

ESTRUCTURAS ORDENADAS II

por

Víctor S. ALBIS GONZALEZ

§ 3. ALGUNAS PROPIEDADES DE LOS MONOIDES Y GRUPOS ORDENADOS.

Consideremos el monoide de los números naturales (respecto de la multiplicación) y la relación de divisibilidad. El elemento neutro de este monoide es el número 1, y decir que d es el máximo común divisor de a y b es lo mismo que decir que $d = \inf(a, b)$ para este orden. Decimos también que a y b son primos entre sí si y solo si

$$(3 (1)) \quad d = \inf(a, b) = 1,$$

o lo que es lo mismo

$$(3 (2)) \quad x | a, x | b \Rightarrow x = 1.$$

Consideremos ahora un monoide preordenado cualquiera, notado aditivamente y con elemento neutro 0. Estamos tentados de decir que a y b son primos entre sí, si

$$(3 (3)) \quad \begin{array}{l} \text{i) } 0 \leq a, b \\ \text{ii) } 0 \leq x \leq a, b \Rightarrow x = 0, \end{array}$$

como en (2), y que, además estas condiciones "son" equivalentes a

$$(3 (4)) \quad \text{existe } \inf(a, b) = 0 \text{ único}$$

Sin embargo, P. JAFFARD [4] ha mostrado la existencia de un monoide pre-ordenado en el cual dos elementos satisfacen (3) pero no (4). Esto es de esperar, pues i) y ii) pueden satisfacerse sin que exista $\inf(a, b)$. En consecuencia, ponemos

la siguiente definición :

DEFINICION 3.1. Dos elementos a, b de un monoide preordenado G se dirán **extraños** si y solo si $0 = \inf(a, b)$, único. Se llamarán **primos entre sí**, si y solo si

$$i) \quad 0 \leq a, b$$

$$ii) \quad 0 \leq x \leq a, b \Rightarrow x = 0.$$

PROPOSICION 3.1. Sea G un monoide preordenado. Si $a, b \in G$ son extraños, entonces a y b son primos entre sí.

Demostración. De la relación $0 = \inf(a, b) \leq x \leq a, b$, concluimos $0 \leq x$; luego $x \in \bar{0}$, pues x es una cota inferior de $\{a, b\}$. Como $\inf(a, b)$ es único, resulta que $x = \inf(a, b) = 0$. ■

Sin embargo,

PROPOSICION 3.2. Sea G un grupo pre-reticulado. Entonces a y b son primos entre sí si y solo si a y b son extraños.

Demostración. Sea $\bar{x} = \inf(\bar{a}, \bar{b}) \geq \bar{0}$. Entonces para todo $x \in \bar{x}$, $0 \leq x \leq a, b \Rightarrow x = 0$ (por hipótesis a y b son primos entre sí); luego, $\bar{x} = \{0\}$. Recíprocamente, si c es una cota inferior de $\{a, b\}$ (la cual existe pues G es pre-reticulado), tenemos $\bar{c} \leq \bar{a}, \bar{b}$, y, por lo tanto, $\bar{c} \leq \bar{x} = \inf(\bar{a}, \bar{b})$; por consiguiente, $c \leq x = 0$, es decir, $0 = \inf(a, b)$. ■

TEOREMA 3.1 (GAUSS). Sea G un grupo pre-ordenado. Si $c \in G$ es tal que $\inf(a, c) = \inf(b, c) = 0$, entonces $\inf(b + a, c) = 0$.

Demostración. Como $\inf(a, c) = \inf(b, c) = 0$, tenemos $0 \leq a, 0 \leq b$; en consecuencia, $0 \leq b + a$; luego 0 es una cota inferior de $\{a + b, c\}$. Sea ahora $0 \leq x \leq b + a, c$; como $0 \leq a$, tenemos $x \leq a + b, a + c$; de aquí resulta que $x - a \leq b, c$; y como $\inf(b, c) = 0$, tenemos $x - a \leq 0$. Ahora bien, de $x \leq a, c$, resulta $x \leq 0$ ya que $\inf(a, c) = 0$. Por lo tanto, $0 = \inf(a + b, c)$. ■

TEOREMA 3.2 (Lema de EUCLIDES). Sea G un grupo pre-ordenado; sean $a, b, c \in G_+$ tales que $\inf(a, c) = 0$, $c \leq a + b$. Entonces $c \leq b$.

