Boletín de Matemáticas
Vol. VI No. 25-32

ESTRUCTURAS ORDENADAS, III

VICTOR S. ALBIS

6. *Anillos Euclideanos y de valuación. Sus relaciones con los factoriales.*

Hemos visto que si A es un dominio factorial, entonces su grupo de divisibilidad $D = K^*/U$ es un grupo reticulado ([1], proposición 5.5). Es pues pertinente identificar los dominios cuyos grupos de divisibilidad gozan de otras propiedades de orden. Uno de los casos más importantes está contenido en la siguiente definición :

Definición 6.1. Un dominio A se dice un *anillo de valuación* si su grupo de divisibilidad D está totalmente ordenado.

La siguiente proposición caracteriza estos dominios.

Demostración 6.1. *Sean A un dominio y K su cuerpo de fracciones. Entonces A es un anillo de valuación cuando, y sólo cuando, para todo $x \in K$ se tiene que $x \notin A \Rightarrow x^{-1} \in A$.*

Demostración: $(\Rightarrow)$ Si D está totalmente ordenado, debemos tener para todo $x \notin A \cap U$ que $U \mid \bar{x}$ ó $\bar{x} \mid U$. La primera posibilidad no la tenemos, pues de lo contrario x pertenecería a A. La segunda equivale a $x \mid 1$, es decir, $x^{-1} \in A$.

$(\Leftarrow)$ Sean $x, y \in K^*$, $\bar{x} \neq \bar{y}$, de modo que $x \nmid y$ ó $y \nmid x$, Pero si $yx^{-1} \notin A$, entonces $xy^{-1} \in A$, por hipótesis; luego $y \mid x$, y así $\bar{y} \mid \bar{x}$. ∎

Ejemplos. 1. Sea $p \in \mathbb{Z}$ un número primo positivo. El anillo

$$A_p = \{ a/b \in \mathbb{Q} \; ; \; (b, p) = 1 \}$$

es un dominio de integridad con elemento unidad. Su cuerpo de fracciones es $\mathbb{Q}$. Veamos que A_p es un anillo de valuación: sea $x = a/b$ tal que $a/b \notin A_p$; entonces $p \mid b$, y como $(a,b) = 1$, tenemos que $p \nmid a$; luego $b/a = x^{-1} \in A$. Observemos que $U = \{ a/b \in A_p ; (a,p) = (b,p) = 1 \}$. Como todo elemento a/b de $\mathbb{Q}$ puede escribirse de manera única, en la forma

$$\frac{a}{b} = p^n . z \quad , \quad \text{donde} \quad n \in \mathbb{Z}, \; z \in U ,$$

es fácil verificar que $\mathbb{Q}^* / U \simeq \mathbb{Z}$ (usando: $a/b \mapsto n$ el cual es un homomorfismo de $\mathbb{Q}^*$ sobre $\mathbb{Z}$).

2. Sea k un cuerpo conmutativo. Consideremos el anillo $A = k[[T]]$ cuyos elementos son todas las *series potenciales formales*

$$x = x_o + x_1 T + x_2 T^2 + \ldots + x_n T^n + \ldots$$

en la indeterminada T, con coeficientes en k (i.e., cada $x_i \in k$). Su cuerpo de fracciones $K = k((T))$ está formado por todas las *series meromorfas*

formales

(6.1) . $x = x_{-n} T^{-n} + \ldots + x_{-1} T^{-1} + x_o + x_1 T + \ldots + x_m T^m + \ldots$,

$x_{-n} \neq 0$,

en la indeterminada T con coeficientes en k. Supongamos que x esté dada por (6.1) y que $x \notin A$; entonces

$$T^n x = x_{-n} + \ldots + x_{-1} T^{n-1} + x_o T^n + x_1 T^{n+1} + \ldots + x_m T^{n+m} + \ldots$$

$$= x_{-n} (1 + y) ,$$

donde $y \in A$ y no tiene término constante. De aquí resulta

$$x^{-1} = T^n x_{-n}^{-1} \left(\frac{1}{1+y}\right) = x_{-n}^{-1} T^n (1 - y + y^2 - \ldots + (-1)^i y^i + \ldots)$$

(usando el conocido desarrollo de una serie geométrica), y como claramente el miembro derecho de la anterior igualdad pertenece a $A = k [[T]]$, resulta que $x^{-1} \in A$. Luego A es de valuación. Un raciocinio análogo al anterior muestra que $U = \{ x = x_o + x_1 T + \ldots + x_n T^n + \ldots \in A : x_o \neq 0 \}$. Es fácil compro - bar entonces que todo $x \in K$ se escribe de manera única en la forma $x = T^n . u$, donde $n \in U$, y, como en el ejemplo anterior, que $K^* / U \approx \mathbb{Z}$.

