SISTEMA DE MONOMIOS PARA UN CUERPO RESIDUAL ALGEBRAICAMENTE CERRADO

Francisco Ugarte Guerra[1,2]

Noviembre, 2011

Resumen

En el presente artículo demostramos que si el cuerpo valorado es henseliano y su cuerpo residual es algebraicamente cerrado, es posible construir un sistema de monomios.

MSC(2010): 16W60.

Palabras clave: *Cuerpos valorados heselianos, cuerpo algebraicamente cerrado, sistema de monomios.*

[1] *Sección de Matemáticas, Departamento de Ciencias, PUCP.*
[2] *Becario del MAEC-AECID.*

1. Introducción

Para construir el *desarrollo en serie* de elementos de un cuerpo valorado necesitamos fijar los *monomios*, es decir, las potencias de una variable, lo cual no es posible en general. En este artículo probaremos que si el cuerpo residual del cuerpo valorado es algebraicamente cerrado, esto es posible.

2. Sistemas de Monomios

Llamaremos sistema coherente de monomios a una familia de *monomios* $\{f_\gamma\}_{\gamma\in\Gamma}$, de modo que la imagen de cada monomio, vía la valoración ν, cumpla que $\nu(f_\gamma) = \gamma$ y $f_\gamma f_{\gamma'} = f_{\gamma+\gamma'}$. Estos monomios jugaran el papel de los x^α.

Si K es un cuerpo valorado con una valoración $\nu : K \to \Gamma$ y $k_\nu \subset K$ (ver[1]) y supuesto construido un sistema de monomios $S = \{x^{\gamma_i}\}_{i\in I}$, podemos construir el subespacio vectorial de K sobre k_ν generado por S. Los elementos de este espacio son combinaciones lineales finitas $\displaystyle\sum_{i=1}^{n} c_i x^{\gamma_i}$ con coeficientes en k_ν. Este subespacio tiene estructura de álgebra sobre k_ν, su cuerpo de fracciones al que llamaremos $k_\nu(x)_S$ es un subespacio de K. Observemos ahora que formalmente dada una expresión $t = \displaystyle\sum_{i=1}^{n} c_i x^{\gamma_i}$, como Γ es totalmente ordenado podemos suponer que $\gamma_1 < \gamma_2 < \ldots < \gamma_n$ y escribir $t = c_1 x_1^{\gamma_1}\left(\displaystyle\sum_{i=1}^{n}\frac{c_i}{c_1}x^{\gamma_i-\gamma_1}\right) = c_1 x_1^{\gamma_1}\cdot t^*$.

Los exponentes de t^* son todos no negativos y la forma inicial de t^* para el sistema de exponentes es 1, $\dfrac{1}{t} = \dfrac{1}{c_1}x^{-\gamma_1}\cdot\dfrac{1}{t^*}$ y $\dfrac{1}{t^*} = \displaystyle\sum_{n\geq 0}(-1)^n(t^*-1)^n$.

Es decir, formalmente, $\dfrac{1}{t}$ es una serie reticulada generada por $1, \gamma_2 - \gamma_1, \ldots, \gamma_n - \gamma_1$. En consecuencia, los elementos de $k_\nu(x)_S$ admiten un desarrollo en serie reticulada con exponentes en el sistema S (ver [2]).

Caso de Cuerpo Residual Algebraicamente Cerrado

En lo que sigue consideraremos un cuerpo valorado completo (K, ν) con $\nu : K \to \Gamma$ y donde Γ es divisible, henseliano y de característica cero. Además el cuerpo residual de la valoración k_ν es un cuerpo algebraicamente cerrado y es un subcuerpo de K

Sea L un cuerpo algebraicamente cerrado, definimos:

$$\forall x \in L \text{ y } \forall n \in \mathbb{N} : R_n(x) = \{\alpha \in L / \alpha^n = x\}.$$

Así $R_n(1)$ denota al *conjunto de las n raíces enésimas de la unidad*, que sabemos que tiene estructura de grupo abeliano, multiplicativo y cíclico de orden n.

Lema 2.1.

1. Para cada $n \in \mathbb{N}$ y para cada $t \in R_n(x)$ existe una biyección $\varphi_t : R_n(x) \to R_n(1)$ dado por $\varphi_t(\alpha) = \frac{\alpha}{t}$.

