Lecturas Matemáticas
Volumen **35** *(2) (2014), páginas 169–182*
ISSN 0120–1980

El problema de Waring en anillos conmutativos[1]

Waring's problem in commutative rings

Jose Rafael Huertas Sanabria
Bogotá, Colombia

Resumen. Para un anillo conmutativo unitario A y un número entero $d \geq 1$, consideramos las constantes $w(d, A)$ y $v(d, A)$. Estas constantes generalizan el problema de Waring al anillo A. Presentamos resultados del problema en una $K-$álgebra A, donde K es un cuerpo y en el caso que A sea un anillo local henseliano de característica residual $p > 0$.

Key words: Commutative unitary ring, local Henselian ring, K-algebra, Henselization, rank binary form.

Abstract. For a commutative unitary ring A and an integer $d \geq 1$, we consider the constants $w(d, A)$ and $v(d, A)$. These constants generalize Waring's problem to the ring A. We present results of the problem in a $K-$algebra A, where K is a field and in the case that A is a Henselian local ring of residual characteristic $p > 0$.

2010 AMS Mathematics Subject Classification. 11P05. 12E20, 13-02, 13B40

Introducción

El *problema de Waring* en $\mathbb{N}$ consiste en determinar si dado $k \in \mathbb{N}$, existe un entero s, que depende solo de k, tal que cada entero $n \geq 1$ se puede expresar de la forma

$$n = n_1^k + n_2^k + \cdots + n_s^k \tag{1}$$

con $n_1, n_2, \ldots, n_s \in \mathbb{N}$.

Se denota por $g(k)$ el menor valor de s tal que todo $n \geq 1$ se puede representar de la forma (1).

[1]Este artículo esta basado en el trabajo final titulado *El problema de Waring en anillos conmutativos*, presentado para optar al título de Magister en Matemáticas en la Universidad Nacional de Colombia.

En 1770 LAGRANGE probó que $g(2) = 4$, resultado conocido como teorema de los cuatro cuadrados ([9] teorema 6.26) y en 1909 D. HILBERT probó la existencia de $g(k)$ para todo entero positivo k ([2] teorema 5.1). Para otros resultados se puede ver [2].

El problema de Waring se ha generalizado a otros conjuntos, por ejemplo para un cuerpo finito $\mathbb{F}_q$ con $q = p^n$ elementos, ver [3] y [4].

El propósito de este artículo es presentar algunos resultados del problema de Waring en un anillo conmutativo unitario.

En la sección 1 se enuncian algunos resultados relativos a cuerpos y anillos.

En la sección 2 se presentan algunos resultados sobre las constantes $w(d, A)$ y $v(d, A)$. Estas constantes permiten generalizar el problema de Waring a un anillo conmutativo A.

En la sección 3 se presentan resultados del problema de Waring en una K-álgebra donde K es un cuerpo y en un anillo local henseliano A.

Para finalizar, en la sección 4 se estudia el problema de Waring para formas binarias de grado d con coeficientes en un cuerpo de característica cero. En particular, como consecuencia del estudio del rango de la forma binaria xy^{d-1}, se obtienen resultados del problema para $K = \mathbb{R}$ y $K = \mathbb{C}$.

1. **Preliminares.**

En este trabajo la palabra anillo significa anillo conmutativo con elemento unidad $1 \neq 0$. Sea A un anillo. Un elemento $a \in A$ es *invertible* o una *unidad* en A si existe un elemento $b \in A$ tal que $ab = 1$. El grupo multiplicativo de los elementos invertibles de A se denota por $A^\times$. El anillo A es un *cuerpo* si $A^\times = A \setminus \{0\}$.

Definición 1. Dados dos anillos A y B, un *homomorfismo unífero* es un homomorfismo de anillos $f : A \to B$ tal que $f(1) = 1$.

En lo que sigue, la palabra homomorfismo significa homomorfismo unífero.

Sean $A_1, A_2, \ldots, A_n$ anillos. El *producto*

$$A = \prod_{i=1}^{n} A_i = \{(x_1, x_2, \ldots, x_n) : x_i \in A_i, 1 \leq i \leq n\}$$

es un anillo conmutativo unitario con las operaciones suma y producto componente a componente. Cada proyección $p_i : \prod_{i=1}^n A_i \to A_i$ es un homomorfismo sobreyectivo.

Si I es un ideal de A, la función $\pi : A \to A/I$, dada por $\pi(r) = r + I$ es un epimorfismo llamado *epimorfismo canónico*.

La característica de un cuerpo K es 0 o un número primo $p > 0$. Si $p = 0$, K contiene como subcuerpo una imagen isomorfa de los números racionales y si $p > 0$, contiene una imagen isomorfa de $\mathbb{F}_p$.