Demostración. En efecto, $c \cdot b \leq a$, c implica $c \cdot b \leq 0$ porque $0 = \inf(a, c)$. ■

Los dos teoremas anteriores son generalizaciones de hechos harto conocidos en el caso del monoide multiplicativo \mathbf{N} y la relación de divisibilidad :

a) Si $(a, c) = (b, c) = 1$ entonces $(ba, c) = 1$.

b) Si $a, b, c \in \mathbf{N}$, $(a, c) = 1$, $c | ab$, entonces $c | b$. (cfr. [5], pág. 5).

Por otra parte, la idea de número natural primo se generaliza así :

DEFINICION 3.2. Sea G un grupo ordenado ; $p \in G$ se dice *minimal* si

- (3.5) i) $0 < p$;
 ii) $0 < x \leq p$ ($x \in G$) $\Rightarrow x = p$.

PROPOSICION 3.3. Sea G un grupo reticulado; si $p, q \in G$, $p \neq q$, son minimales, entonces

a) p y q son extraños.

b) mp y nq son extraños, para todo $m, n \in \mathbf{Z}$.

Demostración. En efecto, como G es un grupo reticulado, existe $a = \inf(p, q) > 0$; si $a \neq 0$, entonces $0 < a \leq p, q \Rightarrow a = p, q$ (porque p y q son minimales), lo cual contradice la hipótesis $p \neq q$. Luego $\inf(p, q) = 0$, i.e., p y q son extraños. Esto demuestra a). Por otra parte, $\inf(p, q) = 0$ implica

$$\inf(p, 2q) = \dots = \inf(p, nq) = 0$$

por aplicación recurrente del teorema 3.1 ; en la misma forma, $\inf(p, nq)$ implica

$$0 = \inf(2p, nq) = \dots = \inf(mp, nq) = 0 \quad \blacksquare$$

PROPOSICION 3.4. Sea G un grupo reticulado; $x \in G$ se puede representar de una y solo una manera en la forma

$$x = a_1 p_1 + \dots + a_n p_n$$

donde los p_i son elementos minimales distintos y los a_i son números enteros.

Demostración. Supongamos que tenemos una igualdad de la forma

$$(3.6) \quad \alpha_1 p_1 + \dots + \alpha_n p_n = \beta_1 p_1 + \dots + \beta_n p_n.$$

Podemos siempre suponer que $0 \leq \alpha_i, \beta_i$ ($i = 1, \dots, n$), trasponiendo, si es el caso, los sumandos $\alpha_i p_i, \beta_i p_i$. Supongamos ahora que $\alpha_1 > \beta_1$; entonces

$$(\alpha_1 - \beta_1) p_1 + \alpha_2 p_2 + \dots + \alpha_n p_n = \beta_2 p_2 + \dots + \beta_n p_n.$$

El segundo miembro es extraño para p_1 (teorema 3.1, proposición 3.3); luego el primer miembro es extraño para p_1 . Sea $a = \alpha_2 p_2 + \dots + \alpha_n p_n$, y supongamos $\alpha_1 \neq \beta_1$; entonces $p_1 \leq (\alpha_1 - \beta_1) p_1 + a$, por consiguiente, $\inf(p_1, (\alpha_1 - \beta_1) p_1 + a) = p_1 = 0$, contradicción. Luego $\alpha_1 = \beta_1$. El mismo raciocinio se hace para cada par (α_i, β_i) , completando así la demostración. ■

PROPOSICION 3.5. Sea G un grupo ordenado; sean A, B dos partes de G extremadas superiormente (resp. inferiormente); entonces $A + B$ también está extremada superiormente (resp. inferiormente) y

$$(3.7) \quad \sup(A + B) = \sup A + \sup B$$

(resp.,

$$\inf(A + B) = \inf A + \inf B).$$

Demostración. En efecto, sean $a = \sup A$ y $b = \sup B$; entonces $\sup A + \sup B$ es una cota superior de $A + B$. Sea ahora x una cota superior de $A + B$; entonces $x \geq c + d$ para todo $c \in A$ y todo $d \in B$; por consiguiente, $x - c \geq d$, es decir, $x - c \geq b = \sup B$, para todo $c \in A$; luego $x \geq \sup B + \sup A$. La otra relación se demuestra semejantemente. ■

COROLARIO 1. Sea G un grupo ordenado. Si $\sup(a, b)$ (resp. $\inf(a, b)$) existe para $a, b \in G$, entonces

$$(3.8) \quad \sup(a+x, b+x) = \sup(a, b) + x$$

(resp., $\inf(a+x, b+x) = \inf(a, b) + x$).

Demostración. En la proposición tómesese $A = \{a, b\}$, $B = \{x\}$. ■

COROLARIO 2. Sea G un grupo ordenado. Entonces G es reticulado $\Leftrightarrow G$ es un retículo.

