v(b_n) \ .$$

Entonces la familia $\{b_1,\ldots,b_n\}$ es v-dependiente y esto obliga a que algún b_i es v-dependiente de $b_1,\ldots,b_{i-1}$ (por el algoritmo débil). Esto contradice el hecho de ser B una v-base débil.

Finalmente, $\P$ tiene rango único, pues dadas dos bases cualesquiera X e Y, ellas son v-bases débiles, (por COROLARIO 15), y entonces se tiene

$$\text{card}(X) = \text{card}(Y).$$

(Véase la nota al TEOREMA 12).

ANILLOS GRADUADOS ASOCIADOS

DEFINICION 18: Un ANILLO GRADUADO H, es una familia $\{H_i\}_{i=0,1,..}$ de grupos abelianos disjuntos, tales que

i) Existe una multiplicación σ

$$\sigma: H_i \times H_j \to H_{i+j}$$

la cual es asociativa.

ii) H_o tiene estructura de anillo, y cada H_i es un H_o-módulo.

iii) $H = \sum H_i$.

NOTA: De esta definición se concluye que para cada $a \in H$, existe un único entero no negativo $d(a)$ tal que

$$a \in H_{d(a)}$$

$d(a)$ será llamado el grado de a.

DEFINICION 19: Sea H un anillo graduado. Una relación

$$\sum a_i b_i = 0 \qquad (*)$$

donde $d(a_i) + d(b_i)$ es igual para todo i, se dice TRIVIAL, si

$$a_i = 0 \quad o \quad b_i = 0$$

para todo i.

DEFINICION 20: Una familia de elementos $\{a_i\}$ en H, se dice linealmente dependiente si satisfacen una relación del tipo (*), y los b_i no todos son nulos.

TEOREMA 21: Sea R un anillo con filtración v. Para cada $i \geq 0$ definimos

$$R_i = \{a \in R \mid v(a) \leq i\}$$

Entonces cada R_i es un subgrupo del grupo abeliano R. Además, se cumple:

a) $0 = R_{-\infty} \subseteq R_0 \subseteq R_1 \subseteq \ldots,$

b) $UR_i = R$

c) $R_i R_j \subseteq R_{i+j}$.

DEMOSTRACION: Consecuencia directa de las propiedades de v.

DEFINICION 22: Sea R un anillo con filtración v. Entonces

$$gr(R) = \bigoplus_{i=1}^{\infty} \frac{R_i}{R_{i-1}}$$

se llama ANILLO GRADUADO ASOCIADO A R.

NOTA: gr(R) es, en efecto, un anillo graduado. La multiplicación viene dada por

$$R_i/R_{i-1} \times R_j/R_{j-1} \longrightarrow R_{i+j}/R_{i+j-1}$$

$$(\overline{\alpha}, \overline{\beta}) \longrightarrow \overline{\alpha\,\beta}$$

Aquí, α es un elemento de R_i, y β es un elemento de R_j. Luego

$$v(\alpha\,\beta) \leq v(\alpha) + v(\beta) \leq i + j ,$$

o sea,

$$\overline{\alpha\ \beta} \in R_{i+j}/_{R_{i+j-1}} .$$

Además, esta operación esta bien definida, y no depende del representante de la clase. Es decir, si se supone

$$\overline{\alpha} = \overline{a} \quad y \quad \overline{\beta} = \overline{b}$$

se tiene que

$$a - \alpha = \gamma_1 \qquad \text{con} \quad \gamma_1 \in R_{i-1}$$

$$b - \beta = \gamma_2 \qquad \text{con} \quad \gamma_2 \in R_{j-1}$$

luego

$$v(ab - \alpha\beta) = v(\gamma_1 b + \alpha\gamma_2)$$

$$\leq \max\{v(\gamma_1 b),\ v(\alpha\gamma_2)\}$$

$$\leq i + j - 1 .$$

Luego

$$ab \equiv \alpha\beta \bmod R_{i+j-1}$$

y así

$$\overline{ab} = \overline{\alpha\beta} \quad \text{en} \quad R_{i+j}/_{R_{i+j-1}} .$$

En lo que sigue, dado $a \in R^*$, la imagen de a en

$R_{v(a)}/R_{v(a)-1}$, será denotada por $\bar{a}$, y se llama <u>coeficiente principal de a</u> .

En los siguientes teoremas, veremos como se reflejan en gr(R) los conceptos de v-dependencia, y el algoritmo débil de n-términos. Se supone que R es un anillo con filtración v.

<u>TEOREMA 13</u>. Una familia de elementos $\{a_i\}$, $a_i \in R$ es v-dependiente a la derecha si y sólo si algún a_i es 0 o $\{\bar{a}_i\}$ es linealmente dependiente en gr(R).

<u>DEMOSTRACION</u>: Si $\{a_i\}$ v-dependiente a la derecha, existen $b_i \in R$ tales que

$$v(\sum a_i\, b_i) < \max\{v(a_i) + v(b_i)\} = t.$$

Esto sucede si y sólo si

$$\sum \bar{a}_i\, \bar{b}_i \in R_t/R_{t-1}$$

y además

$$\sum \bar{a}_i\, \bar{b}_i = \bar{0} \quad \text{en} \quad R_t/R_{t-1}$$

<u>TEOREMA 24</u>: Un elemento $a \in R$ es v-dependiente de una familia $\{a_i\}$ en R, si y sólo si $\bar{a}$ es una combinación lineal de $\{\bar{a}_i\}$.

DEMOSTRACION: Si a es v-dependiente a la derecha de $\{a_i\}$, entonces, existen $b_i \in R$ tales que

$$v(a - \sum a_i\, b_i) < v(a) = t$$

con

$$v(a_i) + v(b_i) \leq v(a)$$

para todo i.

Esto sucede si y sólo si

$$\bar{a} - \sum \bar{a}_i\, \bar{b}_i \in R_t/R_{t-1}$$

y además

$$\bar{a} - \sum \bar{a}_i\, \bar{b}_i = \bar{0} \quad \text{en} \quad R_t/R_{t-1}$$

COROLARIO 25: R satisface el algoritmo débil de n-términos si y sólo si gr(R) satisface lo siguiente.

Dado cualquier sucesión linealmente dependiente a la derecha $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_m$ $(m \leq n)$ con

$$d(\bar{a}_1) \leq \ldots \leq d(\bar{a}_m) .$$

Entonces, algún $\bar{a}_i$ es combinación lineal de $\bar{a}_1, \bar{a}_2, .., \bar{a}_{i-1}$.

DEMOSTRACION: Sale directamente de los dos teoremas

anteriores.

Con el objeto de expresar el corolario 24 en términos de matrices, damos la siguiente definición.