Definición 2. Un subconjunto S de un anillo A es *multiplicativo* si:

i) $0 \notin S, 1 \in S$,
ii) Si $a, b \in S$, entonces $ab \in S$.

Sea A un anillo y M un grupo abeliano. Se dice que M es un A-módulo si existe una aplicación

$$A \times M \to M$$

$$(a, x) \mapsto ax$$

tal que para cada $a, b \in A$ y cada $x, y \in M$ se cumplen las siguiente condiciones:

$$a(x + y) = ax + ay,$$

$$(a + b)x = ax + bx,$$

$$(ab)x = a(bx),$$

$$1x = x.$$

Sea R un subconjunto de un A-módulo M. El conjunto

$$\langle R \rangle = \left\{ \sum_{i=1}^{n} a_i r_i : a_i \in A, r_i \in R, n \geq 1 \right\}$$

es un submódulo de M llamado el *submódulo generado por R*. Se dice que M es *de generación finita* o *finitmente generado* si R es finito y $\langle R \rangle = M$.

Definición 3. Sea A un anillo. Un anillo B es una $A-$*álgebra* si existe un homomorfismo de anillos $f : A \to B$.

Si $f : A \to B$ es un homomorfismo de anillos, entonces B es un A-módulo con el producto $ab = f(a)b$. El anillo B es una $A-$álgebra *finita* si B es de generación finita como A-módulo.

Es claro que todo anillo A es una $\mathbb{Z}$-álgebra con el homomorfismo $n \mapsto n \cdot 1$.

Sean A un anillo K un cuerpo. A es una K-álgebra si y solo si A contiene una copia isomorfa de K como un subanillo.

Sea A un anillo. Recordemos que un ideal $M \neq A$ de A es *maximal* si no existe un ideal B de A tal que $M \subsetneqq B \subsetneqq A$. Un ideal P de A es *primo* si $P \neq \langle 1 \rangle$ y si $xy \in P$ implica $x \in P$ o $y \in P$.

Definición 4. Un anillo A se llama *local* si tiene un único ideal maximal.

Teorema 1. *Sea M un ideal en un anillo A. Entonces M es un ideal maximal si y solo si A/M es un cuerpo.*

Sea A un anillo local con ideal maximal M. El cuerpo A/M se denomina *el cuerpo residual* de A.

Sean A un anillo local con ideal maximal M y $K = A/M$ el cuerpo residual. Si $a \in A$, la clase de $a + M \in K$ se denota por $\overline{a}$. Si $f(x) = \sum_{i=0}^{n} a_i x \in A[x]$, se define $\overline{f}(x) = \sum_{i=0}^{n} \overline{a}_i x \in K[x]$. Se puede demostrar que si $f(X) \in A[X]$ es tal que $\overline{f}(x) \in K[X]$ tiene una raíz simple $a \in K$, entonces $f(x)$ tiene una raíz simple $\alpha \in A$ tal que $\overline{\alpha} = a$ (ver [11] p. 4.).

Definición 5. Sea A un anillo local con ideal maximal M. Se dice que A es *Henseliano* si todo polinomio mónico $f(X) = X^n + \cdots + a_1 X + a_0 \in A[X]$ con $a_1 \in A^\times$ y $a_0 \in M$ tiene una raíz en M.

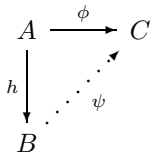
Se puede probar que si $f(X) = X^n + \cdots + a_1 X + a_0$ con $a_1 \in A^\times$ y $a_0 \in M$ tiene una raíz en M, entonces esta raíz es única.

El siguiente resultado está demostrado en [10], teorema 4.2.

Teorema 2. *Las siguientes afirmaciones son equivalentes:*

(i) A es henseliano.
(ii) Cada A-álgebra finita B es un producto de anillos locales.

Definición 6. Sean A un anillo local y $h : A \to B$ un homomorfismo de anillos locales. Se dice que B es la *henselización* de A si B es henseliano y para cada homomorfismo local ϕ de A en un anillo local henseliano C, existe un único homomorfismo local de anillos $\psi : B \to C$ tal que el siguiente diagrama conmute



