SISTEMA DE MONOMIOS PARA UN CUERPO RESIDUAL REAL CERRADO

Francisco Ugarte Guerra[1,2]

Mayo, 2011

Resumen

Para extender técnicas tipo Polígono de Newton a ecuaciones algebraicas con coeficientes en cuerpos valorados, es necesario un desarrollo en serie de los coeficientes y para ello se requiere fijar los monomios, lo cual no siempre es posible. En este artículo probaremos que si el cuerpo valorado es henseliano y el cuerpo residual asociado a la valoración es real cerrado, la construcción del sistema de monomios es posible.

MSC(2010): 16W60.

Palabras clave: *Cuerpos valorados henselianos, cuerpo cuerpo real cerrado, sistema de monomios.*

[1] *Sección Matemáticas, Departamento de Ciencias, PUCP.*

[2] *Proyecto DGI0090-2010*

1. Introducción

Sea $f(x,y) = \sum_{i=0}^{n} f_i(x)y^i \in K[y]$ con K un cuerpo y consideremos la ecuación en y dada por $f(x,y) = 0$. Para resolver esta ecuación utilizando técnicas del polígono de Newton necesitamos alguna forma de *desarrollo en serie* de los coeficientes de la ecuación, para obtenerlo necesitamos fijar los *monomios*, es decir, las potencias de una variable. En lo que sigue probaremos que es posible seleccionar, en determinados casos, un sistema de monomios en un cuerpo valorado, es decir, vamos a probar que dado el cuerpo K y una valoración de K, $\nu : K \to \Gamma$, existe $\forall \gamma \in \Gamma$ un *monomio* f_γ de modo que $\nu(f_\gamma) = \gamma$ y $f_\gamma f_{\gamma'} = f_{\gamma+\gamma'}$. Estos monomios jugaran el papel de los x^α. Observe que si $K[[x]]_\Gamma$ es un cuerpo de series, es claro que la familia de monomios $\{x^\gamma\}_{\gamma\in\Gamma}$ cumple esta propiedad.

Si tomamos en un cuerpo valorado K un sistema coherente de monomios $\{x^\gamma\}_{\gamma\in\Gamma}$, $\forall a \in K$ con $\nu(a) = \gamma$, $\nu\left(\frac{a}{x^\gamma}\right) = 0$, entonces $a_\gamma = \frac{a}{x^\gamma} + m_\nu \in k_\nu$, $a_\gamma \neq 0$ y si $k_\nu \subset K$, $a_\gamma \in K$ y $\frac{a}{x^\gamma} - a_\gamma \in m_\nu$, implica $\nu\left(\dfrac{a - a_\gamma x^\gamma}{x^\gamma}\right) > 0$, es decir, $\nu\left(a - a_\gamma x^\gamma\right) > \gamma$. Entonces a $a_\gamma x^\gamma$ le llamaremos *forma inicial* de a respecto a ν. De este modo podemos usar los algoritmos de Newton-Puiseux (ver [2]) para ecuaciones con coeficientes en cuerpos valorados, siempre que se halla fijado un sistema coherente de monomios y siempre que K contenga al cuerpo residual.

2. Sistema de Monomios

En adelante consideraremos un cuerpo K, una valoración $\nu : K \to \Gamma$ de modo que:

i. K es de característica cero y henseliano respecto a la valoración. En particular esto se cumple si K es completo respecto a la valoración.

ii. El homomorfismo natural de ϑ_ν en k_ν admite una retracción (ver [1])

$\varphi : k_\nu \to \vartheta_\nu \hookrightarrow K$ y, en consecuencia, el cuerpo residual de la valoración k_ν se puede identificar a un subcuerpo de K.

iii. k_ν será un cuerpo real cerrado.

iv. Γ es un grupo divisible.