Volvamos nuevamente a un anillo de valuación arbitrario, con cuerpo de fracciones K. Como D está totalmente ordenado, dados $x, y \in K^*$, tenemos, verbigracia, que $\bar{x} \mid \bar{y}$; es decir $y = xq$, con $q \in A^*$. De aquí resulta que $x + y = x(1 + q)$, o equivalentemente, que $\bar{x} \mid \overline{x + y}$. Puesto de otra manera ,

$$min\,(v(x)\,,\ v(y)\,)\ |\ v(x+y)$$

donde $v\,;\ K^{*} \longrightarrow D$ designa el epimorfismo canónico. Hemos, pues, demostrado la

Proposición 6.2. *Sean A un anillo de valuación, K su cuerpo de fracciones. Entonces el epimorfismo canónico $v\colon K^{*} \longrightarrow D = K^{*}/U$ goza de las propiedades siguientes :*

i) $v(xy) = v(x)\,v(y)$

ii) $min\,(v(x),\ v(y)\,)\ |\ v(x+y)$. ∎

Definición 6.2. Sea D un grupo abeliano totalmente ordenado (escrito multiplicativamente y con $|$ como la relación de orden) y sea K un cuerpo. Una *valuación de K con valores en D* es una aplicación $v\colon K^{*} \longrightarrow D$ que satisface las propiedades i) y ii) de la proposición 6.2.

Para completar el cuadro, demostramos en seguida que una valuación de K con valores en un grupo abeliano totalmente ordenado define canónicamente un anillo de valuación, cuyo cuerpo de fracciones es precisamente K.

Proposición 6.3 *Sea $v\colon K^{*} \longrightarrow D$ una valuación de K. Entonces*

a) $A_v = \{\, x \in K^{*};\ \overline{1}\ |\ v(x)\,\}$ *es un anillo de valuación de K*

b) $v(K^{*})$ *es el grupo de divisibilidad de* A_v .

Demostración. Usando i) y ii) es fácil ver que A_v es un dominio. Ahora bien, si $x \in K^{*}$ y $x \notin A_v$, entonces $v(x)\ |\ \overline{1}$, de donde $v(x)v(x^{-1}) = \overline{1}\,|v(x^{-1})$ i.e., $x^{-1} \in A_v$, lo cual muestra que K es el cuerpo de fracciones de A_v y que éste es de valuación. Finalmente, como $x\,|y \ mod\ A_v$ cuando y solo cuan-

do $\bar{I} \mid v(x^{-1}y)$, tenemos que $U = \{ x \in A^* ; v(x) = \bar{I} \}$, y por tanto, $K^*/U \approx v(K^*)$ por el teorema de isomorfismo. ∎

La teoría de valuaciones (o lo que es lo mismo, de los anillos de valuación) juega un papel importantísimo en la moderna teoría de números y funciones algebraicas. (Véase, e.g., [3] y [4]).

Definición 6.3. Conservando las notaciones anteriores, si $D \approx \mathbb{Z}$ decimos que el dominio A es un *anillo de valuación discreta*.

Los anillos de los ejemplos son de valuación discreta.

Proposición 6.4. *Un anillo de valuación discreta es factorial.*

Demostración. Resulta de las propias definiciones.

Otra clase de anillos que son también factoriales está formada por los llamados anillos euclideanos. Seguimos ahora los pasos de P. Samuel en su hermoso trabajo sobre anillos euclideanos [6].

Definición 6.4. (Samuel-Motzkin). Dado un dominio A, un *algoritmo euclideano en* A es una aplicación φ de A en un conjunto bien ordenado W tal que

(E) dados $a, b \in A$, $b \neq 0$, existen q y r en A tales que

$$a = bq + r \quad \text{y} \quad \varphi(r) < \varphi(b).$$

Decimos entonces que A es *euclideano* si admite un tal algoritmo y, para mayor precisión, decimos además que A es *euclideano para* φ.