2. Para cada u, v tal que $v|u$, existe una aplicación $\varphi_{u,v} : R_u(x) \to R_v(x)$ dada por $\varphi_{u,v}(\alpha) = \alpha^{\frac{u}{v}}$, que es sobreyectiva.

3. Si $r|n|m$, $\varphi_{n,r}\varphi_{m,n} = \varphi_{m,r}$.

4. $\forall u, v \in \mathbb{N}$ con $v|u$ y $\forall x \in L$, $\forall t \in R_u(x)$ el siguiente diagrama es conmutativo:

$$\begin{tikzcd} R_u(x) \arrow[r, "\varphi_{u,v}"] \arrow[d, "\varphi_t"] & R_v(x) \arrow[d, "\varphi_{t^{\frac{u}{v}}}"] \\ R_u(1) \arrow[r, "\varphi_{u,v}"] & R_v(1) \end{tikzcd}$$

Demostración.

1. Obvio.

2. La aplicación $\varphi_{u,v}$ está bien definida,pues $v|u$ y $\left(\alpha^{\frac{u}{v}}\right)^v = \alpha^u = x$. Veamos ahora que la aplicación es sobre. Sea $\beta \in R_v(x)$, como $v|u$, $\exists p \mid u = vp$. Luego, las p raíces p-ésimas de β que están en $R_u(x)$ son las preimágenes de β vía $\varphi_{u,v}$, es decir, $\sharp\left(\varphi_{u,v}^{-1}(\beta)\right) = p = \frac{u}{v}$. En particular $\varphi_{n,1} : R_n(x) \to R_1(x)$ es $\varphi_n(\alpha) = \alpha^n = x, \forall\alpha$.

3. Obvio porque $\left(\alpha^{\frac{m}{n}}\right)^{\frac{n}{r}} = \alpha^{\frac{m}{r}}$.

4. El diagrama conmuta, pues si $\alpha \in R_u(x)$, entonces $\varphi_t(\alpha) = \frac{\alpha}{t}$ y $\varphi_{u,v}\left(\frac{\alpha}{t}\right) = \left(\frac{\alpha}{t}\right)^{\frac{u}{v}}$.
   Por otro lado, $\varphi_{u,v}(\alpha) = \alpha^{\frac{u}{v}}$ y $\varphi_{t^{\frac{u}{v}}}\left(\alpha^{\frac{u}{v}}\right) = \dfrac{\alpha^{\frac{u}{v}}}{t^{\frac{u}{v}}} = \left(\dfrac{\alpha}{t}\right)^{\frac{u}{v}}$.
   Por lo tanto, el diagrama conmuta. □

Observemos que las aplicaciones $\varphi_{u,v}$ no dependen de t.

Proposición 2.1.

Sea L un cuerpo algebraicamente cerrado.

i. Si $n \in \mathbb{N} : n = p_1^{r_1} \cdot \ldots \cdot p_t^{r_t}$, con p_i primo y $p_i \neq p_j$ para $i \neq j$, entonces
   $\forall x \in L$, la correspondencia $\psi_n : R_n(x) \longrightarrow \prod_{i=1}^{t} R_{p_i^{r_i}}(x)$, inducida por los $\varphi_{n,p_i^{r_i}} : R_n(x) \to R_{p_i^{r_i}}(x)$ es biunívoca.

ii. Si $m|n$, $m = \prod_{i=1}^{t} p_i^{s_i}$ con $0 \leq s_i \leq r_i$, p_i primo, $p_i \neq p_j$ para $i \neq j$, entonces el siguiente diagrama es conmutativo:

$$\begin{tikzcd}
R_n(x) \arrow[r, "\psi_n"] \arrow[d, "\varphi_{n,m}"] & \prod_{i=1}^{t} R_{p_i^{r_i}(x)} \arrow[d, "\prod_{i=1}^{t} \varphi_{p_i^{r_i}, p_i^{s_i}}"] \\
R_m(x) \arrow[r, "\psi_m"] & \prod_{i=1}^{t} R_{p_i^{s_i}(x)}
\end{tikzcd}$$

Demostración.