Recordemos la noción de *cuerpo valorado henseliano*. Para un cuerpo valorado (K, ν) y para cada elemento $a \in \vartheta_\nu$ llamaremos $\overline{a} = a + m_\nu \in k_\nu$ y dado un polinomio $p(x) \in \vartheta_\nu[x]$: $p(x) = \sum a_i x^i$, llamaremos $\overline{p}(x) = \sum \overline{a}_i x^i \in k_\nu[x]$. Con esta notación, decimos que (K, ν) es henseliano si y solo si cada ecuación algebraica $p(x) = 0$ con $p(x) \in \vartheta_\nu[x]$ tal que $\overline{p}(x) = 0$ admite una raíz simple $\alpha \in k_\nu$, admite una raíz $\beta \in \vartheta_\nu$ con $\overline{\beta} = \alpha$.

Caso de cuerpo residual real-cerrado

Decimos que L es un *cuerpo real-cerrado* si y solo si

i. Todo elemento $a \in L$ es un cuadrado, o bien el opuesto de a, $-a$ es un cuadrado.

ii. Todo polinomio de grado impar con coeficientes en L tiene al menos una raíz en L.

Un cuerpo real-cerrado es un cuerpo ordenado y, en consecuencia, de característica cero cuyo cono positivo es un conjunto de cuadrados y, en consecuencia, en él un elemento es positivo si y solo si tiene raíz cuadrada.

Lema 2.1.

Sea (K, ν) un cuerpo valorado tal que k_ν sea real cerrado,

Si $x \in \vartheta_\nu$ y $\exists y \in K \mid x = y^2$, entonces $x + m_\nu \geq 0$ en k_ν.

Recíprocamente, sea (K, ν) un cuerpo valorado henseliano tal que k_ν sea real cerrado y $\nu(x) = 0$,

$$\text{Si } x + m_\nu > 0, \text{ entonces } \exists y \in K \mid x = y^2$$

Demostración.

Si $\nu(x) \geq 0$, como $x = y^2$, $\nu(y) \geq 0$. Luego, $x + m_\nu = (y + m_\nu)^2 \geq 0$. Recíprocamente, como $x + m_\nu > 0$ y k_ν es real cerrado, entonces la ecuación $z^2 - \overline{x} = 0$ tiene una solución necesariamente simple pues k_ν es de característica cero y, como (K, ν) es henseliano, $z^2 - x = 0$ tiene una solución
$y \in \vartheta_\nu \hookrightarrow K$ con $\overline{y}^2 = \overline{x} > 0$. □

Lema 2.2.

Si (K, ν) es henseliano, k_ν es real cerrado y Γ es divisible, entonces $\forall x \in K$: o bien $\exists y \in K \mid x = y^2$ o bien $\exists y \in K \mid -x = y^2$ y si $x \neq 0$ solo sucede uno de los dos casos.

Demostración.

Si $x \neq 0$, existen dos posibilidades:

i. $\nu(x) = 0$, en este caso, como k_ν es totalmente ordenado y $x + m_\nu \neq 0$, entonces $x + m_\nu > 0$ o $-x + m_\nu > 0$ y, aplicando el lema 2.1 hemos terminado.

ii. $\nu(x) \neq 0$, en este caso elegimos $x_0 \in K$ de modo que $\nu(x_0) = \frac{\nu(x)}{2}$, esto es posible pues Γ es divisible y ν es sobre. Además $x_0 \neq 0$ y como K es cuerpo, existe $\frac{1}{x_0}$ y $\nu\left(\dfrac{x}{{x_0}^2}\right) = 0$, entonces aplicando la parte i.: o bien $\exists y \mid \dfrac{x}{x_0^2} = y^2$ lo que implica que $x = (x_0 y)^2$, o bien $\exists y \mid \dfrac{-x}{x_0^2} = y^2$ lo que implica que $-x = (x_0 y)^2$, en cualquier caso hemos terminado.