Para un polinomio $f(x)$, sea $\Delta(f(x)) = f(x+1) - f(x)$ el operador lineal de primera diferencia. Para un entero $m > 0$, sea $q_m(x) = x(x-1)\cdots(x-m+1)$. Entonces $\Delta(q_m(x)) = m q_{m-1}(x)$. Sea $s(d,k)$ el coeficiente de x^k en el polinomio $q_d(x)$, es decir

$$q_d(x) = \sum_{k=0}^{d} s(d,k) x^k.$$

Aplicando $(d-1)-$veces el operador Δ a ambos lados de la igualdad y como $s(d-1,d) = \dfrac{d(d-1)}{2}$ se obtiene

$$d!x = \Delta^{(d-1)}\left(s(d-1,d)x^{d-1}\right) + \Delta^{d-1}(x^d)$$

$$= \frac{d(d-1)(d-1)!}{2} + \Delta^{d-1}(x^d).$$

Luego se obtiene la siguiente identidad:

$$d!x + \frac{(d-1)d!}{2} = \sum_{h=0}^{d-1}(-1)^{(d-1-h)}\binom{d-1}{h}(x+h)^d. \tag{2}$$

2. Generalidades sobre las funciones $w(d, A)$ y $v(d, A)$.

Sean $d \geq 1$ un entero y A un anillo. Consideremos los conjuntos

$$A^d = \{a^d : a \in A\},$$

$$A_d^+ = \{x \in A : x = a_1^d + a_2^d + \cdots + a_n^d,\ n \geq 1,\ a_1, a_2, \ldots, a_n \in A\},$$

$$\begin{aligned} A_d = \{&x \in A : x = e_1 a_1^d + e_2 a_2^d + \cdots + e_n a_n^d,\ n \geq 1, \\ &e_i = \pm 1,\ a_1, a_2, \ldots, a_n \in A\}. \end{aligned}$$

Se tienen que $A^d \subset A_d^+ \subset A_d \subset A$ y A_d es un subanillo de A generado por A^d.

Denotamos con $w(d, A)$ al menor entero s tal que todo elemento x de A_d^+ se puede expresar de la forma

$$x = a_1^d + a_2^d + \cdots + a_s^d \tag{3}$$

con $a_1, \ldots, a_s \in A$ si tal entero existe, de lo contrario $w(d, A) = \infty$; con $v(d, A)$ al menor entero s tal que todo elemento x de A_d se puede expresar de la forma

$$x = e_1 a_1^d + e_2 a_2^d + \cdots + e_s a_s^d \tag{4}$$

con $a_1, \ldots, a_s \in A$ y $e_i = \pm 1$, si tal entero existe; de lo contrario $v(d, A) = \infty$ y por $u(d, A)$ el menor entero s tal que

$$-1 = a_1^d + a_2^d + \cdots + a_s^d$$

con $a_1, \ldots, a_s \in A$ si tal entero existe, de lo contrario $u(d, A) = \infty$.

Proposición 3. *Sean A un anillo y $d \geq 1$ un entero. Si $u(d, A) < \infty$, entonces*

$$u(d, A) \leq w(d, A);$$

$$v(d, A) \leq w(d, A);$$

$$w(d, A) \leq u(d, A)v(d, A).$$

En particular , si d es impar,

$$v(d, A) = w(d, A).$$

Demostración. Como $u(d,A) = s < \infty$, entonces $A_d^+ = A_d$. Luego $-1 \in A_d^+$. Esto implica que $u(d,A) \leq w(d,A)$ y que $v(d,A) \leq w(d,A)$. Ahora, si $v(d,A) = \infty$ la tercera desigualdad se cumple. Supongamos que $v(d,A) = t < \infty$. Sea $x \in A_d^+$. Entonces existen $a_1, a_2, \ldots, a_s, b_1, b_2, \ldots, b_t \in A$ y tales que $-1 = a_1^d + a_2^d + \cdots + a_s^d$ y $x = e_1 b_1^d + e_2 b_2^d + \cdots + e_t b_t^d$, donde $e_i = \pm 1$. Reemplazando -1 en la última ecuación se obtiene que $w(d,A) \leq u(d,A)v(d,A)$. ☑

Proposición 4. *Sea $h : A \to B$ un homomorfismo de anillos. Sean N el núcleo de h y $d \geq 1$ un entero. Entonces*

(i) $h(A_d) \subset B_d$;
(ii) $u(d,B) \leq u(d,A)$.
Si h es sobreyectivo, entonces
(iii) $h(A_d) = B_d$, $h(A_d^+) = B_d^+$;
(iv) $w(d,B) \leq w(d,A)$, $v(d,B) \leq v(d,A)$;
(v) *si todo elemento x del ideal N se expresa de la forma 4, entonces*

$$v(d,A) \leq w(d,B) + s;$$

(vi) *si todo elemento x del ideal N se expresa de la forma 3, entonces*

$$w(d,A) \leq w(d,B) + s.$$

Demostración. Las partes (i), (ii) y (iii) resultan de las definiciones y del hecho de que h es sobre.