Demostración. Resulta de las definiciones y el corolario anterior.

TEOREMA 3.3. En un grupo ordenado G se tienen las siguientes igualdades en la medida que tengan sentido:

$$(3.9) \quad \inf(a, b) = -\sup(-a, -b)$$

$$(3.10) \quad \sup(a, b) + \inf(a, b) = a + b$$

Si el primer miembro de (9) existe, también existe el segundo. Si existe $\sup(a, b)$, también existe $\inf(a, b)$, y recíprocamente.

Demostración. Demostramos (3.9): sea $x = \inf(a, b)$; entonces $x \leq a, b$, i.e., $-a, -b \leq -x$, es decir, $-x$ es una cota superior de $\{-a, -b\}$. Sea ahora z una cota superior de $\{-a, -b\}$, y supongamos que $z < -x$; esto implica que $x < -z < a, b$, es decir, $x \neq \inf(a, b)$; luego $-x = -\inf(a, b) = \sup(-a, -b)$. Demostramos (3.10): $-b + \sup(a, b) - a = \sup(a - b, 0) - a = \sup(-b, -a) = -\inf(a, b)$, donde hemos usado (3.9) y el corolario 1 de la proposición 3.5.

PROPOSICION 3.6. Sea G un grupo pre-ordenado. Entonces G es prefiltrante $\Leftrightarrow G$ está engendrado por el conjunto de sus elementos positivos.

Demostración. (\Rightarrow). Sean G prefiltrante y $x \in G$; entonces existe $a \in G$ tal que $a \geq x, 0$; sea $b = a - x$. Es claro ahora que $x = a - b$, donde $a, b \in G^+$.

(\Leftarrow). Sean $x = a - b, y = c - d$, donde $a, b, c, d \in G_+$. Entonces, $a - x = b, c - y = d, x + b = a, y + d = c$ implican $a \geq x, c \geq y, x \geq -b, y \geq -d$, y por tanto, $-(b + d) \leq x, y \leq a + c$; es decir, G es prefiltrante. ■

PROPOSICION 3.7. Para que un grupo filtrante G sea reticulado es necesario y suficiente que verifique una de las dos condiciones siguientes:

- para toda pareja $a, b \in G_+$ existe $\sup(a, b)$.
- Para toda pareja $a, b \in G_+$ existe $\inf(a, b)$.

Demostración. El teorema 3.3 muestra que a) y b) son condiciones equivalentes además ellas son evidentemente necesarias. Recíprocamente, sean $a, b \in G$ y sea $c \leq a, b$ (un tal c existe puesto que G es filtrante). Luego $a \cdot c, b \cdot c \in G_+$ y, por consiguiente existen $\inf(a, b)$ y $\sup(a, b)$, en virtud de (7). ■

DEFINICION 3.3. Sea G un grupo ordenado; si para $x \in G$ existe $\sup(x, 0)$ (y por lo tanto existe $\inf(x, 0)$), decimos que $x^+ = \sup(x, 0)$ (resp. $x^- = -\inf(x, 0)$) es la parte positiva (resp., negativa) de x .

PROPOSICION 3.8. Sean G un grupo ordenado y $x \in G$. Para que existan x^+ y x^- es necesario y suficiente que exista una pareja $(a, b) \in G \times G$ de elementos extraños entre sí y tales que $x = a \cdot b$; en este caso, $x^+ = a, x^- = b$.

Demostración. (\Rightarrow). Usando (10): $x^+ \cdot x^- = \sup(x, 0) \cdot \inf(x, 0) = x + 0 = x$. Veamos que x^+ y x^- son extraños; en efecto: $\inf(x, 0) = -x^-$ implica $\inf(x^+ \cdot x^-, 0) = -x^- = \inf(x^+ \cdot x^-, x^- \cdot x) = \inf(x^+, x^-) \cdot x^-$, es decir, $\inf(x^+, x^-) = 0$.

(\Leftarrow) Si $x = a \cdot b$ y $\inf(a, b) = 0$, entonces $-x = \inf(x, 0) = \inf(a \cdot b, 0) = \inf(a, b) \cdot b = -b$; por otra parte, existe $\sup(a \cdot b, 0) = x^+$, luego $\sup(a, b) = x^+ \cdot b = x^+ \cdot x^-$; pero $\sup(a, b) = \sup(a, b) + \inf(a, b) = a + b = a + x^-$, en consecuencia, $a = x^+$ ■

COROLARIO. Sea G un grupo ordenado. G es reticulado \Leftrightarrow todo elemento de G es la diferencia de dos elementos positivos extraños entre sí.