DEFINICION 26: Sea H un anillo graduado

$$H = H_o \oplus H_1 \oplus \ldots \oplus H_n \oplus \ldots$$

Sea la sucesión de enteros no negativos

$$D = (d_1, d_2, \ldots, d_n) \quad \text{con} \quad d_1 \leq d_2 \leq \ldots \leq d_n$$

Entonces se llama GRUPO DE MATRICES TRIANGULARES SUPERIORES RELATIVAS A D, y se denota por $T_{rD}(H)$ al conjunto de matrices $n \times n$, de la forma (x_{ij}) tales que

$$x_{ij} \in H_{dj} - H_{di} \qquad \text{si} \quad i < j$$

$$x_{ij} = 1 \qquad \text{si} \quad i = j$$

$$x_{ij} = 0 \qquad \text{si} \quad i > j$$

NOTA: Los elementos de $T_{rD}(H)$ forman un grupo multiplicativo y operan a la derecha sobre los elementos de

$$H_{d_1} \oplus H_{d_2} \oplus \ldots \oplus H_{d_n} = H_D \ .$$

En efecto, sea

$$a = (a_{d_1},\ldots,a_{d_n}) \in H_D$$

y

$$(x_{ij}) \in T_{rD}(H) \ .$$

Luego

$$(a_{d_1},\ldots,a_{d_i},\ldots,a_{d_n}) \begin{pmatrix} 1 & x_{12}\cdots x_{1j}\cdots x_{1n} \\ & 1 & & \\ & & \ddots & \\ & & & 1 \\ 0 & & & \ddots x_{jn} \\ & & & & \ddots \\ & & & & & 1 \end{pmatrix}$$

$$= (a_{d_1},\ldots, \sum_{j\leq i} a_{dj}\, x_{ji}\, ,\ldots, \sum_{j=1}^{n} ad_j\, x_j n) = (c_1,\ldots,c_i,\ldots,c_n)$$

Como

$$x_{ji} \in H_{di} \cdot d_j \quad y \quad a_{dj} \in H_{dj}$$

entonces

$$c_i = \sum_{j\leq 1} a_{dj}\, x_{ji} \in H_{di} \qquad \forall \ 1 \leq i \leq n \ .$$

Luego si

$$\mu \in Tr_D(H)$$

se tiene

$$\mu a \in H_D \qquad \forall\, a \in H_D \ .$$

Para mostrar que $Tr_D(H)$ es un grupo multiplicativo, basta con demostrar

$$\mu\ \eta\ \varepsilon\ Tr_D(H) \qquad \forall\ \mu,\eta\ \varepsilon\ Tr_D(H)\ .$$

Podemos hacer

$$\mu = (x_{ij}),\quad \eta = (y_{kl})\ .$$

Entonces

$$\mu\ \eta = (z_{ik})$$

donde

$$z_{ik} = \sum_{j=1}^{n} x_{ij}\ y_{jk}\ .$$

I) Si $\underline{i < k}$. Se presentan dos casos

$$i \leq j \qquad \text{implica} \qquad x_{ij} = 0$$
$$i \geq j \qquad \text{implica} \qquad j < k$$

y de aquí se sigue $y_{jk} = 0$.

Así,

$$\underline{z_{ik} = 0}$$

II) Si $\underline{i = k}$. Hay tres casos

$$j = k \qquad \text{implica} \qquad x_{ij}\ y_{jk} = 1$$

$$j > k \quad \text{implica} \quad x_{ij} = 0$$

$$j < k \quad \text{implica} \quad y_{jk} = 0 \ .$$

Luego

$$z_{ik} = 1 \quad \text{si} \quad i = k.$$

III) Si $i > k$, solamente aparecen términos si $i < j < k$.

En este caso

$$z_{ik} = x_{ij}\, y_{jk} \in H_{d_k} - H_{d_i} \ .$$

Con esto, hemos demostrado $(z_{ik}) \in Tr_D(H)$.

DEFINICION 27: Sea

$$D' = (d'_1, d'_2, \ldots, d'_n)$$

con

$$D'_1 \geq d'_2 \geq \ldots \geq d'_n \geq 0$$

se define el GRUPO DE MATRICES TRIANGULARES INFERIORES RELATIVAS A D, y se denota por $Tr_D(H)$, al conjunto de matrices $n \times n$ de la forma (x_{ij}), con

$$x_{ij} = 0 \quad \text{si} \quad i > j$$

$$x_{ij} = 1 \quad \text{si} \quad i = j$$

$$x_{ij} \in H'_{dj} - H'_{dj} \quad \text{si} \quad i < j \ .$$

Estas matrices, operan a la izquierda, sobre el anillo graduado

$$H'_D = H_{d'_n} \theta \ldots . \theta H_{d'_1} \quad ,$$

y forman un grupo multiplicativo.

Si

$$d = d_1 + d'_1 = d_2 + d'_2 = \ldots = d_n + d'_n$$

y además

$$d_1 \leq d_2 \leq \ldots \leq d_n$$

$$d'_1 \geq d'_2 \geq \ldots \geq d'_n$$

Entonces

$$Tr_D(H) = Tr^{o}_{D'}(H)$$

(donde A^{o} = transpuesta de A).

DEFINICION 28: Una relación en H

$$\sum a_i \, b_i = 0 \qquad (*)$$

se dice bien ordenada, si

$$g_r(a_i) = g_r(b_i) = d \qquad \forall i,$$

y además

$$g_r(a_i) \leq g_r(a_2) \leq \ldots \leq g_r(a_n).$$

Podemos escribir la relación (*) en términos de matrices

$$(a_1, a_2, \ldots, a_n) \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = 0$$

o también

$$a.b = 0$$

NOTA: Si $a.b = 0$ es una relación bien ordenada en H, y $\mu \in Tr_D(H)$, se cumple

$$(a.\mu).b = a.(\mu.b) \ .$$

DEFINICION 29: Una relación bien ordenada

$$\sum a_i \, b_i = 0$$

se dice Tr-trivializable, si existe $\mu \in Tr_D(H)$ con

$$D = (g_r(a_1), \ldots, g_r(a_n))$$

tal que

$$a\mu . \mu^{-1} b = 0$$

es una relación trivial.

TEOREMA 30: Sea H un anillo graduado, y $n \geq 1$.

Entonces las siguientes condiciones son equivalentes:

a) Dada cualquier sucesión linealmente dependiente a la derecha $a_1,\ldots,a_m \in H$ $(m \leq n)$ con

$$d(a_1) \leq d(a_2) \leq \ldots \leq d(a_m),$$

algún a_i es linealmente dependiente de $a_1,\ldots,a_{i-1}$.

b) Dados $a_1,a_2,\ldots,a_m \in H$ $(m \leq n)$ con

$$d(a_1) \leq d(a_2) \leq \ldots \leq d(a_m)$$

$\mu \in Tr_D(H)$ tal que los términos no cero de

$$(a_1, a_2,\ldots,a_m)\mu$$

son linealmente independientes a la derecha.

c) Toda relación

$$\sum a_i b_i = 0$$

con

$$d(a_1) \leq d(a_2) \leq \ldots \leq d(a_m) \qquad m \leq n$$

es Tr-trivializable.