(iv) Si $w(d,A) = \infty$ el resultado es evidente. Supongamos que $w(d,A) = t$ y sea $y \in B_d^+$. Por (iii) existe $x = a_1^d + a_2^d + \cdots + a_t^d \in A_d^+$ tal que $h(x) = h(a_1)^d + h(a_2)^d + \cdots + h(a_t)^d = y$. Luego $w(d,B) \leq w(d,A)$. Por un razonamiento similar se prueba que $v(d,B) \leq v(d,A)$.

(v) Si $v(d,B) = \infty$ el resultado se cumple. Supongamos que $v(d,B) = t$ y sea $x \in A_d$. Existen $a_1, a_2, \ldots, a_t \in A$ tales que $x = e_1 a_1^d + e_2 a_2^d + \cdots + e_t a_t^d$. Esto implica que $x - e_1 a_1^d - e_2 a_2^d - \cdots - e_t a_t^d \in N$. Entonces existen $b_{t+1}, b_{t+2}, \ldots, b_{t+s} \in A$ tales que $x = e_1 a_1^d + e_2 a_2^d + \cdots + e_t a_t^d + e_{t+1} b_{t+1}^d + e_{t+2} b_{t+2}^d + \cdots + e_{t+s} b_{t+s}^d$. Por lo tanto $w(d,A) \leq t + s = w(d,B) + s$. De manera similar se prueba (vi). ☑

Corolario 5. *Sean A un anillo, $d \geq 1$ un entero y B el anillo cociente $A/d!A$. Entonces*

$$v(d,A) \leq v(d,B) + 2^d;$$

si d es impar o si 2 es invertible en A, entonces

$$v(d,A) \leq v(d,B) + 2^{d-1}.$$

Demostración. Por la identidad

$$d!x = \sum_{h=0}^{d-1} (-1)^{(d-1-h)} \binom{d-1}{h} \left[(x+h)^d - h^d \right], \tag{5}$$

todo elemento del ideal $d!A$ se expresa de la forma 4 con

$$s = 2\sum_{h} \binom{d-1}{h} = 2 \cdot 2^{d-1} = 2^d;$$

por la parte (v) de la proposición 4, se tiene que $v(d, A) \leq v(d, B) + 2^d$. Usando la identidad

$$d!x + \frac{(d-1)d!}{2} = \sum_{h=0}^{d-1} (-1)^{(d-1-h)} \binom{d-1}{h} (x+h)^d \tag{6}$$

se prueba la otra desigualdad. ☑

Proposición 6. *Sean $A_1, A_2, \ldots, A_k$ anillos, $B = \prod_{i=1}^{k} A_i$ y $d \geq 1$ un entero. Entonces,*

$$w(d, B) = \sup_i w(d, A_i).$$

Demostración. Como cada proyección $P_i : B \to A_i$ es un homomorfismo sobre, por la proposición 4, $w(d, A_i) \leq w(d, B)$ para cada i, luego $\sup_i w(d, A_i) \leq w(d, B)$. Veamos ahora que $w(d, B) \leq \sup_i w(d, A_i)$. Si $w(d, A) = \infty$ para algún i el resultado se cumple. Supongamos que $w(d, A) < \infty$ para todo i y sea $x \in B_d^+$. Entonces $x = (x_1, x_2, \ldots, x_k)$ donde $x_i \in (A_i)_d^+$ para $i = 1, 2, \ldots, k$. Por lo tanto $w(d, A) \leq \sup_i w(d, A_i)$. ☑

Proposición 7. *Sean A un anillo, S una parte multiplicativa de A y $d \geq 1$ un entero. Entonces,*

$$w(d, S^{-1}A) \leq w(d, A),$$

$$v(d, S^{-1}A) \leq v(d, A).$$

Demostración. Si $w(d, A) = \infty$ se tiene que $w(d, S^{-1}A) \leq w(d, A)$. Supongamos que $w(d, A) < \infty$ y sea $x \in \left(S^{-1}A\right)_d^+$. Entonces $x = \left(\frac{a_1}{s_1}\right)^d + \left(\frac{a_2}{s_2}\right)^d + \cdots + \left(\frac{a_n}{s_n}\right)^d$ con $\frac{a_1}{s_1}, \frac{a_2}{s_2}, \ldots, \frac{a_n}{s_n} \in S^{-1}A$. Si $s = s_1 s_2 \cdots s_n$, x se puede escribir de la forma $x = (s^{-1}b_1)^d + (s^{-1}b_2)^d + \cdots + (s^{-1}b_n)^d$ donde $s^{-1}b_i \in A$, $i = 1, \ldots, n$. Esto implica que $w(d, S^{-1}A) \leq w(d, A)$. De manera similar se prueba que $v(d, S^{-1}A) \leq v(d, A)$. ☑

3. El Problema de Waring en Anillos Conmutativos Generales.

El número $w(d, A)$ generaliza a un anillo conmutativo unitario A el problema de Waring y el número $v(d, A)$ generaliza lo que se conoce como el problema fácil de Waring.