i. Si $x = 1$ la correspondencia $\psi_n^{(1)} : R_n(1) \to \prod_{i=1}^{t} R_{p_i^{r_i}}(1)$ coincide con el isomorfismo de grupos cíclicos: $\mathbb{Z}/(n) \approx \prod_{i=1}^{t} \mathbb{Z}/(p_i^{r_i})$ con $n = \prod_{i=1}^{t} p_i^{r_i}$, $p_i \neq p_j$ para $i \neq j$ y p_i primo $\forall i$

Por otra parte, fijado un $t \in R_n(x)$, por el lema 2.1 tenemos que el siguiente diagrama es conmutativo:

$$\begin{tikzcd}
R_n(x) \arrow[r, "\varphi_n"] \arrow[d, "\psi_n"] & R_n(1) \arrow[d, "\psi_n^{(1)}"] \\
\prod_{i=1}^{t} R_{p_i^{r_i}}(x) \arrow[r, "\prod_{i=1}^{t} \varphi_{p_i^{r_i}}"] & \prod_{i=1}^{t} R_{p_i^{s_i}}(1)
\end{tikzcd}$$

Como φ_n es biunívoca, $\psi_n^{(1)}$ biunívoca y $\prod_{i=1}^{t} \varphi_{p^{r_i}}$ biunívoca, entonces ψ_n es biunívoca.

ii. Se observa directamente. Sea $\alpha \in R_n(x)$, $\psi_n(\alpha) = (\alpha^{n_1}, \ldots, \alpha^{n_t})$ con $n_i = \frac{n}{p^{r_i}}$, entonces $\prod_{i=1}^{t} \varphi_{p_i^{r_i}, p_i^{s_i}} \psi_n(\alpha) = (\alpha^{m_1}, \ldots, \alpha^{m_t})$ donde

$m_i = \frac{n}{p^{r_i}} \frac{p^{r_i}}{p^{s_i}} = \frac{n}{p^{s_i}}$. Calculemos ahora $\varphi_{n,m}(\alpha) = \alpha^{\frac{n}{m}}$, entonces $\psi_m \varphi_{n,m}(\alpha) = (\alpha^{a_1}, \ldots, \alpha^{a_n})$ con $a_i = \frac{n}{m} \frac{m}{p_i^{s_i}} = m_i$. Luego, el diagrama conmuta. $\square$

Proposición 2.2.

Si L es un cuerpo algebraicamente cerrado, entonces $\forall x \in L$, $x \neq 0 : \exists e_x : \mathbb{Q} \to L$ una aplicación inyectiva tal que:

i. Si $r = \frac{m}{n}$ con $m \in \mathbb{N}$ y $n \in \mathbb{N} - \{0\}$, entonces $e_x(r)^n = x^m$.

ii. $e_x(r+s) = e_x(r) e_x(s)$.

Demostración.

Construimos una aplicación $p_x : \mathbb{N} \to L$ de la forma siguiente: $\forall q \in \mathbb{N}$, q primo elegimos una raíz q-ésima de x, a la que llamaremos $p_x(q)$, es decir, $\forall q \in \mathbb{N}$, q primo: elegimos $p_x(q) \in R_q(x)$. Inductivamente y $\forall n \in \mathbb{N}$ construimos $p_x(q^n)$ del siguiente modo:

- $p_x(q^2)$ es una raíz q-ésima de $p_x(q)$ elegida arbitrariamente, es decir,
  $p_x(q^2) \in R_{q^2}(x)$ y la aplicación $\varphi_{q^2,q} : R_{q^2}(x) \to R_q(x)$, definida por $\varphi_{q^2,q}(\alpha) = \alpha^q$ verifica que $\varphi_{q^2,q}\left(p_x(q^2)\right) = p_x(q)$.

- Construido $p_x(q^s)$ tomamos como $p_x(q^{s+1})$ una raíz q-ésima, elegida arbitrariamente, de $p_x(q^s)$, esto es $p_x(q^{s+1}) \in R_{q^{s+1}}(x)$. Además $\varphi_{q^{s+1},q^s}\left(p_x\left(q^{s+1}\right)\right) = p_x\left(q^s\right)$.