DEMOSTRACION: (a => b). Sean

$$a_1,\ldots,a_m \qquad (m \leq n)$$

y

$$d(a_1) \leq d(a_2) \leq \ldots \leq d(a_m) \ .$$

Si $a_1,a_2,\ldots,a_n$ es v-dependiente, entonces por (a), algún a_i es v-dependiente de $a_1,a_2,\ldots,a_{i-1}$. Luego

$$a_i = \sum_{j=1}^{i-1} a_j b_j$$

y en vista de ello, existe

$$\mu_1 \in Tr_D(H)$$

tal que

$$(a_1,\ldots,a_{i-1}, a_i, a_{i+1},\ldots,a_n)\mu_1 =$$

$$=(a_1,\ldots,a_{i-1}, 0,a_{i+1},\ldots,a_n) \ .$$

Procediendo de esta manera, después de un número finito de pasos, se tendrá una matriz $\mu \in Tr_D(H)$ tal que los términos no cero de

$$(a_1, a_2,\ldots,a_m)\mu$$

son linealmente independientes a la derecha

(a → c). Sea la relación

$$a.b = \sum a_i\, b_i = 0$$

con

$$d(a_1) \leq d(a_2) \leq \quad \leq d(a_m) \qquad (m \leq n) \ .$$

Por la parte b) existe $\mu \in Tr_D(H)$ tal que los elementos no nulos de

$$(a_1,\ldots,a_n)\mu$$

son linealmente independientes.

Puesto que μ es una matriz invertible, $a.b = 0$ implica

$$a\mu \,.\, \mu^{-1}b = 0 \ .$$

Si hacemos

$$(a_1,\ldots,a_m)\mu = (a_1',\ldots,a_m')$$

$$\mu^{-1}(b_1,\ldots,b_m) = (b_1',\ldots,b_m')^t \ .$$

Entonces se tiene la relación

$$a\mu \,.\, \mu^{-1}b = (a_1',\ldots,a_m') \begin{pmatrix} b_1' \\ \vdots \\ b_m' \end{pmatrix} = 0$$

Pero los términos no nulos de $(a'_1,\ldots,a'_m)$ son linealmente independientes, luego

$$a'_i = 0 \quad o \quad b'_i = 0 \qquad 1 \leq i \leq m$$

(c => a). Sean

$$a_1, a_2,\ldots,a_n \in H$$

linealmente dependientes con $d(a_1) \leq \ldots \leq (a_n)$.

Luego existen $b_1,\ldots,b_n$ en H (no todos nulos) tales que

$$\sum a_i b_i = 0$$

es decir

$$a.b = 0 .$$

Por c) existe $\mu \in Tr_D(H)$, tal que

$$a\mu \,.\, \mu^{-1}b = 0$$

es una relación trivial.

Luego

$$a\mu \,.\, \mu^{-1}b = (a'_1,\ldots,a'_n) \begin{pmatrix} b'_1 \\ \vdots \\ b'_n \end{pmatrix} = 0$$

Como algún b_i es diferente de cero, se tiene que

$$\mu^{-1} b \neq 0$$

lo cual implica $b'_j \neq 0$ para algún j .

Pero

$$\sum a'_i \, b'_i = 0$$

es una relación trivial.

Entonces debe ser $a'_j = 0$.

Luego

$$a'_j = a_j + \sum_{k=1}^{j-1} a_k \, b_k = 0$$

de donde se concluye que a_j es linealmente dependiente a la derecha de $a_1, \ldots, a_{j-1}$.

NOTA: La condición c) es equivalente a la siguiente:

c') Si se tiene una relación en H

$$\sum a_i \, b_i = 0$$

con

$$d(b_1) \geq d(b_2) \geq \ldots \geq d(b_n) \qquad (m \leq n)$$

entonces es Tr-trivializable.

Luego, el TEOREMA 30 es simétrico, pues todo lo que se

afirma para el lado derecho, también es cierto para el lado izquierdo.

Además, el anillo graduado gR = H, satisface las condiciones a) b) y c) si y sólo si R tiene el algoritmo débil (COROLARIO 25). Por lo tanto hemos demostrado.

COROLARIO 31: El algoritmo débil de n-términos a la derecha, para anillos filtrados, implica el algoritmo débil de n-términos a la izquierda y recíprocamente.

CARACTERIZACION DE ANILLOS CON ALGORITMO DEBIL

En esta sección, R será un anillo con filtración v.

DEFINICION 32: Si se tiene una expresión

$$\sum_i a_{i1}\cdots a_{in_i} \quad \text{con} \quad a_{ik} \in R, \quad 1 \leq k \leq n$$

entonces el grado formal de esta expresión viene dado por

$$\max_i \{v(a_{i_1}) + \ldots + v(a_{in_i})\}$$

NOTA: De esta definición se sigue que el grado de un elemento de R, siempre es menor que el grado formal de cualquier de sus representaciones. En los resultados que siguen, asumiremos que $K \subset R$ es un campo donde

$$K = R_o = \{a \in R \mid v(a) \leq 0\}$$

DEFINICION 33: Un conjunto $X \subset R$ se llama BASE DEBIL DE LA K-ALGEBRA R si

i) R es generado por todos los monomios de X como K-espacio.

ii) Ningún elemento $x \in X$ es v-dependiente de $X-\{x\}$.

TEOREMA 34: R tiene una base débil X.

DEMOSTRACION: Para $t \geq 0$ sea

$$R_t = \{a \in R \mid v(a) \leq t\}$$

R_t es un k-espacio vectorial.

Entonces se define R'_t, como el k-subespacio de R_t generado por todos los productos de la forma:

$$a.b \quad \text{donde} \quad a,b \in R_{t-1}$$

y

$$v(a) + v(b) \leq t.$$

Sea X_t una k-base de R_t (mod R'_t) y consideremos

$$X = \bigcup X_t \ .$$

Afirmamos que X satisface las condiciones i) y ii) de la DEFINICION.

ii) Sea $x \in X$, x v-dependiente de $X-\{x\}$. Supongamos

$$v(x) = t.$$

Existen elementos x_i en $X-\{x\}$ y $b_i \in R$ tales que

$$v(x - \sum x_i\, b_i) < v(x) = t,$$

y

$$v(x_i) + v(b_i) \leq v(x) = t.$$

Se presentan dos casos:

A) Si $v(x_i) = t$, entonces $v(b_i) = 0$ y esto implica $b_i \in k$.

B) Si $v(x_i) \leq t-1$ entonces $x_i\, b_i \in R'_t$. Luego

$$x - \sum x_i\, b_i \in R'_t$$

o bien, podemos asumir

$$x \equiv \sum x_i\, b_i \bmod R'_t$$

con $v(x_i) = t$ para todo i.

Por lo tanto, en el caso A como en el B, hemos llegado a

expresar x como una combinación lineal de elementos de la k-base de $R_t \pmod{R'_t}$.

Esto es una contradicción, pues $[x, x_i]$ son linealmente independientes mod R'_t .

i) Demostraremos que X genera R sobre K. Más precisamente, los monomios de X de grado $\leq t$ generan R_t . La prueba es por inducción sobre el grado de los elementos de R.

Para n=1, X_1 genera R_1 como k-espacio y por lo tanto, R_1 está generado por monomios de grado 1.

Supongamos que R_{t-1} es generado por monomios en X de grado $\leq t-1$.