Ejemplo 8. Sean $\mathbb{F}_q$ un cuerpo finito con $q = p^n$ elementos y k un entero positivo. Denotamos por $g(k, p^n)$ el menor entero positivo s tal que cada $\alpha \in \mathbb{F}_q$ se puede expresar de la forma

$$\alpha = x_1^k + x_2^k + \cdots + x_s^k,$$

con $x_1, x_2, \ldots, x_s \in \mathbb{F}_q$ si tal entero existe, de lo contrario $g(k, p^n) = \infty$.

El problema de Waring en $\mathbb{F}_q$ consiste en determinar $g(k, p^n)$ para cada entero positivo k. Se tiene el siguiente resultado (ver [3], p.172)

Proposición 9. *Si $g(k, p^n)$ existe, entonces $g(k, p^n) \leq k$.*

Para otros resultados del problema de Waring en $\mathbb{F}_q$ se puede consultar [3] y [4].

Ejemplo 10. Si K es un cuerpo de números algebraicos, la suma de cuadrados en K, son los elementos totalmente positivos de K, y todo elemento totalmente positivo de K es la suma de 4 cuadrados, de donde $w(2, K) \leq 4$ (ver [1], ejemplo 7.7).

Ejemplo 11. Si $\mathbb{Q}_p$ es el cuerpo de los racionales $p-$ádicos, $p \neq 2$ y d no es una potencia de 2, entonces $w(d, \mathbb{Q}_p) \leq d^2$. En el caso que $p = 2$ y d es una potencia de 2, se tiene que $w(d, \mathbb{Q}_p) \leq 2d^2$. Ahora, para el anillo $\mathbb{Z}_p$ de los enteros p-ádicos y $d \geq 1$ un entero, se cumple que $w(d, \mathbb{Z}_p) \leq 4d - 1$ (ver [1], p. 97 y 105).

Ejemplo 12. Para todo cuerpo K,

$$v(2, K) \leq 2.$$

En efecto, si la característica de K es 2, entonces $-1 = 1$ y la suma de cuadrados es un cuadrado, de donde $v(2, K) = 1$. Si la característica de K es distinta de 2, todo $x \in K$ se puede escribir de la forma $x = \left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2$, luego $v(2, K) \leq 2$.

Teorema 13. *Para todo anillo A,*

$$v(2, A) \leq 3.$$

Demostración. Sea $a \in A_2$. Existen $m \geq 1$, $x_1, x_2, \ldots, x_m \in A$ y $e_1, e_2, \ldots, e_m = \pm 1$ tales que

$$a = e_1 x_1^2 + e_2 x_2^2 + \cdots + e_m x_m^2.$$

Sea $x = x_1 + x_2 + \cdots + x_m + 1$. Entonces

$$a - x^2 = \sum_i (e_i - 1) x_i^2 - 2 \sum_{i<j} x_i x_j - 2 \sum_i x_i - 1.$$

Para todo i, $e_i - 1 = 0$ o $e_i - 1 = -2$ y como $-1 = -2 + 1$, entonces $a - x^2 = 2y + 1$ con $y \in A$. Pero $2y + 1 = (y+1)^2 - y^2$. Entonces $a = x^2 + (y+1)^2 - y^2$, es decir $v(2, A) \leq 3$. ☑

Lema 14. *Sean A una álgebra sobre un cuerpo de característica 0 y $d \geq 1$ un entero. Entonces*

$$v(d, A) \leq 2^{d-1}.$$

Demostración. Sea K el cuerpo de característica 0 tal que $K \subset A$. Entonces $d!$ es invertible en K y por lo tanto en A. La aplicación

$$x \mapsto d!x + \frac{(d-1)d!}{2}$$

es una biyección de A en A. Por la identidad 2, todo elemento de A se puede escribir de la forma

$$\sum_{h=0}^{d-1} (-1)^{(d-1-h)} \binom{d-1}{h} (x+h)^d;$$

de donde $A = A_d$ y

$$v(d, A) \leq \sum_{h=0}^{d-1} \binom{d-1}{h} = 2^{d-1}.$$

☑

Lema 15. *Sean K un cuerpo de característica $p > 0$, A una K-álgebra y $d \geq 1$ un entero con $d \leq p$. Entonces*

$$w(d, A) \leq d^2;$$
$$v(d, A) \leq d^2.$$

Demostración. Si $d = p$, entonces $(x+y)^p = x^p + y^p$ para todo $x, y \in A$, de donde $w(d, A) = 1$. Si $d < p$, entonces $d!$ no es divisible por p, luego es invertible en A. La aplicación