El interés de los anillos euclideanos reside en su propiedad de ser *principales*,

es decir, cada uno de sus ideales es generado por solo un elemento. Y por tanto, sus aritméticas son más sencillas. Usando entonces que *todo anillo principal es factorial* ([2] pág. 46), deducimos que *todo anillo euclideano es factorial*. Demostramos, pues, la

Proposición 6.5. *Sea A un anillo euclideano con algoritmo φ. Entonces*

a) Para $b \in A^*$ tenemos $\varphi(b) > \varphi(0)$, de modo que $\varphi(0)$ es el menor elemento de $\varphi(A)$.

b) Un elemento $b \in A$ tal que $\varphi(b)$ es el menor elemento de $\varphi(A) - \{\varphi(0)\}$ es una unidad de A.

c) A es principal.

Demostración. a) Usando (E), escribamos $0 = bq + b_1$ con $\varphi(b_1) < \varphi(b)$ Recurrentemente definamos una sucesión $b, b_1, \ldots, b_n$ de elementos de A usando la siguiente regla : si $b_n = 0$ nos detenemos, si $b_n \neq 0$ escribimos $0 = b_n q + b_{n+1}$ con $\varphi(b_{n+1}) < \varphi(b_n)$. Como $(\varphi(b_n))$ es una sucesión decreciente de elementos de un conjunto bien ordenado, debe ser finita [5]. Existe pues un $n \geq 1$ tal que $b_n = 0$ y así $\varphi(0) = \varphi(b_n) < \varphi(b)$.

b) Por hipótesis, tenemos $b \neq 0$. Para cualquier a en A, tenemos $a = bq + r$, con $\varphi(r) < \varphi(b)$, de donde $r = 0$. Consecuentemente $A = Ab$ y b es una unidad.

c) Sea $\mathcal{U}$ un ideal de A. Podemos suponer que $\mathcal{U} \neq (0)$. Tomando, entre los elementos no nulos de $\mathcal{U}$, un elemento b con el menor valor para φ, tenemos que para cualquier $a \in \mathcal{U}$, $a = bq + r$, con $\varphi(r) < \varphi(b)$.

Como $r = a - bq \in \mathcal{A}$, necesariamente $r = 0$, de donde $\mathcal{A} = Ab$. ∎

La siguiente proposición relaciona los anillos de valuación con los anillos euclideanos.

Proposición 6.6 *Un anillo de valuación discreta A es euclideano si definimos $\varphi(x) = 1 + v(x)$ para $x \neq 0$, donde v es la valuación asociada con A ($v(x) \in \mathbb{Z}$, para todo $x \neq 0$).*

Demostración. Como ahora $v(x) \geq v(y)$ si y solo si $y \mid x$, tenemos que $v(r) \geq v(b)$ para todo r tal que $a = r + bq$ (para algún q), implica que $b \mid r$ y por tanto $b \mid a$, pudiendo tomar $r = 0$. Luego si $b \nmid a$, la euclideanidad resulta inmediatamente. ∎

Resummendo, tenemos la siguiente cadena de implicaciones : valuación discreta => euclideano => principal => factorial.

Referencias

[1] V. S. Albis González, "Estructuras ordenadas, II," Bol. Mat. (Bogotá), 3 (1969), 1-15.

[2] J. Barshay, *Topics in ring theory*, Benjamin, New York, 1969.

[3] Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, New York, 1966.

[4] P.J. McCarthy, *Algebraic extensions of fields*, Blaisdell Pub. Co., Waltham, 1966.

[5] G. H. Meisters, "El teorema del punto fijo de Zermelo en los conjuntos parcialmente ordenados y los principios transfinitos de existencia," Bol. Mat. (Bogotá), 6, 4 (1972), 1-9.

[6] P. Samuel, "About euclidean rings" (próximo a aparecer en J. of Algebra).

* * *

Gottfried Willhelm Leibniz

(1646 - 1716)

Se destacó igualmente en filosofía y en matemáticas. Además fue abogado, diplomático, teólogo, historiador, geólogo, economista, bibliotecario y linguista.

Durante casi toda su vida estuvo al servicio de la nobleza germana. Fundó la Academia de Ciencias de Berlín y publicó una de las primeras revistas científicas.

Desarrolló el cálculo un poco más tarde que Newton, pero trabajando independientemente de él. Además Leibniz fue un precursor de la lógica matemática, dio la definición de determinante y diseñó una computadora, notándose desde entonces la relación existente entre dos campos aparentemente disímiles : la lógica formal y el cálculo algorítmico.