Sea $x \in R$, con $v(x) = t$.

Luego

$$x + R'_t \in R_t/R'_t \quad .$$

Pero X_t es una base de R_t/R'_t y así

$$x + R'_t = \sum x_i \, a_i$$

con

$$x_i \in x_t \ , \ a_i \in k.$$

Notemos que R'_t esta formado por elementos del tipo

$$a.b \ , \quad \text{con} \quad a,b \in R_{t-1} \ ,$$

y

$$v(a) + v(b) \leq t \ .$$

De esta definición y de la hipótesis de inducción, se sigue que R'_t está generado por monomios de X de grado $\leq t$. Luego x es una combinación k-lineal de monomios de X de grado $\leq t$. Con esto termina la demostración.

Los monomios en X, serán denotados por

$$x_I = x_1 \, x_2 \ldots x_n \ .$$

En virtud del teorema precedente, todo elemento $a \in R$, se puede escribir

$$a = \sum x_I \, \alpha_I \quad , \qquad \alpha_I \in K$$

Además, si $v(a) = t$, entonces $v(x_I) \leq t$ para cada I.

Y así, el grado formal de a es igual a t.

A continuación, construiremos una función AUXILIAR en el Anillo R, la cual será de gran utilidad para probar que R satisface el algoritmo débil.

Fijamos un monomio de grado r, $x_1 \ldots x_k$, y definimos una aplicación k-lineal

$$R \longrightarrow R$$

$$a \longrightarrow a^*$$

dada por la fórmula

$$x_1 \ldots x_k . b \longrightarrow b$$

$$\text{otro monomio} \longrightarrow 0 .$$

Esta aplicación está bien definida, pues X es una k-base de R, y todos los elementos de X son monomios.

Afirmamos que

$$v(a^*) \leq v(a) - r \qquad \forall\ a \in R .$$

En efecto, sea

$$a = \sum x_{i_1} x_{i_2} \ldots x_{in_j} \alpha_{i_1} \ldots \alpha_{in_j}$$

y

$$v(a) = t .$$

Luego $a \in R_t$, y por la escogencia de la base X, (véase el TEOREMA 34) se tiene

$$v(x_{i_1} \ldots x_{in_j}) \leq t$$

para cada j.

Por lo tanto a^* es una combinación lineal de monomios de grado $t-r$, y de esto se sigue

$$v(a^*) \leq t-r = v(a) - r.$$

TEOREMA 35: Para todo $a,b \in R$ se tiene

$$(ab)^* \equiv a^*b \pmod{R_{v(b)-1}} .$$

DEMOSTRACION:

CASO 1) Si $v(a) < r$, entonces $a^* = 0$ y además

$$\begin{aligned} v((ab)^*) &\leq v(ab) - r \\ &\leq v(a) + v(b) - r \\ &\leq v(b) - 1 \end{aligned}$$

y entonces

$$(ab)^* \in R_{v(b)-1}$$

CASO 2) $v(a) \geq r$ y a es un monomio de la base X.

Entonces

$$a = x_1 . x_2 \ldots x_k \; a^*$$
$$ab = x_1 . x_2 \ldots x_k \; a^*b$$

y por lo tanto

$$(ab)^* = a^*b \ .$$

CASO GENERAL. Se sigue por linealidad.

A continuación, daremos una condición necesaria y suficiente, para que se tenga el algoritmo débil en un anillo filtrado.

TEOREMA 36: R satisface un algoritmo débil, si y sólo si $R_o = k$ es un cuerpo, y R tiene una base débil X como algebra, de elementos de grado mayor o igual a uno.

Cuando esto es cierto, entonces los monomios de cualquier base débil X forman una k-base para R y el grado de una expresión

$$\sum x_I \alpha_I$$

es su grado formal.

DEMOSTRACION: R tiene algoritmo débil, entonces $R_o = k$ es un cuerpo y ya se ha visto como se construye una base débil X para R. (TEOREMA 34).

Recíprocamente, sea X una base débil de la k-algebra R. Afirmamos que los monomios en X son linealmente independientes.

Supongamos que se tiene una relación

$$(*) \qquad \sum_I x_I \alpha_I = 0 \ ,$$

donde

$$x_I = x_1 \ldots x_n \quad ; \quad x_i \in X$$

y

$$\alpha_I \in R \ .$$

Probaremos que la relación dada es una relación trivial, usando inducción sobre el grado formal.

n=1. Si el grado formal de la relación (*) es 1, entonces tenemos por definición

$$\max_I \{v(x_I) + v(\alpha_I)\} = 1$$

y por lo tanto $v(x_I) = 1$ para todo I, lo cual implica

$$x_I \in X \qquad \forall I \ .$$

Luego la relación (*) nos queda

$$\sum x_j \alpha_j = 0 \qquad (**)$$

con

$$x_j \in X$$

y como los elementos de la base débil X son independientes, la relación (**) es trivial.

Supongamos que el resultadc es cierto para toda expresión (*) con grado formal < n .

Sea

$$\sum x_I \alpha_I = 0$$

una relación del tipo (*) con grado formal igual a n.

Podemos factorizar algunos términos arriba, para obtener.

$$\sum x\, a_x + \alpha = 0$$

con

$$x \in X , \quad a_x \in R, \quad \alpha \in K$$

o sea

$$v(\sum x\, a_x) = v(-\alpha) = 0 .$$

Así, tenemos una relación de v-dependencia en X, luego cada $a_x = 0$ y $\alpha = 0$.

Pero para cada x, la relación

$$a_x = 0,$$

tiene grado formal < n , y por hipótesis de inducción es una relación trivial.

De aquí se concluye que cada $\alpha_I = 0$, y la afirmación queda probada.

A continuación demostraremos que R tiene algoritmo débil.

Sea $b_1, b_2, \ldots, b_n$ una familia de elementos de R los cuales son v-dependientes a la izquierda, es decir, existen $a_1, a_2, .., a_n$ en R tales que

$$v(\sum a_i\, b_i) < m = \max\{v(a_i) + v(b_i)\} .$$

Podemos asumir

$$v(b_1) \geq v(b_2) \geq \ldots \geq v(b_n)$$

y

$$v(a_i) + v(b_i) = m \qquad \forall\ i .$$

Por lo tanto se tiene

$$v(a_1) \leq v(a_2) \leq \ldots \leq v(a_n) .$$

Elegimos el monomio de grado maximal $x_1 \ldots x_k$ que aparezca en la representación de a_1, con coeficiente $\alpha \neq 0$. Es decir

$$v(a_1) = v(x_1 \ldots x_k) = r .$$

Definimos la función auxiliar,

$$a \longrightarrow a^*$$

como ya lo habíamos hecho, y consideremos

$$\sum a_i^* b_i \ .$$

Por el TEOREMA 35, tenemos

$$(a_i\ b_i)^* \equiv a_i^*\ b_i \pmod{R_{v(b_i)-1}},$$

para cada i.