$$x \mapsto d!x + \frac{(d-1)d!}{2}$$

es una biyección de A en A. Por la identidad 2, todo elemento de A se puede escribir de la forma

$$\sum_{h=0}^{d-1} (-1)^{(d-1-h)} \binom{d-1}{h} (x+h)^d.$$

Cada coeficiente $(-1)^{(d-1-h)}\binom{d-1}{h}$ pertenece al cuerpo $\mathbb{F}_1$ y por lo tanto se puede escribir como la suma de a lo más d potencias d-ésimas. Luego todo elemento e A se puede escribir como la suma de a lo más d^2 potencias d-ésimas, es decir $w(d, A) \leq d^2$. Ahora, por la proposición 3, $v(d, A) \leq w(d, A)$, de donde $v(d, A) \leq d^2$. ☑

Proposición 16. *Sean A una álgebra sobre un cuerpo de característica 0 y $d \geq 1$ un entero. Si $u(d, A) < \infty$, entonces*

$$w(d, A) \leq 2^{d-2}(1 + u(d, A)).$$

Demostración. Todo elemento de A se puede escribir e la forma

$$\sum_{h=0}^{d-1}(-1)^{(d-1-h)}\binom{d-1}{h}(x+h)^d.$$

Para $h = d-2, d-4, \ldots$, al reemplazar $-1 = (-1)^{d-1-h}$ por una suma de $u(d;A)$ potencias d-ésimas se obtiene una suma

$$\left[\binom{d-1}{d-1}+\binom{d-1}{d-3}+\cdots\right]+\left[\binom{d-1}{d-2}+\binom{d-1}{d-4}+\cdots\right]u(d,A)$$

de $2^{d-2}+2^{d-2}u(d,A)$ potencias d-ésimas. Luego
$w(d,A) \leq 2^{d-2}+2^{d-2}u(d,A) = 2^{d-2}(1+u(d,A))$. ☑

Para un anillo local henseliano se tienen los siguientes resultados.

Lema 17. *Sea A un anillo local henseliano con ideal maximal M y cuerpo residual K. Sean $p>0$ la característica de K, $d \geq 1$ un entero no divisible por p y $\pi : A \to K$ el homomorfismo canónico. Entonces $w(d,A) \leq w(d,K)+1$.*

Demostración. Como π es sobre, por la proposición 4, (iii), se tiene que $\pi(A_d^+) = K_d^+$. Si $w(d,K) = \infty$, el resultado se cumple. Supongamos que $w(d,K) = m < \infty$. Sea $a \in A_d^+$. Entonces $\pi(a) = y_1^d + \cdots + y_m^d$ con $y_1, \ldots, y_m \in K_d^+$. Si a es una unidad, entonces $\pi(a) \neq 0$; supongamos por ejemplo que $y_1 \neq 0$. Sean $a_2, \ldots, a_m$ lo elementos de A tales que $\overline{a_2} = y_2, \ldots, \overline{a_m} = y_m$. Consideremos en $A[X]$ el polinomio $f(X) = X^d + a_2^d + \cdots + a_m^d - a$. Como A es henseliano, existe a_1 en A tal que $f(a_1) = 0$ y como $p \nmid d$, $a = a_1^d + \cdots + a_m^d$, es decir $w(d,A) \leq w(d,K)$. Si a no es una unidad, entonces $a-1$ es una unidad y por un razonamiento similar al anterior se prueba que $a-1 = a_1^d + \cdots + a_m^d$ con $a_1, \ldots, a_m \in A$; luego $a = 1^d + a_1^d + \cdots + a_m^d$, de donde $w(d,A) \leq w(d,K)+1$. ☑

Lema 18. *Sea A un anillo local henseliano de característica residual $p>0$. Entonces*

$$w(p,A) \leq \begin{cases} 6, & \text{si } p=2, \\ 2p-1, & \text{si } p>2. \end{cases}$$

Demostración. Sean $\mathbb{Z}_{(p)}$ la localización de $\mathbb{Z}$ en $\langle p\rangle$ y B la henselización de $\mathbb{Z}_{(p)}$. Como A es henseliano de característica residual p, el homomorfismo canónico $\mathbb{Z} \to \mathbb{A}$, se prolonga a un homomorfismo $h : B \to A$. Se presentan dos casos:
i) Caso $p=2$. Consideremos el polinomio $X^2 - X + 2 \in B[X]$. Este polinomio tiene do raíces en B. Sea a una de ellas, entonces $a^2 - a + 2 = 0$, de donde $-1 = (2a-1)^2 + 2^2 + 1^2 + 1^2$. Por el teorema 13, todo elemento $a \in A_2$ se puede escribir de la forma $a = x^2 + (y+1)^2 - y^2$; reemplazando -1 se obtiene que $a = x^2 + (y+1)^2 + [(2a-1)y]^2 + (2y)^2 + y^2 + y^2$, es decir $w(2,A) \leq 6$.