Por 3. del lema 2.1, tenemos que $\forall r, s \in \mathbb{N} : \varphi_{q^{r+s},q^s}\left(p_x\left(q^{r+s}\right)\right) = p_x\left(q^s\right)$. Como para cada $n \in \mathbb{N}$ con $n = \prod_{i=1}^{t} p_i^{r_i}$, $R_n(x) \overset{\psi_n}{\approx} \prod_{i=1}^{t} R_{p_i^{r_i}}(x)$, existe un único elemento de $R_n(x)$ que se aplica, vía ψ_n, en la t-upla $\left(p_x\left(p_i^{r_i}\right)\right) \in \prod_{i=1}^{t} R_{p_i}^{r_i}(x)$, a dicho elemento le llamaremos $p_n(x)$.

Si $n|m$, entonces por la proposición 2.1, el siguiente diagrama es conmutativo:

$$\begin{tikzcd} R_m(x) \arrow[r, "\psi_m"] \arrow[dd, "\varphi_{m,n}"] & \prod_{i=1}^{t} R_{p_i^{r_i}(x)} \arrow[dd, "\prod_{i=1}^{t} \varphi_{p_i^{r_i},p_i^{s_i}}"] \\ & \\ R_n(x) \arrow[r, "\psi_n"] & \prod_{i=1}^{t} R_{p_i^{s_i}(x)} \end{tikzcd}$$

Luego, $\psi_n^{-1}\left(\prod_{i=1}^{t} \varphi_{p_i^{r_i},p_i^{s_i}}\right)\psi_m = \varphi_{m,n}$ y aplicando esta igualdad a $p_x(m)$:

$$\begin{aligned} \varphi_{m,n}\left(p_x(m)\right) &= p_x(m)^{\frac{m}{n}} \\ &= \psi_n^{-1}\left[\prod_{i=1}^{t} \varphi_{p_i^{r_i},p_i^{s_i}}\left(\psi_m\left(p_x(m)\right)\right)\right] \end{aligned}$$

$$\begin{aligned} \varphi_{m,n}\left(p_x(m)\right) &= \psi_n^{-1}\left[\prod_{i=1}^{t} \varphi_{p_i^{r_i},p_i^{s_i}}\left(\left(p_x(p_i^{r_i})\right)\right)\right] \\ &= \psi_n^{-1}\left[\left(p_x((p_i^{s_i}))\right)\right] \\ &= p_x(n) \end{aligned}$$

Por lo tanto, $p_x(m)^{\frac{m}{n}} = p_n(x)$.
De la igualdad anterior aplicada a $m = nt$ y n se sigue que
$\forall t \in \mathbb{N} : p_x(nt)^t = p_x(nt)^{\frac{nt}{n}} = \varphi_{m,n}\left(p_x(m)\right) = p_x(n)$ (1)
entonces
$\forall t \in \mathbb{N} : p_x(nt)^{mt} = [p_x(nt)^t]^m = p_x(n)^m$ (2)
Si $\frac{m}{n} = \frac{s}{t}$, para $m, s \in \mathbb{N}$ y $n, t \in N - \{0\}$, entonces $mt = ns$ y

$\frac{m}{n} = \frac{mt}{nt} = \frac{ns}{nt} = \frac{s}{t}$. Luego,

$$\begin{aligned} p_x(n)^m &= p_x(nt)^{mt} \text{ por } (2) \\ &= p_x(nt)^{ns} \\ &= [p_x(nt)^n]^s \\ &= p_x(t)^s \text{por } (1) \end{aligned}$$

y en consecuencia $p_x(n)^m$ depende solo de x y del número racional $\frac{m}{n}$ y no de la fracción que lo representa. Definimos la aplicación $e_x : \mathbb{Q} \to \mathbb{N}$, como $e_x\left(\dfrac{m}{n}\right) = p_x(n)^m$ y donde $m \in \mathbb{N}$ y $n \in \mathbb{N} - \{0\}$, es decir, $e_x(n) = p_x(1)^n = x^n$ y $e_x\left(\frac{1}{n}\right) = p_x(n)$, e_x es obviamente inyectiva y

$$\begin{aligned} e_x(r)^n &= \left[e_x\left(\frac{m}{n}\right)\right]^n \\ &= ([p_x(n)]^m)^n \\ &= ([p_x(n)]^n)^m \\ &= x^m \end{aligned}$$