Además,

$$v(b_i) \leq v(b_1) \quad \text{para todo } i$$

implica

$$R_{v(b_i)-1} \subseteq R_{v(b_1)-1} \ .$$

Luego

$$(\sum a_i\ b_i)^* = \sum (a_i\ b_i)^* \equiv \sum a_i^*\ b_i \pmod{R_{v(b_1)-1}}$$

y por lo tanto

$$(\sum a_i\ b_i)^* - \sum a_i^*\ b_i \in R_{v(b_1)-1}$$

o bien

$$v((\sum a_i\ b_i)^* - \sum a_i^*\ b_i) \leq v(b_1)-1 \ .$$

Por otro lado, obtenemos

$$v((\sum a_i\, b_i)^*) \leq v(\sum a_i\, b_i) - r$$
$$< m - r = v(b_1)$$

y de aquí se concluye

$$v(\sum a_i^*\, b_i) < v(b_1)$$

como $a_1^* = \alpha \in k$, podemos tomar su inverso α^{-1} y entonces tenemos

$$v(b_1 - \sum_{i=2}^{n} \alpha^{-1}\, a_i^*\, b_i) = v(\sum a_i^*\, b_i) < v(b_1)\ .$$

Luego b_1 es v-dependiente de $b_2,\ldots,b_n$.

UN EJEMPLO DE ANILLO CON ALGORITMO DEBIL

Sea k un cuerpo, y M un k-bimodulo. Denotemos por M^r el producto tensorial

$$M^r = M \otimes \ldots \otimes M \qquad r\text{-veces}\ .$$

Existe un isomorfismo

$$M^i \otimes M^j \longrightarrow M^{i+j}$$

que permite definir una multiplicación asociativa entre és tos módulos.

Por ejemplo, para $i=2$, $j=3$ se tiene

$$(x_1 \otimes x_2) \otimes (x_3 \otimes x_4 \otimes x_5) = x_1 \otimes x_2 \otimes x_3 \otimes x_4 \otimes x_5$$

DEFINICION: Se llama Anillo Tensorial sobre M, y se deno ta por T(M), al anillo

$$T(M) = k \oplus M \oplus M^2 \oplus \ldots.$$

T(M) tiene estructura de anillo no conmutativo. La demostración de este hecho aparece en [5] .

Si X es una k-base de M, entonces los elementos de la forma

$$x_1 \otimes x_2 \otimes \ldots. \otimes x_n \qquad \text{con} \quad x_i \in X$$

forman una k-base de M^n .

Por lo tanto, los monomios en X forman una k-base de T(M).

Podemos obtener una filtración sobre T(M), asignando a cada elemento de X el grado 1 y a los otros de la forma

$$\sum x_i \alpha_I$$

se le asigna el grado formal.

Con esta filtración v, X es un conjunto v-independiente , pues si se tiene una expresión

$$\sum x_i \alpha_i \qquad \text{con} \quad x_i \in X, \quad \alpha_i \in T(M),$$

entonces

$$v(\sum x_i \alpha_i) = \max_i \{v(x_i) + v(\alpha_i)\} .$$

Luego, no hay una relación de v-dependencia entre los elementos $\{x_i\}$.

Entonces T(M) satisface el algoritmo débil, pues satisface todas las hipótesis del teorema 36.

CAPITULO 3

RESOLUCION DE ALGUNOS PROBLEMAS

MODULOS CON ALGORITMO DEBIL

Si R es un anillo con filtración v, y si

$$R_n = \{ x \in R \mid v(x) \leq n \}$$

Entonces se satisface

i) $0 = R_{-\infty} \subseteq R_o \subseteq R_1 \subseteq \ldots$

ii) $\bigcup R_n = R$

iii) $R_i R_j \subseteq R_{i+j}$

iv) $1 \in R_o$.

En base a estas propiedades, podemos definir una filtración en un R - módulo M de la siguiente forma.

DEFINICION 2: Una familia $\{M_n\}_{n=o}^{\infty}$ de subgrupos del grupo aditivo M, se dice que es una filtración de M, se

i) $M_o \subseteq M_1 \subseteq M_2 \subseteq \ldots$

ii) $\bigcup M_n = M$

iii) $M_j R_i \subseteq M_{i+j}$ $\quad \forall\, i, j \,,\ i \geq o \,,\ j \geq o$

iv) $M_{-\infty} = \{0\}$

Con esta definición, cada M_j es un R_o - módulo. Además, se puede definir una función

$$v : M \to N \cup \{0\}$$

$$v(x) = \min \{ n \mid x \in M_n \}$$

(Usaremos indistintamente la letra v para esta función y la filtración sobre R).

Luego, valen las propiedades

i) $v(m) \geq 0 \quad \forall\, m \in M - \{0\}$, $v(0) = -\infty$

ii) $v(m_1 - m_2) \leq \max \{v(m_1) , v(m_2)\}$

iii) $v(ma) \leq v(a) + v(m) \quad \forall\, a \in R , \forall\, m \in M$

DEFINICION 2: Un conjunto de elementos $\{m_i\}$ de M es v-dependiente, si existe $\{a_i\} \subset R$ tales que

$$v(\sum m_i a_i) < \max \{ v(a_i) + v(m_i) \}.$$

o algún $m_i = 0$

NOTA : Si los $\{m_i\}$ son linealmente dependientes, entonces son v - dependientes.

DEFINICION 3: Un elemento $m \in M$ es v - dependiente de una familia $(m_i) \subset M$, si existen $\{a_i\} \subset R$ tales que

$$v(m - \sum m_i a_i) < v(m)$$

con $v(m_i) + v(a_i) \leq v(m) \quad \forall i$

DEFINICION 4: Sea N un submódulo de el módulo filtrado M, un conjunto $B \subset N$ es una v - base débil para N si

i) Todos los elementos de N son v-dependientes sobre B.

ii) Ningún elemento $b \in B$ es v-dependiente de $B - \{b\}$

DEFINICION 5: Un R - módulo filtrado posee algoritmo débil, si para cualquier familia v-dependiente (m_i) de elementos de M, con

$$v(m_1) \leq v(m_2) \leq \ldots \leq v(m_n)$$

entonces algún m_i es v-dependiente de $m_1, m_2, \ldots, m_{i-1}$

Si $k = R_o$ es un cuerpo y M tiene algoritmo débil, entonces se obtiene un resultado analogo al TEOREMA 11. Mas precisamente .

TEOREMA 5: Si M cumple las hipotesis anteriores entonces M es libre como R - módulo.

DEMOSTRACION: Sea M con filtración (M_n).
De acuerdo a la definición 1, cada M_n es un k espacio vectorial.
Para cada $t > 0$ definimos .

$$M'_t = \{x \in M_t \mid x \text{ es v-dependiente de } M_{t-1}\}$$

Afirmamos que cada M'_t es un k-espacio vectorial.