ii) Caso $p > 2$. En la demostración que presenta Joly usa el hecho de que A es una B-álgebra y considera un cociente de una álgebra de polinomios $C = B[T]$, donde T es una familia de indeterminadas. Primero prueba que $w(p, C/pC) = 1$. Luego observa que todo elemento de pC es suma de $2p-2$ potencias p-ésimas ya que el polinomio $X^{p-1} - 1$ tiene en B y por lo tanto en C, las raíces $(p-1)$-ésimas de la unidad $\zeta_1, \zeta_2, \ldots, \zeta_{p-1}$. Obtiene para todo $x \in C$, la igualdad

$$(-1)^p p(p-1)x = \sum_{j=1}^{p-1} \left((\zeta_i - x)^p + x^p\right);$$

y concluye que

$$w(p, B) \leq w(p, B/pB) + (2p-2) = 1 + (2p-2) = 2p-1.$$

☑

Teorema 19. *Sea A un anillo local henseliano con cuerpo residual K finito. Si d es primo, entonces*

$$w(d, A) \leq \begin{cases} 6, & \text{si } d = 2, \\ 2d-1, & \text{si } d > 2. \end{cases}$$

Demostración. Sea p la característica de K. Si $d = p$, la desigualdad resulta del lema 18. Si $d \neq p$, entonces $\operatorname{mcd}(d, p) = 1$. Por la proposición 9, $w(d, K) \leq d$. Por el lema 17, $w(d, A) \leq w(d, K) + 1 = d + 1$. Ahora, si $d = 2$, $d + 1 \leq 6$ y si $d > 2$, $d + 1 \leq 2d - 1$. ☑

Teorema 20. *Sea A un anillo finito y d un primo. Entonces*

$$w(d, A) \leq \begin{cases} 6, & \text{si } d = 2, \\ 2d-1, & \text{si } d > 2. \end{cases}$$

Demostración. A es el producto directo finito de anillos locales henselianos, es decir, $A = A_1 \times A_2 \times \cdots \times A_n$. Por la proposición 6 y el teorema 19 se tiene el resultado. ☑

Teorema 21. *Sean A un anillo y d un primo. Si el anillo cociente $A/d!A$ es un producto finito de anillos locales henselianos, entonces*

$$v(d, A) \leq \begin{cases} 3, & \text{si } d = 2, \\ 2^{d-1} + 2d - 1, & \text{si } d > 2. \end{cases}$$

Demostración. Si $d = 2$, por 13, $v(d, A) \leq 3$. Si $d > 2$, d es impar y por el corolario 5 $v(d, A) \leq 2^{d-1} + v(d, A/d!A)$. Ahora, por 6 y 19 se tiene que $w(d, A) \leq 2d - 1$. Por 3, $v(d, A) \leq w(d, A)$ de donde $v(d, A) \leq 2d - 1$. Así, $v(d, A) \leq 2^{d-1} + 2d - 1$. ☑

Corolario 22. *Sean A un anillo y d un primo. Si el anillo cociente $A/d!A$ es finito, entonces*

$$v(d,A) \leq \begin{cases} 3, & si\ d=2, \\ 2^{d-1}+2d-1, & si\ d>2. \end{cases}$$

Demostración. El anillo $A/d!A$ se puede expresar como un producto finito de anillos locales henselianos, por ser finito. ☑

4. El Problema de Waring en $K[x,y]$.

Sea K un cuerpo de característica cero. Para $d \geq 1$ entero, sea $K[x,y]_d$ el espacio de los polinomios homogéneos de grado d en las variables x, y con coeficientes en K.

Definición 7. Sea $f \in K[x,y]_d$. El *rango* de f, $R_K(f)$, es el menor entero r tal que f se puede escribir de la forma

$$f = c_1 l_1^d + \cdots + c_r l_r^d$$

con $c_i \in K$ y $l_i \in K[x,y]_1$, $i = 1, \ldots, r$.

El rango de f también se llama *rango de Waring*. Si K es algebraicamente cerrado los coeficientes no son necesarios ya que $c_i l^i$ puede ser reemplazado por $(c_i^{1/d} l_i)^d$.

Para $K = \mathbb{C}$ se tiene el siguiente resultado, proposición 3.1 [13].