Demostración. La necesidad resulta de la anterior proposición. Supongamos ahora que todo elemento $x \in G$ es la diferencia de dos elementos positivos extraños entre sí. La proposición nos dice que existen x^+ y x^- . Por consiguiente, si $x, y \in G$, existe $(x \cdot y)^+ = \sup(x \cdot y, 0)$, luego existe $\sup(x, y)$, y por consiguiente existe $\inf(x, y)$. ■

EJERCICIOS

1. En un grupo reticulado, demuestre las siguientes afirmaciones:

- $\inf(x \cdot z, y \cdot z) = 0 \Leftrightarrow \inf(x, y) = z$
- $\inf(x, y) = 0 \text{ y } z \geq 0 \Rightarrow \inf(x, z) = \inf(x, y + z)$

$$c) \quad \inf(x, y) = 0 \quad y \quad z \geq 0 \quad -y \quad x \leq y + z \Rightarrow x \leq z.$$

2. En un monoide semi-reticulado muestre que

$$\inf_i (x_i + y_i) \geq \inf_i (x_i) + \inf_i (y_i)$$

para todas las sucesiones finitas de n términos $(x_i), (y_i)$.

3. Muestre que un monoide semi-reticulado inferiormente se tiene

$$n \cdot \inf(x, y) + \inf(nx, ny) = 2n \cdot \inf(x, y),$$

donde $n \in \mathbf{Z}$. Deducir que $\inf(nx, ny) = n \cdot \inf(x, y)$ si $\inf(x, y)$ es un elemento regular del monoide (i.e., si se puede cancelar).

4. Sea $G = \mathbf{Z}_I \times \mathbf{Z}$ con el orden $(m, n) \leq (p, q) \Leftrightarrow m \leq p$ y $n \leq q$. Muestre que G es filtrante y reticulado. Muestre que el subgrupo $H = \{m, n\}; m+n=0\}$ con el orden inducido no es reticulado ni filtrante.

5. Sea G un grupo reticulado. Para todo $x \in G$, definimos $|x| = \sup(x, -x)$. Muestre que :

a) $|x| = |-x|$

b) $|x| = x^+ + x^- \geq 0$

c) $|x+y| \leq |x| + |y|, \quad x, y \in G$

d) $|\sum_{i=1}^n x_i| \leq \sum_{i=1}^n |x_i|, \quad x_i \in G$

e) $||x| \cdot |y|| \leq |x+y|$

f) $(nx)^+ = nx^+; (nx)^- = nx^-, \quad \text{para } n \in \mathbf{Z}, x \in G$

g) $|nx| = |n| \cdot |x|, \quad \text{para } n \in \mathbf{Z}, x \in G.$

h) Si $\inf(x_i, x_j) = 0$ para $i \neq j$ ($i, j = 1, \dots, n$), entonces
 $\sup(x_1, \dots, x_n) = \sum_{i=1}^n x_i.$

6. Sea G un grupo reticulado. Usando el ejercicio 3, muestre que :

$$(x+y)^+ \leq x^+ + y^+, \quad |x^+ \cdot y^+| \leq |x-y| \quad \text{para } x, y \in G.$$

7. Muestre que en un grupo reticulado $|x^+ \cdot y^+| + |x^- \cdot y^-| = |x \cdot y|.$

§ 4. GRUPOS FACTORIALES.

Sean Γ un grupo aditivo y I un conjunto arbitrario. El grupo aditivo $G = \Gamma^I$ de las aplicaciones de I en Γ está ordenado por la relación: $f \leq g \Leftrightarrow f(i) \leq g(i)$ para todo $i \in I$. Esta relación es claramente compatible con la estructura de grupo de G y por lo tanto $(G, +, \leq)$ es un grupo ordenado. Así mismo $G' = \Gamma^{(I)}$ grupo de las aplicaciones de I en G con soporte finito (i.e. $f \in G' \Leftrightarrow f(i) = 0$ salvo un número finito de índices i) es un grupo ordenado para la misma relación de orden. La siguiente proposición nos muestra que G (resp. G') y Γ comparten ciertas propiedades simultáneamente:

PROPOSICION 4.1. G es filtrante (resp. reticulado) $\Leftrightarrow \Gamma$ es filtrante (resp. reticulado). G' es filtrante (resp., reticulado) $\Leftrightarrow \Gamma$ es filtrante (resp. reticulado).