En efecto, sean x_1, x_2 en M'_t

Entonces, si $v(x_1 + x_2) = t$

x_1 v - dependiente de M_{t-1} , implica que existen $y_i \in M_{t-1}$, $a_i \in R$ tal que

$$v(x_1 - \sum y_i a_i) < v(x_1) \qquad (*)$$

con $$v(y_i) + v(a_i) \leq v(x_1)$$

Analogamente, existen z_i M_{t-1} , b_i R tal que

$$v(x_2 - \sum z_i b_i) \quad v(x_2) \qquad (**)$$

con $$v(z_i) + v(b_i) \leq v(x_2)$$

Combinando las expresiones (*) y (**) tenemos

$$v(x_1+x_2) - (\sum x_i a_i + \sum y_i b_i)) \leq \max \{v(x_1), v(x_2)\}$$

$$= t = v(x_1 + x_2)$$

Si $v(x_1 + x_2)$ t , entonces $x_1 + x_2$ M_{t-1}

Luego en ambos casos se llega a que $x_1 + x_2 \in M'_t$, y con esto se demuestra que M'_t es cerrado bajo la suma.

Además $Km \in M'_t$ siempre que $m \in M'_t$

Para cada $t > 0$, podemos entonces elegir un conjunto minimal X_t que genera M_t mod M_t'

Entonces $X = \bigcup X_t$ es una v - base débil para M. La demostración es similar a la prueba del teorema 11.

Finalmente probaremos que X es una base de M como R - módulo.

1) <u>X es un conjunto de generadores de M</u>

Sea N el submódulo generado por X

Supongamos $M - N \neq \phi$. Sea $x \in M - N$ tal que $v(x)$ es mínimo.

Por hipotesis existen $\{x_i\}$ en x tal que

$$v(x - \sum x_i a_i) < v(x) \qquad \text{con} \qquad a_i \in R$$

luego $x - \sum x_i a_i \in N$

y además $\sum x_i a_i \in N$.

De aquí se sigue $x \in N$, pero es una contradicción. Por lo tanto $M = N$

2) <u>X es un conjunto linealmente independiente</u>.

Supongamos que se tenga una relación nula entre elementos $\{x_i\} \subseteq X$

$$\sum x_i a_i = 0 \qquad \text{con} \qquad a_i \in R$$

Entonces.

$$v(\sum x_i a_i) < \max \{v(x_i) + v(a_i)\}$$

y esto quiere decir que que la familia $\{x\}$ es v - dependiente. Pero M tiene algoritmo débil y esto implica que algún x_i es v - dependiente del resto, lo cual es una contradicción, por ser X una v - base débil.

DEFINICION 6: Sea M un R-módulo, entonces la filtración trivial v - se define mediante

$$v(0) = -\infty \quad , \quad v(a) = 0 \qquad a \neq 0 \ , \ \forall a \in R$$

$$v(0) = -\infty \quad , \quad v(x) = 0 \qquad x \neq 0 \ , \ \forall x \in M$$

NOTA: Si R es un anillo con algoritmo débil relativo a la filtración trivial, entonces R es un anillo de división.

PROBLEMA 1: Dar una caracterización para módulos con algoritmo débil, relativo a la filtración trivial.

En primer lugar, deduciremos dos propiedades interesantes.

LEMA 7: Toda familia $\{x_i\}$ de elementos de M es v - dependiente, si y sólo si es linealmente dependiente.

DEMOSTRACION: Si para algunos $a_i \in R$, se tiene

$$(\sum x_i a_i) < \max \{v(x_i) + v(a_i)\}$$

Entonces $\sum x_i a_i = 0$

El reciproco es inmediato

LEMA 8: Si una familia $\{x_i\}$ es linealmente dependiente, entonces algún x_i es linealmente dependiente del resto.

DEMOSTRACION: Supongamos, existen $a_i \in R$, tal que

$$\sum x_i a_i = 0$$

y además $v(x_1) \leq v(x_2) \leq \ldots \leq V(x_n)$.

Luego, por el algoritmo débil, algún x_i es v - dependiente de $x_1,\ldots,x_{i-1}$. O sea, existen $C_j \in R$ tal que

$$v(x_i - \sum_{j=1}^{i-1} x_j c_j) < v(x_i)$$

y por lo tanto

$$x_i = \sum_{j=1}^{i-1} x_j c_j$$

TEOREMA 9: M satisface el algoritmo débil, relativo a la filtración trivial, si y sólo si, todo submódulo N de M de la forma

$$N = x_1R + x_2R + \ldots + x_nR, \quad \text{con} \quad x_i \in M$$

es ó suma directa

ó

$$x_i R \subseteq x_1 R + \ldots + x_{i-1} R + x_{i+1} R + \ldots + x_n R$$

DEMOSTRACION: Sea N el submódulo

$$N = x_1 R + \ldots + x_n R$$

Si N no es suma directa, entonces la familia $\{x_i\}$ es linealmente dependiente, y entonces por el Lema 8, algún x_i es linealmente dependiente del resto.

Entonces

$$X_i R \subseteq x_1 R + \ldots + x_n R$$

Reciprocamente, para demostrar que M posee algoritmo débil , sea $\{x_i\}$ una familia de elementos de M los cuales son v - dependientes. Entonces por el Lema 7, estos elementos son linealmente dependientes

Así, el submódulo N

$$N = x_1 R + \ldots + x_n R$$

no es suma directa.

Entonces, para algún i

$$x_i R \subseteq x_1 R + \ldots + x_n R$$

o sea x_i es linelamente dependiente de $x_1, \ldots, x_n$. Por lo tanto M tiene algoritmo débil.

PROBLEMA 2: Demostrar que el centro de un anillo R no ORE , con algoritmo débil es un campo.

DEMOSTRACION: Para demostrar que el centro es un campo es suficiente con probar que todos sus elementos son unidades. Lo cual será cierto si $v(x) = 0$ para todo x en el centro de R.

En efecto $\{x, 1\}$ es una familia v - depediente, pues

$$v(x \cdot 1 - 1 \cdot x) = v(0) < \max\ v(x) + v(1)$$

Además, $v(x) \leq v(1)$

Luego, usando algoritmo débil, 1 es v - depediente de x, y por lo tanto

$$v(1 - x b) < v(1) = 0$$

para algún $b \in R$

Esto implica

$$1 - x b = 0$$

y entonces x es una unidad.

Sea x en el centro de R, $x \neq 0$, $v(x) \neq 0$
Entonces la sucesión $\{v(x), v(x^2) , \ldots, v(x^n), \ldots\}$
es una sucesión de enteros positivos creciente.
Supongamos por, el absurdo que $v(x) = r > 0$ y a partir de un cierto n

$$v(x^n) = v(x^{n+1}) = t > 0$$

Entonces $\{ x^n , x^{n+1} \}$ son v - dependientes, y por el algoritmo débil existe un r tal que

$$v(x^n - x^{n+1} r) < v(x^n) = t \qquad \text{con} \qquad r \in R_o .$$

Ahora bien , $x^n - x^{n+1} r$ es un elemento de grado menor que t, luego x^{n+1} es de grado menor o igual a t.

x^n se puede escribir como combinación lineal de monomios de la k - base de R

$$X^n = \sum x_I a_I \qquad \text{con} \quad a_I \in R, \quad x_I \text{ - monomio}$$

Por el teorema 36 capítulo 2 , el grado de x^n es su grado formal en esta representación.