Con lo cual queda establecida la parte i. de la proposición.
A continuación probaremos la parte ii. de la proposición. Si $r, s \in \mathbb{Q}$, podemos elegir fracciones $r = \frac{m}{t}$, $s = \frac{n}{t}$ y

$$\begin{aligned} e_x(r+s) &= e_x\left(\frac{m+n}{t}\right) \\ &= p_x\,(t)^{m+n} \\ &= p_x(t)^m p_x(t)^n \\ &= e_x(r)e_x(s) \end{aligned}$$

Usando como notación $e_x(r) = x^r$, lo que hemos hecho es elegir $\forall r \in \mathbb{Q}$ una única potencia r-ésima de x: x^r, entonces para que fórmulas como $x^r y^r = (xy)^r$ o $(x^r)^s = x^{rs}$ tengan sentido, hay que elegir de modo coordinado las aplicaciones e_y, $\forall y \in L$ para la segunda fórmula elegimos e_y, $\forall y : y = x^r$, $r \in \mathbb{Q}$.
La construcción de e_y depende de la construcción de la aplicación p_y :

$\mathbb{N} \to L$ y esta a su vez depende de la elección de la raíz p-ésima de y, esto es, de $p_y(p)$ para p primo, pero esta última elección ya vimos que es arbitraria y la elección de los $p_y(p^n)$ que está sujeta a la única condición de ser tales que $p_y(p^n)^p = p_y(p^{n-1})$.
Para dar sentido a la fórmula $(x^r)^s = x^{rs}$ construimos:

- $\forall n \in \mathbb{N}$ y $\forall m \in \mathbb{N} : p_{p_x(n)}(m) = p_x(nm)$. Esta construcción es coherente con el algoritmo de construcción de $p_{p_x(n)}$ ya que proviene de la elección $\forall q$ primo de $p_{p_x(n)}(q)$ como $p_{p_x(n)}(q) = p_x(qn)$ y $\forall q$ primo, $\forall m \in \mathbb{N}$:$p_{p_x(n)}(q^m) = p_x(q^m n)$.
- Ahora, $\forall r \in \mathbb{Q} : r = \frac{m}{n}$ definimos $p_{x^r}(t) = \left[p_{p_x(n)}(t)\right]^m$, $\forall t \in \mathbb{N}$. Esta elección proviene también de la función p_{x^r} construida para cada primo p por la misma fórmula.

De este modo se garantiza claramente que si $r = \frac{m}{n}$, $s = \frac{t}{u}$,

$$\begin{aligned}(x^r)^s &= e_{x^r}(s)\\ &= p_{x^r}(u)^t\\ &= \left[p_{p_x(n)}(u)\right]^{mt}\\ &= p_x(nu)^{mt}\\ &= x^{\frac{mt}{nu}}\\ &= x^{rs}\end{aligned}$$

El que $x^r y^r = (xy)^r$ no es claro y, en principio, dados dos elementos x, y podemos elegir x_i^r, $r \in \mathbb{Q}$ de modo que $x_i^r x_j^r = (x_i x_j)^r$, pero no podemos afirmar que se pueda hacer la misma elección en todo L.
En resumen, hemos visto que si L es un cuerpo algebraicamente cerrado y $x \in L$, se puede elegir $\forall r \in \mathbb{Q}$ (los números negativos no son problema) un elemento x^r único al que llamaremos *potencia racional principal* de modo que:

x^n coincida con la potencia enésima usual.

$\left(x^{\frac{1}{n}}\right)^n = x$

$$x^{\frac{m}{n}} = \left(x^{\frac{1}{n}}\right)^m$$

$$x^r x^s = x^{r+s}$$

$$(x^r)^s = x^{rs}$$

Proposición 2.3.

Sea K un cuerpo valorado, con una valoración $\nu : K \to \Gamma$, tal que K es de característica cero, completo respecto a ν, $k_\nu \subset K$, Γ un grupo divisible y k_ν algebraicamente cerrado,

1. $\forall x \in K$ y $\forall n \in \mathbb{N}$: x tiene n raíces enésimas diferentes.
2. Podemos elegir $\forall x \in K, x \neq 0$ y $\forall r \in \mathbb{Q} : x^r \in K$ de modo que:
   i. Si $r = \frac{m}{n}$, $(x^r)^n = x^m$
   ii. $x^r x^s = x^{r+s}$
   iii. $(x^r)^s = x^{rs}$

Demostración.