Demostración. Hacemos únicamente la de: G es filtrante $\Leftrightarrow \Gamma$ es filtrante. Las otras afirmaciones se demuestran de manera semejante. Si G es filtrante, y si $x, y \in \Gamma$, definamos para $i \in I$, $x_{(i)} = (x(j))_{j \in I}$ donde $x_{(i)}(j) = 0$ si $i \neq j$ y $x_{(i)}(i) = x$. Análogamente, $y_{(i)} = (y(j))_{j \in I}$, donde $y_{(i)}(j) = 0$ si $i \neq j$ y $y_{(i)}(i) = y$. Entonces existe $f, g \in G$, tales que $f \leq x_{(i)}$, $y_{(i)} \leq g$, y por lo tanto, $f(i) \leq x$, $y \leq g(i)$, es decir, Γ es filtrante. Recíprocamente, si Γ es filtrante y $f, g \in G$, entonces para cada $i \in I$, existen $x(i), y(i) \in \Gamma$ tales que $x(i) \leq f(i)$, $g(i) \leq y(i)$, es decir, $x \leq f, g \leq y$, donde $x = (x(i))$ y $y = (y(i))$. Luego G es filtrante. ■

DEFINICION 4.1. Sean G, G' dos monoides ordenados. Un isomorfismo de grupos $n: G \rightarrow G'$ se dice un isomorfismo de grupos ordenados si: $x \leq y \Leftrightarrow n(x) \leq n(y)$. En tal caso G y G' se dicen isomorfos, como grupos ordenados.

DEFINICION 4.2. Un grupo ordenado isomorfo a un grupo de la forma $\mathbf{Z}^{(I)}$ se dice un grupo factorial.

PROPOSICION 4.1. El subgrupo H engendrado por los elementos minimales de un grupo reticulado G es factorial.

Demostración. Sea $(p_i)_{i \in I}$ el conjunto de los elementos minimales de G ; la proposición 3.4 muestra que todo elemento $x \in H$ puede escribirse de una manera y de una sola en la forma $x = \sum_{i \in I} a_i p_i$ donde los $a_i \in \mathbf{Z}$ son todos nulos salvo para un número finito de índices i . Es claro ahora que $x \rightarrow (a_i)$ define un isomorfismo de H sobre $\mathbf{Z}^{(I)}$. ■

PROPOSICION 4.2. Sea G un grupo reticulado. Entonces G es factorial \Leftrightarrow toda sucesión estrictamente decreciente de elementos de G^+ tiene sólo un número finito de términos.

Demostración. (\Rightarrow) Sean G factorial y $(x_k)_{k \geq 1}$ una sucesión de elementos positivos; ahora bien, por el isomorfismo que identifica a G con un conjunto de la forma $\mathbf{Z}^{(I)}$, a x_1 corresponde $(a_i^1)_{i \in I}$ donde $a_i^1 = 0$, salvo para un número finito de índices y $a_i^1 \geq 0$ para todo $i \in I$. Como el número de los $a_i^1 \neq 0$ es finito y además $0 \leq a_i^2 \leq a_i^1$, para todo $i \in I$, el número de los $a_i^2 \neq 0$ es menor que el de los $a_i^1 \neq 0$; etc.. Por lo tanto, existe N tal que $a_i^n = 0$ para todo $i \in I$, si $n > N$. Luego (x_k) es finita.

(\Leftarrow) Para mostrar que la condición es suficiente, basta, en virtud de la proposición 4.1, mostrar que G es engendrado por el conjunto de sus elementos minimales. Pero por la prop. 3.8, basta mostrar que todo elemento de G_+ es una suma de elementos minimales de G , ya que siendo G reticulado él está engendrado por sus elementos positivos.

Sea entonces $x \in G_+$; si $x \neq 0$, existe un elemento minimal menor que x ; en efecto, si x no es minimal (si x es minimal, la afirmación es trivial), existe $x_1 \in G_+$ tal que $x > x_1 > 0$; si x_1 es minimal la demostración se completa; si no, existe $x_2 \in G_+$ tal que $x > x_1 > x_2 > 0$; ... En esta forma vamos construyendo una sucesión estrictamente decreciente de elementos positivos, la cual debe tener solo un número finito de términos. Sea $N = \max\{n; x_n > 0\}$. Es claro que x_N es minimal, y $x \geq x_N$.