Luego $v(x^n) = v(x_I) = t$ para algún I

y entonces

$$v(x^{n+1}) = v(x \sum x_I a_I)$$

$$= v(\sum x x_I a_I) > t$$

(Usando el grado formal) .

Finalmente, como R es un anillo no 0RE, podemos escojer a y b en R, con la propiedad

$$a\,R \cap b\,R = (0) \qquad (*)$$

Sea n, tal que

$$v(a) \leq v(x^n) \quad y \quad v(b) \leq v(x^n)$$

La familia $\{a, x^n\}$ es v - dependiente, pues

$$v(x^n a - a x^n) = v(0) < \max\{v(a) + v(x^n)\} .$$

Por el algoritmo débil, x^n es v - dependiente de a; luego existe r_1 tal que

$$v(x^n - a\,r_1) < v(x^n) \quad \text{con} \quad v(a) + v(r_1) = v(x^n)$$

Analogamente, existe un r_2 en R tal que

$$v(x^n - b\,r_2) < v(x^n) \quad \text{con} \quad v(b) + v(r_2) = v(x^n)$$

Haciendo

$$x^n - a\,r_1 = t_1 , \quad x^n - a\,r_2 = t_2$$

nos queda

$$\begin{aligned} v(a\,r_1 - b_2) &= v(t_1 - t_2) \\ &\leq \max\{v(t_1) , v(t_2)\} \\ &< v(x^n) \\ &= v(a) + v(r_1) \end{aligned}$$

Luego la familia $\{a, b\}$ es v - dependiente. Pero a y b son linealmente independientes (por *). Luego en el ideal

a R + b R no puede ser a v - depediente de b (por el TEOREMA 12 capítulo 2). Hemos llegado así a una contradicción, que viene de suponer $v(x) > 0$.

CALCULO DE LA GOCHA PARA UN ANILLO CON ALGORITMO DEBIL

Sea R un anillo filtrado.

Si hacemos

$$gr_n = {}^{R_n}/_{R_{n-1}}$$

entonces si cada gr_n es un k - espacio de dimensión finita, podemos formar la serie de potencias

$$\gamma_R(t) = \sum \alpha_n t^n$$

donde

$$\alpha_n = \dim_k \frac{R_n}{R_{n-1}}$$

$\gamma_R(t)$ se llama la GOCHA de R.

Cuando R posee algoritmo débil, es posible expresar la GOCHA, mediante otra fórmula.

Sea X la base débil de la k - álgebra R, como en la definición 33 capítulo 2.

Vamos a dotar a R de una nueva estructura.

Para cada $h \geq 0$, consideremos

i) R_{h+1} igual a el k - espacio vectorial que tiene por k - base, los monomios de X , de grado menor o igual a

h+1, y del tipo

$$x_I = x_{i_1} \ldots x_{i_n} \qquad x_i \in X$$

y $\quad v(x_{i_j}) \leq h$

R_{h+1} es un anillo filtrado, con función de grado igual a el grado formal de los elementos expresados como combinación lineal de la base.

ii) R_{h+1} es un k - módulo que contiene R_{h+1} como k - submódulo.

Con esta definición, sea ahora

$$\lambda_n = \dim_k \left({}^{R_n}/_{R_n'} \right)$$

TEOREMA 10:

$$\gamma_R(t) = \left(1 - \sum \lambda_n t^n \right)^{-1}$$

DEMOSTRACION: Notemos que ${}^{R_n}/_{R_{n-1}}$ está generado sobre k por todos los monomios x_I de grado n.
Para cada sucesión $(n_1,\ldots,n_r)$ que satisface $n_1+\ldots n_r = n$, da origen a $\lambda_{n_1} \cdot \lambda_{n_2} \ldots \lambda_{n_r}$ monomios de grado n. Luego

$$\alpha_n = \sum_{n_1} \lambda_{n_2} \ldots \lambda_{n_r}$$

donde la suma se toma sobre todas las particiones de n. Por lo tanto

$$\gamma_R(t) = \sum \lambda_{n_1} t^{n_1} \ldots \lambda_{n_r} t^{n_r}$$

Puesto que $\alpha_o = 1$, podemos escribir

$$\gamma_R(t) = 1 + \left(\sum \lambda_{n_i} t^{n_i} \right) + \left(\sum \lambda_{n_i} \lambda_{n_j} t^{n_i+n_j} \right) + \ldots$$

$$= 1 + \sum \lambda_{n_i} t^{n_i} + \left(\sum \lambda_{n_i} t^{n_i} \right)^2 + \ldots$$

Usando la relación

$$(1 - x)^{-1} = 1 + x + x^2 + \ldots$$

se tiene finalmente

$$\gamma_R(t) = \left(1 - \sum \lambda_n t^n \right)$$

Si ¶ es un ideal de R, se define su gocha como:

$$\gamma_R(t); \P) = \sum \beta_n(\P) t^n$$

donde $\beta_n(\P)$ es el número de v - generadores de ¶ de grado n (Ver DEFINICION 13 capitulo 2)

El cociente R/¶ es un k espacio, y cuya base daremos a continuación

Se define $u_o = 1$

Si $n > 0$ y si se tiene una base de $(R_{n-1} + \P)/\P$, entonces se tiene

$$R_{n/\P} = \left(R_n + \P \Big/ R_{n-1} + \P \right) / \left(R_{n-1} + \P \Big/ \P \right)$$

luego, elegimos un conjunto U_n de representantes de la k-base de $\left(R_n + \P\right)\Big/\left(R_{n-1} + \P\right)$

Así, $U = \bigcup U_n$ da una k - base de $R/\P$

Si $\dim_k\left[(R_n + \P) \Big/ (R_{n-1} + \P)\right] = V_n$, entonces se define la gocha relativa de $R/\P$ por

$$\gamma_R(t;\ R/\P) = \sum V_n t^n$$

TEOREMA 11: Se tiene entonces la siguiente relación entre las gochas

$$\gamma_R(t\ ;\ R/\P) = \gamma_R(t)(1 - \gamma_R(t\ ;\ \P))$$

DEMOSTRACION: Sea $U = (u_i)$ la k - base tenida para $R/\P$, y (e_λ) la v - base débil de $\P$.

Entonces R, tiene la representación como suma directa

$$R = \sum u_i k + \sum e_\lambda R \qquad (*)$$

Sustituyendo por R en la segunda suma (*) obtenemos

$$R = \sum u_i k + \quad e_\lambda u_i k + \sum e_\lambda e_\mu R$$

Afirmamos que los elementos

$$u_i \ , \ e_\lambda u_i \ , \ e_\lambda e_\mu u_i \ , \ \ldots \qquad (**)$$

son k - linealmente independientes.

En efecto, presentan dos posibilidades

i) Si se tiene una combinación k - lineal en donde aparezcan los u_i

$$0 = \sum u_i a_{i_1} + \sum e_\lambda u_i a_{i_2} + \ldots + \sum e_{\lambda_1} \ldots \ e_{\lambda_n} u_i \ a_{i_n}$$

entonces al tomar clases módulo ¶ se obtiene

$$\sum u_i a_{i_1} \equiv 0 \mod ¶ \ .$$

pero esto es una contradicción, por la forma como fueron elegidos los u_i .

ii) Si no hay términos en u_i, entonces por la v - independencia de los e_λ , cada coeficiente de los e_λ debe ser cero. Pero cada uno de estos coeficientes, es una combinación de términos en u_i solamente, y entonces llegamos a una contradicción.