Teorema 23. *Sea $m = x^a y^b$ un monomio en $\mathbb{C}[x,y]$. Si $0 < a \leq b$, entonces $R_{\mathbb{C}}(m) = b + 1$.*

El teorema 23 implica que $R_{\mathbb{C}}(xy^{d-1}) = d$ para $d \geq 2$, es decir xy^{d-1} se puede expresar de la forma

$$xy^{d-1} = l_1^d + \cdots + l_d^d$$

donde $l_1, \ldots, l_d$ son formas lineales. Si evaluamos la forma xy^{d-1} en $y = 1$, podemos concluir que para cada $x \in \mathbb{C}$, $x = a_1^d + \cdots + a_d^d$ con $a_1, \ldots, a_d \in \mathbb{C}$, lo cual implica que $w(d, \mathbb{C}) \leq d$.

Si $K = \mathbb{R}$ se tiene lo siguiente, proposición 4.4 [13].

Teorema 24. *Sea $m = x^a y^b$ un monomio en $\mathbb{R}[x,y]$. Si $0 < a \leq b$, entonces $R_{\mathbb{R}}(m) = a + b$.*

Si $d \geq 2$, por el teorema 24 se tiene que $R_{\mathbb{R}}(xy^{d-1}) = d$. Entonces

$$xy^{d-1} = c_1 l_1^d + \cdots + c_d l_d^d$$

con $c_i \in \{-1, 1\}$. Evaluando la forma xy^{d-1} en $y = 1$ obtenemos que $v(d, \mathbb{R}) \leq d$.

En el trabajo realizado por Bialynicki y Schinzel, presentan el siguiente resultado para la forma binaria xy^{d-1}, lema 7.1 [14].

Lema 25. *La fórmula*

$$dxy^{d-1} = \sum_{i=1}^{d} \frac{(x + z_i y)^d}{\prod\limits_{j=1, j\neq i}^{d} (z_i - z_j)}$$

para distintos z_i que satisfacen

$$z_1 + \cdots + z_d = 0$$

da todas las presentaciones de la forma dxy^{d-1} con rango d.

Ejemplo 26. Si $z_1 = 1$, $z_2 = -1$, $z_3 = 2$ y $z_4 = -2$, entonces

$$xy^3 = \frac{1}{48}\left[2(x-y)^4 - 2(x+y)^4 + (x+2y)^4 - (x-2y)^4\right].$$

Al reemplazar $y = 1$ en la igualdad anterior se obtiene que $v(4, \mathbb{R}) \leq 4$.

Ahora, sea B una K-álgebra con homomorfismo $f : K \to B$. Si f es sobre y $K = \mathbb{R}$ o $K = \mathbb{C}$, por la proposición 4 parte (iv) y los teorema 23 y 24, podemos concluir que $v(d, B) \leq d$ y $w(d, B) \leq d$.

Referencias

[1] J. R. Joly, *Sommes de puissances d-iémes dans un anneau commutatif*, Acta Arithmetica, **17** (1970), 37–113.

[2] W. J. Ellison, *Waring's problem*, American Mathematical Monthly, January **(**1971), 10–36.

[3] Arne Winterhof, *On Waring's problem in finite fields*, Acta Arithmetica, **87** (1998), 171–177.

[4] Arne Winterhof & Christiaan van de Woestijne. *Exact solutions to Waring's problem for finite fields*, Acta Arithmetica, **141** (2010), 171–190.

[5] Serge Lang, *Álgebra*, Addison-Wesley, 1984.

[6] B. J. Birch, *Waring's problem for* $\mathfrak{p}$*-adic number fields*, Acta Arithmetica, **9** (1964), 169–176.

[7] C. P. Ramanujam, *Sums of m-th powers in* $\mathfrak{p}$*-adic rings*, Mathematika, **10** (1963), 137–146.

[8] Michael F. Atiyah & I. G. Mac Donald. *Introducción al álgebra conmutativa*, Reverté, 1980.

[9] Ivan Niven, Herbert S. Zuckerman & Hugh L. Mongomery. *An Introduction to the Theory of Numbers*, Wiley, 1991.

[10] J. S. Milne, *Etale Cohomology*, Princeton University Press, New Jersey, 1980.

[11] Mariemi Alonso, Henri Lombardi & Herv Perdr. *Henselian Local Rings: Around a Work in Progress.*

- Disponible en: http://drops.dagstuhl.de/volltexte/2006/437/pdf/05021.PerdryHerve.Paper.437.pdf

[12] Enrico Carlini, Maria Virginia Catalisano & Anthony V. Geramita, *The solution to Waring's Problem for Monomials*, J. of Algebra, **370** (2012), 5–14.

[13] Mats Boij, Enrico Carlini & Anthony V. Geramita, *Monomials as sums of powers: The real binary case*, American Mathematical Society, **139** (9) (2011), 3039–3043.

[14] Andrzej Bialynicki–Birula & Andrzej Schinzel, *Extreme binary forms*, Acta Arithmetica **142** (3) (2010), 219–249.