Definamos ahora $y_0 = x$; existe entonces x , minimal tal que $x = y_0 \geq x_1$. Definamos $y_1 = x_0 - x_1 = y_0 - x_1$. Si $y_1 > 0$ podemos encontrar x_2 minimal tal que $y_1 \geq x_2$. Tómese $y_2 = y_1 - x_2, \dots$

Recurrentemente, si $y_n > 0$, existe x_{n+1} minimal tal que $y_n \geq x_{n+1}$ y definimos $y_{n+1} = y_n - x_{n+1} \geq 0$. Si $y_n = 0$ detenemos la sucesión. Por hipótesis, existe N_0 tal que $y_n = 0$ si $n \geq N_0$. Luego $x = y_1 + z_1 = y_2 + z_1 + z_2 = \dots = y_{N_0} + z_{N_0} + \dots + z_1 = y_1 + \dots + z_{N_0}$. Lo cual demuestra el teorema. ■

§ 5. GRUPO DE DIVISIBILIDAD DE UN DOMINIO DE INTEGRIDAD.

DEFINICION 5.1. Sea K un cuerpo conmutativo. Llamamos un *orden de K* a todo subanillo A de K que contiene el elemento unidad de K y tal que K es el cuerpo de fracciones de A .

Así todo dominio de integridad con elemento unidad es un orden de su cuerpo de fracciones.

Dado un orden A de un cuerpo conmutativo, podemos pre-ordenar el grupo conmutativo $K^* = K - \{0\}$ definiendo $(K^*)_+ = K^* \cap A = A^*$. En efecto,

- a) $1 \in A^*$
- b) $x \in A^*, y \in A^* \Rightarrow xy \in A^*$

Los elementos de A^* son entonces los elementos *positivos* (llamados ahora *enteros*) del grupo pre-ordenado K^* . La relación de preorden $yx^{-1} \in A^*$ se escribe $x|_A y$ y la leemos x divide a y módulos A ($x|y \text{ mod. } A$). Si no, no hay de confusión del orden A al cual nos estamos refiriendo, escribimos sencillamente $x|y$.

Por ejemplo, si A es un dominio de integridad con elemento unidad y K su cuerpo de fracciones, entonces la restricción del preorden $yx^{-1} \in A^*$ a A^* puede expresarse diciendo:

$$x, y \in A^*, x|y \Leftrightarrow \exists q \in A^* \text{ tal que } y = qx,$$

lo cual corresponde exactamente a la noción de divisibilidad en un anillo tal como la estudian los diversos textos de álgebra moderna. Observamos entonces que

$$U = \{x \in K^* ; 1|x, x|1\} = \{x \in A^* ; 1|x, x|1\}$$

no es otra cosa que el grupo de las unidades de A , el cual se sigue llamando aún el *grupo de las unidades de K* .

DEFINICION 5.2. Sea A un orden de K .

- a) Si $x^{-1}y \in A^*$, x se dice un *divisor* de y (mod. A), y es un *múltiplo* de x (mod. A).
- b) Si $yx^{-1} \in A^*$, $xy^{-1} \in A^*$, x y y se dicen *asociados*; los asociados de $x \in K^*$ y las unidades se dicen los *divisores impropios* de x en K^* . Los otros divisores de x , si los hay, se dicen *propios*.
- c) Un elemento $p \in A^*$ que no es una unidad y cuyos únicos divisores son los impropios, se dice un elemento *irreducible* de A .

DEFINICION 5.3. Sea A un orden de K y $|$ la relación de preorden definida por A en K^* . El grupo ordenado D asociado a K^* se llama el *grupo de divisibilidad de K con respecto a A* ó *grupo de divisibilidad de A* .

PROPOSICION 5.1 $D = K^* / U$

Demostración. $D : K^* \rightarrow D$ es un epimorfismo de grupos ordenados cuyo núcleo es precisamente $U = 1$. ■

DEFINICION 5.4. Un dominio de A se dice *factorial* si su grupo de divisibilidad D es factorial, i.e., si D es isomorfo como grupo ordenado a un grupo de la forma $\mathbf{Z}(I)$.

Por ejemplo, \mathbf{Z} es un *anillo factorial*: su cuerpo de fracciones \mathcal{Q} es el cuerpo de los números racionales. Designemos por $P = (p_i)_{i \in I}$ el conjunto de los números primos positivos. Sabemos que todo elemento de \mathcal{Q} se escribe de una y solo una manera en la forma

$$\pm \prod_{i \in I} p_i^{a_i}$$

donde $a_i \in \mathbf{Z}$ y $a_i = 0$ salvo para un número finito de índices i . Por otra parte,

$U = \{+1, -1\}$ y $\bar{x} = \{x, -x\} \in D$. La aplicación: $D \rightarrow \mathbf{Z}^{(I)}$ que a \bar{x} hace corresponder $(\alpha_i)_{i \in I} \in \mathbf{Z}^{(I)}$ es un isomorfismo de grupos ordenados puesto que $\prod p_i^{\alpha_i} \mid \prod p_i^{\beta_i}$
 $\Leftrightarrow \alpha_i \leq \beta_i$, para todo $i \in I$.