Esto demuestra que los elementos en (**) son k - linealmente independientes.

Falta probar que los elementos (**) generan R como k-espacio. Sea $a \in R$, entonces

$$a = \sum u_i \alpha_i + \sum e_\lambda u_i \alpha_\lambda + \ldots + \sum e_{\lambda_1} \ldots e_{\lambda_n} \alpha_{\lambda_1} \ldots \alpha_{\lambda_n}$$

donde todos los α están en k, excepto los de la última suma que están en R.

Podemos tomar $n > v(a)$.

Si $a \in R$, entonces los α_i son todos nulos y se tiene

$$v(a) < n \leq v(e_{\lambda_1} \ldots e_{\lambda_n}) + v(u_i \alpha_{\lambda_1} \ldots \alpha_{\lambda_n})$$

Luego por la v - independencia de los e_λ, el coeficiente $\alpha_{\lambda_1} \ldots \alpha_{\lambda_n}$ debe ser cero. Y por lo tanto, hemos expresado a como una combinación k - lineal de elementos del tipo (**). Si $a \notin \P$ también se tiene el mismo resultado.

Finalmente, calculamos la gocha de R con estos elementos. Primero, hallamos el coeficiente de t^n

$$\alpha_n = V_n + \sum V_\lambda \beta_\mu(\P) + \ldots + \sum V_{\lambda_1} \beta_{\lambda_2}(\P) \ldots \beta_{\lambda_n}(\P)$$

donde $(\lambda_1, \ldots, \lambda_n)$ es cualquier sucesión tal que

$\lambda_1 + \ldots + \lambda_n = n$

Luego

$$\gamma_R(t) = \sum V_n t^n + \ldots + \sum V_{\lambda_1} t^{\lambda_1} \beta_{\lambda}(\P) t^{\lambda_2} \ldots \beta_{\lambda_n}(\P) t^{\lambda_n}$$

$$= (\sum V_{\P} t^{\P}) \ (1 - \sum \beta_s(\P) t^s)^{-1}$$

$$= \gamma_R(t; R/_{\P}) (\gamma_R(t; \P))^{-1}$$

y de aquí se llega a la fórmula

$$\gamma_R(t; R/\P) = \gamma_R(t) \ (1 - \gamma_R(t; \P)).$$

<u>EJEMPLO</u>: Sea $R = F\langle x_1, \ldots, x_d \rangle$ una algebra libre asociativa. Todo elemento de R es la forma

$$\sum x_I a_I \qquad \text{donde} \qquad a_I \in F .$$

$$x_I = x_{i_1} \ldots x_{i_n}$$

Por el teorema 36 capítulo 2, R tiene algoritmo débil.

Supongamos que cada x_i tiene grado 1. Entonces

$$R_0 = k \ , \quad R_1 = R \quad y \quad R_n = R'_n$$

$$n \geq 2$$

Luego

$$\gamma_R(t) = (1 - d\,t)^{-1}$$

Sean ahora un ideal $\P$ de R de rango finito $r \neq 1$ y

$$\dim_k(R/\P) = n$$

Entonces, usando la fórmula del teorema 1, nos queda para $t = 1$

$$n = (1 - d)^{-1}(1 - r)$$

o bien

$$r - 1 = n(d - 1)$$

Esta fórmula se llama FORMULA DE LEWIN y es analoga a la fórmula de Schreier para grupos (Ver [5]).

PROBLEMA Nº 3: Sean R, S algebras graduadas sobre un cuerpo F y $T = R \otimes S$ su producto tensorial. Entonces la gocha de T viene expresada por la fórmula

$$\gamma_T = \gamma_R \cdot \gamma_S$$

DEMOSTRACION: Tenemos

$$R = \bigoplus R_n \qquad S = \bigoplus S_n$$

y por lo tanto

$$\alpha_{R_n} = \dim R_n \quad , \qquad \alpha_{S_n} = \dim S_n$$

$$\gamma_R = \sum \alpha_{R_n} t^n \quad , \qquad \gamma_S = \sum \alpha_{S_n} t^n$$

Analizando un poco la estructura de algebra graduada para R y S, podemos derivar la fórmula

$$T = R \otimes S = R_o \otimes S_o + \bigoplus_n \sum_{i+j=n} R_i \otimes S_j$$

En efecto, si $R = \bigoplus_n R_n$, entonces todo $x_n \in R_n$ se llama elemento homogéneo y si $x \in R$, se tiene

$$x = \sum x_i a_i \quad , \text{ con } \quad x_i \in R_i \quad , \quad a_i \in k \quad ,$$

y los a_i son casi todos nulos.

Ahora bien, los elementos homogeneos de T, vienen dados por

$x \otimes y \in T_n$ si y sólo si

$x \in R_i$, $y \in R_j$ y $i + j = n$

Si (x_{n_i}) es una base de R_n y (y_{m_j}) es una base de S_m entonces los elementos

$(x_{n_i} \otimes y_{m_j})$ con $n + m = p$

forman una base de T_ρ

En consecuencia, se tienen las siguientes relaciones

$$\alpha_{T_1} = \alpha_{R_1} + \alpha_{S_1}$$

$$\alpha_{T_2} = \alpha_{R_2} + \alpha_{R_1}\alpha_{S_1} + \alpha_{S_2}$$

$$\vdots$$

y por lo tanto

$$\gamma_T(t) = 1 + \sum (\alpha_{R_n} + \alpha_{R_1}\alpha_{S_{n-1}} + \ldots + \alpha_{S_n}) t^n \qquad (*)$$

Usando la fórmula del producto para polimonios

$$(1 + a_1 x + \ldots + a_n x^n)(1 + b_1 x + \ldots + b_n x^n)$$

$$= 1 + (a_1 + b_1)x + (a_2 + a_1 b_1 + b_2)x^2 + \ldots\ldots$$

la cual es válida para todo n, podemos factorizar (*)

$$\gamma_T(t) = (\sum \alpha_{R_n} t^n)(\sum \alpha_{S_n} t^n)$$

$$= \gamma_R(t) \cdot \gamma_S(t) .$$

BIBLIOGRAFIA

|1| P. M. COHN — Free Rings and their relations
Academic Press - London - 1971

|2| CHIH SAH — Abstract Algebra
Academic Press - New York-1967

|3| MATIYAH, I.G, MACDONALD — Introducción al Algebra Conmutativa . Ed. Reverte - España-1969

|4| H.W. LENSTRA ,JR. — Lectures on Euclidean Rings
Biellfeld, Summer - 1974

|5| MARSHALL HALL — Teoría de Grupos
Ed. Trillas - México - 1969

|6| P.M. COHN — Free Ideal Rings
Journal of Algebra - 1964

|7| P.M. COHN — Rings with a weak Algorithm
Trans . Amer . Math. Soc 109.
193.