Si $x = 0$, no puede darse que $x = z^2$ y $-x = z^2$ porque en el caso de que $\nu(x) = 0$, tendríamos que $x + m_\nu \geq 0$ y que $x + m_\nu \leq 0$, con lo cual $x \in m_\nu$ lo que es un contradicción. Si $\nu(x) \neq 0$, empleamos el mismo argumento dividiendo a x por un elemento de K que tenga la mitad de su valor. □

Lema 2.3.

Si (K, ν) es henseliano y k_ν es real cerrado,

$$\forall y, z \in K : \exists u \in K \mid y^2 + z^2 = u^2$$

Demostración.

Podemos suponer sin pérdida de generalidad que $\nu(y) \leq \nu(z)$, entonces
$2\nu(y) \leq 2\nu(z)$, es decir, $\nu(y^2) \leq \nu(z^2)$ o, lo que es lo mismo, $\nu\left(\frac{z^2}{y^2}\right) \geq 0$ y en consecuencia $\frac{z^2}{y^2}\vartheta_\nu$, $\frac{z^2}{y^2} + m_\nu \geq 0$, luego $1 + \frac{z^2}{y^2} + m_\nu = \frac{y^2 + z^2}{y^2} + m_\nu > 0$, es decir, $\nu\left(\frac{y^2 + z^2}{y^2}\right) = 0$ y, aplicando el lema 2.1, existe $u \in K$ tal que $y^2 + z^2 = (uy)^2$. □

Proposición 2.1.

Sean $\nu : K \to \Gamma$ una valoración, K un cuerpo henseliano, Γ un grupo divisible, k_ν un cuerpo ordenado. Si $\forall x \in k_\nu : x \geq 0$ se cumple que $\exists y \in k_\nu \mid x = y^2$, entonces

i. K es un cuerpo ordenado.

ii. $\forall x \in K : x \geq 0$ si y solo si $\exists y \in K \mid x = y^2$.

Demostración.

Probaremos que el subconjunto $P \subset K$ definido por $P = \{x \in K \mid \exists y \in K,$
$x = y^2\}$ es un cono positivo para un orden en K, es decir, se cumplen las siguientes propiedades:

i. $P \cup -P = K$

ii. $P \cap -P = \{0\}$

iii. $P + P \subset P$

iv. $P \cdot P \subset P$

lo que equivale a decir que $(K, \leq)$ es un cuerpo totalmente ordenado. Veamos:
Las condiciones i. y ii. se cumplen trivialmente por el lema 2.2.

La condición iii. es consecuencia directa del lema 2. Por lo tanto, $(K, \leq)$ es un grupo totalmente ordenado. Más todavía $(K, \leq)$ es un cuerpo totalmente ordenado y se cumple iv. pues del lema 2.1 se tiene que $\forall a, b \in P : a \geq 0$ y $b \geq 0$ implica que $ab \in P$. □

Proposición 2.2.

Sea K un cuerpo de característica cero, completo y $\nu : K \to \Gamma$ una valoración tal que $k_\nu \subset K$ y con Γ un grupo divisible.
Si k_ν es un cuerpo ordenado y $\forall a \in k_\nu, a > 0$ y $\forall n \in \mathbb{N} : \exists b_n \in k_\nu, b_n > 0$ tal que $a = b_n^n$, entonces

i. K es un cuerpo ordenado y

ii. $\forall x \in K : x > 0$ y $\forall n \in \mathbb{N} : \exists y_n \in k_\nu$ único, $y_n > 0$ tal que $x = y_n^n$.

Demostración.