PROPOSICION 5.2. Sean A un dominio de integridad con elemento unidad y $p \in A$ un elemento irreducible. Entonces $p \in D$ es minimal.

Demostración. a) $\bar{p} \neq 1$ puesto que p no es una unidad. b) si $\bar{x} \neq \bar{1}$ y $\bar{x} \mid \bar{p}$ entonces $\bar{x} = \bar{p}$ puesto que $x \mid p \Rightarrow x = p$, si no es una unidad. ■

TEOREMA 5.1. Un dominio de integridad A con elemento unidad es factorial \Leftrightarrow todo elemento $x \in A^*$, x es distinto de una unidad, y $(p_i)_{i \in I}$ una familia de representantes de las clases \bar{p}_i de elementos irreducibles de A , puede escribirse de manera única salvo unidades en la forma

$$x = u \prod_{i \in I} p_i^{\alpha_i}$$

donde $p_i \in A$ es irreducible, $(\alpha_i) \in \mathbf{Z}_+^{(I)}$, $u \in U$.

Demostración. Sea A un anillo factorial. La imagen de p , donde elemento irreducible $p \in A$, por el isomorfismo $D \rightarrow \mathbf{Z}^{(I)}$ es un elemento minimal de $\mathbf{Z}^{(I)}$, puesto que \bar{p} es minimal (prop. 5.2). Ahora bien, los elementos minimales de $\mathbf{Z}^{(I)}$ son los elementos $b_{(i)} = (b(j))$ con $b(j) = 0$ si $j \neq i$ y $b(i) = 1$. Por lo tanto, existe una correspondencia biunívoca entre los $b_{(i)}$ y las clases de elementos irreducibles: $(p_i)_{i \in I}$. Por otra parte, todo elemento de $\mathbf{Z}^{(I)}$ se expresa de manera única así:

$\sum_{i \in I} \alpha_i b_{(i)}$, donde $\alpha_i \in \mathbf{Z}$ y $\alpha_i = 0$ salvo para un número finito de índices i . Por lo tanto, si $\sum_{i \in I} \alpha_i b_{(i)}$ es la imagen de $x \in D$, podemos escribir

$$(5.1) \quad x = \prod_{i \in I} p_i^{\alpha_i}, \quad (\alpha_i) \in \mathbf{Z}^{(I)}$$

Sea ahora, $x \in A^*$, x distinto a una unidad. En este caso, $(\alpha_i) \in \mathbf{Z}_+^{(I)}$ y, por lo tanto,

$$(5.2) \quad x = u \prod_{i \in I} p_i^{\alpha_i}, \quad (\alpha_i) \in \mathbf{Z}^{(I)}$$

En efecto: si $x \in A^*$, es claro que x es entero en D y (α_i) debe ser entonces positivo en $Z^{(I)}$. Fijada una familia $(p_i)_{i \in I}$ de representantes de p_i , la representación (5.2) es única salvo unidades.

Recíprocamente, si todo $x \in K^*$ puede escribirse de manera única en la forma

$$x = u \prod_{i \in I} p_i^{\alpha_i}, \quad (\alpha_i) \in Z^{(I)}, \quad u \in U,$$

la aplicación: $x \rightarrow (\alpha_i)$ establece el isomorfismo deseado. ■

PROPOSICION 5.3. Sea A un dominio de integridad factorial. Si $p \in A$ es irreducible y $p | ab$, entonces $p | a$ ó $p | b$. ($a, b \in A^*$).

Demostración. Como $p_j | ab$, entonces existe $c \in A^*$ tal que $ab = p_j c$. Ahora bien, a y b no son a la vez unidades; luego podemos suponer en primer lugar que uno de los dos, e.g., a , es una unidad. En tal caso $p | b$. En segundo lugar, si a y b no son unidades, tenemos

$$\bar{p}_j \prod_{i \in I} \bar{p}_i^{r_i} = \prod_{i \in I} p_i^{(\alpha_i + \beta_i)}$$

donde

$$\bar{c} = \prod_{i \in I} \bar{p}_i^{r_i} ; \quad \bar{a} = \prod_{i \in I} \bar{p}_i^{\alpha_i} ; \quad \bar{b} = \prod_{i \in I} \bar{p}_i^{\beta_i}$$