Si probamos 1., como el argumento utilizado para demostrar la existencia de x^r, en un cuerpo algebraicamente cerrado, solo usa la existencia de n raíces enésimas distintas, entonces lo podemos aplicar a K y el punto 2. queda probado. Pero 1. es consecuencia del lema de Hensel. Veamos,

i. Si $\nu(x) = 0$, entonces la ecuación $z^n - x = 0$ verifica que $z^n - \overline{x} = 0$ con $\overline{x} = x + m_\nu$, tiene n raíces simples distintas, luego por el lema de Hensel, $z^n - x = 0$ también las tiene.

ii. Si $\nu(x) \neq 0$, tomando $y \in K$ con $\nu(y) = \frac{\nu(x)}{n}$, entonces $\nu\left(\frac{x}{y^n}\right) = 0$. Luego, $\frac{x}{y^n}$ tiene n raíces distintas: $\alpha_1, \ldots, \alpha_n$ y x tiene n raíces distintas $\alpha_1 y, \ldots, \alpha_n y$, como el número de raíces es n, entonces son exactamente las raíces enésimas de x con independencia de y.

$\square$

Teorema.

Sea K un cuerpo valorado, con una valoración $\nu : K \to \Gamma$, tal que K es de característica cero, completo respecto a ν, $k_\nu \subset K$, Γ un grupo divisible y k_ν algebraicamente cerrado, podemos elegir una familia de elementos $\{x^\gamma\}_{\gamma\in\Gamma}$ tal que:

i. $\nu(x^\gamma) = \gamma$

ii. $x^\gamma x^\beta = x^{\gamma+\beta}$

iii. $\forall r \in \mathbb{Q} : (x^\gamma)^r = x^{\gamma r}$ con $(x^\gamma)^r$ la potencia r-ésima principal.

Demostración.

Como Γ es divisible, Γ tiene una estructura de $\mathbb{Q}$-espacio vectorial y eligiendo una base $\{\gamma_i\}_{i\in I}$ de Γ, tenemos que
$\forall\gamma \in \Gamma : \exists r_i \in \mathbb{Q} \mid \gamma = \sum_{i\in I} r_i\gamma_i$ con $r_i \neq 0$ si y solo si $i \in F \subset I$ finito.
Para cada i elegimos x_i de modo que $\nu(x_i) = \gamma_i$. Y $\forall\gamma \in \Gamma$: definimos $x_\gamma = \prod_{i\in I} x_i^{r_i}$. Claramente, se verifican las siguientes propiedades:

i. $\nu(x^\gamma) = \gamma$, pues $\nu(x^\gamma) = \sum_{i\in I} r_i\nu(x_i) = \sum_{i\in I} r_i\gamma_i = \gamma$.

ii. $x^\gamma x^\beta = x^{\gamma+\beta}$, pues $x^\gamma x^\beta = \prod_{i\in I} x_i^{r_i} \prod_{i\in I} x_i^{s_i} = \prod_{i\in I\cup I} x_i^{r_i+s_i} = x^{\gamma+\beta}$.

iii. $\forall r \in \mathbb{Q} : (x^\gamma)^r = x^{\gamma r}$, pues $(x^\gamma)^r = \left(\prod_{i\in I} x_i^{r_i}\right)^r = \prod_{i\in I} x_i^{r_i r} = x^{\gamma r}$.

$\square$

Referencias

[1] Rimbenboim, P.: *Teoría de las valoraciones*. Les presses de L'Université de Montréal, Montreal, Quebec, (1965).

[2] Ugarte, F.: *Álgebra de series y solución de ecuaciones algebraicas sobre cuerpos valorados*. (Phd. Thesis) Univ. Valladolid, (2010).

Abstract

In this paper we proof that if the Henselian valued field with residue field associated is algebraically closed, then the construction of monomial system will be possible.

Keywords: Henselian valued fields, algebraically closed field, monomial system.

Francisco Ugarte Guerra
Sección Matemática Departamento de Ciencias
Pontificia Universidad Católica del Perú
fugarte@pucp.edu.pe