De la hipótesis para $n = 2$ y de la proposición 2.1se sigue que K es un cuerpo ordenado (ver proposición 2.1) y que $\forall x \in K : \nu(x) = 0$ $x \geq 0$ si y solo si $x + m_\nu \geq 0$.
Sea $x \in K : x > 0$, pueden ocurrir dos cosas:

i. $\nu(x) = 0$, $x \in \vartheta_\nu$ y $\overline{x} = x + m_\nu \neq 0$, entonces $x > 0$, implica que $\overline{x} > 0$ y, por hipótesis, dado n existe $y_n \in k_\nu$, $y_n > 0$ y $y_n^n = x$. Entonces la ecuación $z^n - x = 0$ verifica que

- $z^n - x \in \vartheta_\nu[z]$
- $z^n - \overline{x} = 0$ tiene la solución y_n,

entonces existe un $y \in \vartheta_\nu$ con $z^n = y$ e $\overline{y} = y_n$ y por la observación $y_n > 0$ implica $y > 0$.

ii. $\nu(x) \neq 0$. En este caso elegimos $x_0 \in K$ tal que $x_0 > 0$ y con $\nu(x_0) = \frac{\nu(x)}{n}$, esto siempre es posible, pues Γ es divisible, ν es sobre y $\nu(x_0) = \nu(-x_0)$. Luego, $\nu\left(\frac{x}{x_0^n}\right) = 0$ y aplicando la parte i. a $\frac{x}{x_0^n} > 0$, $\exists y \in K, y \mid \frac{x}{x_0^n} = y^n$, es decir, $x = (x_0 y)^n$ y como $x_0 > 0$, $y > 0$ implica que $x_0 y > 0$, hemos terminado.

Para probar la unicidad de y supongamos que existen z, y tales que $z > 0$, $y > 0$ y $x = z^n = y^n$. Entonces

$$y^n - z^n = (y - z)(y^{n-1} + y^{n-2}z + \ldots + yz^{n-2} + z^{n-1}) = 0$$

pero $y^{n-1}, y^{n-2}, \ldots, y$ son todos mayores que cero y $z, z^2, \ldots, z^{n-1}$ también y como K es un dominio, entonces $y = z$. □

Sea $x \in K$, $x > 0$. Para $m \in \mathbb{Z}$ y $n \in \mathbb{Z} - \{0\}$, denotaremos por $x^{\frac{m}{n}}$ al único elemento $y \in K$ tal que $y^n = x^m$,

$$y = x^{\frac{m}{n}} \Leftrightarrow y^n = x^m$$

El siguiente corolario de la proposición 2.2 prueba que $x^{\frac{m}{n}}$ depende solo del número racional $\frac{m}{n}$ y no del representante elegido.

Corolario 2.1.

Con las mismas hipótesis de la proposición 2.2, se tiene que $\forall x \in K : x > 0$ y $\forall r \in \mathbb{Q} : r = \frac{m}{n} = \frac{p}{q}$, entonces $x^{\frac{m}{n}} = x^{\frac{p}{q}}$.
Notación: $x^r = x^{\frac{m}{n}}$ $\forall m \in \mathbb{Z}, n \in \mathbb{Z} - \{0\} : \frac{m}{n} = r$.

El siguiente corolario extiende la proposición 2.2 a exponentes racionales.

Corolario 2.2.

Con las mismas hipótesis de la proposición 2.2 se tiene que $\forall x \in K : x > 0$ y $\forall r \in \mathbb{Q} : \exists y_r \in K$ único $, y_r > 0 \mid x = y_r^r$ con y_r único.

Demostración.

Sea $r = \frac{n}{m}$, $n, m \in \mathbb{Z}$ y $m \neq 0$, entonces como $x > 0$, $x^m > 0$ y, por la proposición 2.2 $\forall n \in \mathbb{N} : \exists y_n$ único $\in k_\nu, y_n > 0 \mid x^m = y_n^n$, es decir, $y_n = x^{\frac{m}{n}}$. □

Proposición 2.3.

Si $r, s \in \mathbb{Q}$, se cumple que

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

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

Demostración.

i. Si $r = \frac{m}{n}$, $s = \frac{p}{q}$ podemos reducir a común denominador y tener $r = \frac{a}{d}$, $s = \frac{b}{d}$, $r + s = \frac{a+b}{d}$, entonces $x^{r+s} = x^{\frac{a+b}{d}} = z \Leftrightarrow x^{a+b} = z^d, z > 0$.
$x^r = y \Leftrightarrow x^a = y^d, y > 0$
$x^s = t \Leftrightarrow x^b = t^d, t > 0$
entonces
$x^a \cdot x^b = x^{a+b} = y^d t^d = (y \cdot t)^d$, entonces $(yt) = z$, es decir, $x^{r+s} = x^r x^s$.

ii. Si $s \in \mathbb{Z} : (x^r)^m = x^{mr}$, consecuencia de i.
Si $s \in \mathbb{Q} : s = \frac{p}{q}$, $r = \frac{m}{n}$,

$$\begin{aligned}(x^r)^s = z &\Leftrightarrow z > 0 \text{ y } (x^r)^p = z^q \\ &\Leftrightarrow z > 0, x^{pr} = z^q, pr = \frac{pm}{n} \\ &\Leftrightarrow z > 0, x^{pm} = (z^q)^n = z^{qn} \\ &\Leftrightarrow x^{\frac{pm}{qn}} = z \\ &\Leftrightarrow x^{rs} = z = (x^r)^s\end{aligned}$$

Del corolario 2.2 se tiene directamente la siguiente consecuencia.

Consecuencia 2.1.

$\forall x \in K : x > 0, \forall r \in \mathbb{Q} : \exists y \in K$ único $, y > 0$ tal que $x = y^r$. Finalmente, enunciamos el resultado buscado.

Teorema.

Si (K, ν) es un cuerpo valorado henseliano tal que k_ν sea real cerrado y Γ divisible, podemos construir una familia de elementos x^γ, $\forall \gamma \in \Gamma$ tal que

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

ii. $x^\gamma > 0$

iii. $x^\gamma x^\mu = x^{\gamma+\mu}, \forall \gamma, \mu \in \Gamma$

iv. $(x^\gamma)^r = x^{r\gamma}, \forall r \in \mathbb{Q}, \forall \gamma \in \Gamma$

Demostración.

Como Γ es divisible, es un $\mathbb{Q}$-espacio vectorial, tomamos una base $\{\gamma_i\}_{i\in I}$ de Γ como $\mathbb{Q}$- espacio vectorial, entonces $\forall \gamma \in \Gamma : \exists F_\gamma \subset I$ finito y $\{a_i\}_{i\in I} \subset \mathbb{Q}$ con $\gamma = \sum_{i\in I} a_i\gamma_i$ con $a_i \neq 0$ si y solo si $i \in F_\gamma$. Construimos $\forall i \in I : x_i > 0$ con $\nu(x_i) = \gamma_i$ y definimos $x^\gamma = \prod_{i\in I} x_i^{a_i} = \prod_{i\in F_\gamma} x_i^{a_i}$.

i. Por la proposición anterior $\nu(x^\gamma) = \sum_{i\in I} a_i\nu(x_i) = \sum_{i\in I} a_i\gamma_i = \gamma$.

ii. Es consecuencia de la elección de los x_i.

iii. $x^\gamma \cdot x^\mu = \prod_{i\in I} x_i^{a_i} \cdot \prod_{i\in I} x_i^{b_i} = \prod_{i\in I} x_i^{a_i+b_i} = x^{\gamma+\mu}$.

iv. Consecuencia de iii.

□

Llamaremos un *sistema coherente de monomios* en K a una familia $\{x^\gamma\}_{\gamma\in\Gamma}$ que cumple las propiedades del teorema.

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

To extend a Newton polygon techniques to algebraic equations with coefficients in valued field, first it is necessary to obtain a series expansion coefficients, that requires to fix a monomial set, which it is not always possible. In this paper we proof that if the Henselian valued fields with residue fields associated is real closed, then the construction of monomial system will be possible.

Keywords: Henselian valued fields, real closed field, monomial systems.

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