Pero entonces

$$\bar{p}_j^{r_j+1} \left(\prod_{i \neq j} \bar{p}_i^{r_i} \right) = p^{(\alpha_j + \beta_j)} \left(\prod_{i \neq j} p_i^{(\alpha_i + \beta_i)} \right),$$

y

$$\bar{p}_j^{r_j+1} = \bar{p}_j^{(\alpha_j + \beta_j)} = \bar{p}_j^{\beta_j} \bar{p}_j^{-\alpha_j} = \bar{p}_j^{r_j} \bar{p}_j.$$

Luego p_j divide por lo menos a uno de \bar{a} y \bar{b} , puesto que $\beta_j + \alpha_j = r_j + 1 \geq 0$ y $\beta_j, r_j, \alpha_j \geq 0$. Por lo tanto, $p_j | a$, ó $p_j | b$. ■

Recíprocamente :

PROPOSICION 5.4. Sea A un dominio de integridad. Si todo $x \notin 1 = U$ puede expresarse como un producto de elementos irreducibles en número finito y si $p | ab$ implica $p | a$ ó $p | b$, para p irreducible, entonces A es factorial.

Demostración. Se deja como ejercicio. ■

Sea A factorial y sea $a \in K^* - U$, Si $ab^{-1} \in A^*$ ($b|a$), entonces cada factor irreducible de b divide a a en K , y, pasando a D , tenemos que los divisores de a se obtienen como productos de los factores irreducibles de a . Claro está que estos divisores son únicos salvo unidades; así

$$b = v \prod_{i \in I} p_i^{\beta_i} \quad | \quad a = u \prod_{i \in I} p_i^{\alpha_i} \quad \Leftrightarrow \quad \beta_i \leq \alpha_i, \quad \text{para todo } i \in I$$

Si $a, b \in A^*$, es claro que $0 \leq \beta_i \leq \alpha_i$, para todo $i \in I$. Si $a, b \notin U$, podemos encontrar los divisores comunes (salvo unidades) de a y b , así:

$$\bar{d} = \prod_{i \in I} \tilde{p}_i^{\delta_i} \quad \text{divide} \quad \bar{a} = \prod_{i \in I} \tilde{p}_i^{\alpha_i} \quad \text{y} \quad \bar{b} = \prod_{i \in I} \tilde{p}_i^{\beta_i} \quad \Leftrightarrow$$

$$\delta_i \leq \min(\alpha_i, \beta_i) \quad \text{para todo } i \in I.$$

Si $\delta_i = \min(\alpha_i, \beta_i)$, es claro que el correspondiente divisor \bar{d} es divisible por todos los otros divisores comunes de \bar{a} y \bar{b} ; se le llama el máximo común divisor de \bar{a} y \bar{b} , y se nota (\bar{a}, \bar{b}) . En la análoga forma podemos definir el mínimo común múltiplo: $\langle \bar{a}, \bar{b} \rangle$. Tenemos entonces:

PROPOSICION 5.5. Sea A un dominio factorial. Entonces

- A^*/U es un retículo.
- A^* es un pre-retículo.
- $K^*/U = D$ es un grupo reticulado. ■

Observación. Existen dominios que no son factoriales. Por ejemplo,

$A = \{a + b\sqrt{-5}, a, b \in \mathbf{Z}\}$ no lo es. (Cfr. [6], pág. 147).

DEFINICION 5.5. Sea A un dominio factorial con elemento unidad. Decimos que \bar{a} y \bar{b} son primos entre sí (extraños entre sí) si \bar{a} y \bar{b} son extraños (primos) entre sí en el grupo reticulado D . Eso significa que $(a, b) = 1$, salvo unidades.

EJERCICIOS

1. Demuestre la relación : $(\bar{a}, \bar{b}) < \bar{a}, \bar{b} > = \bar{ab}$ (Use $\min(\alpha_1 \beta) + \max(\alpha_1 \beta) = \alpha + \beta$).
2. Muestre que el grupo de divisibilidad de un dominio de integridad con elemento unidad es siempre filtrante.

(Continuará)

REFERENCIAS

1. N. BOURBAKI, *Théorie des ensembles, chap. III, Hermann, (19) París.*
2. M.L. DUBREIL-JACOTIN, *Lecons sur la theorie des treillis, (1953), París.*
3. P. JAFFARD, *Les systems d'idéaux, Dunod (1960), París.*
4. P. JAFFARD, *Contributions a la théorie des groupes ordonnés, J. Math. Pures et Appl., 32 (1953), págs. 203-280 .*
5. B. W. JONES, *Introducción a la teoría de números, Rev. Mat. Elementales, Monografías Matemáticas, No. 4 (1968), Bogotá.*
6. P. DUBREIL, M. L. DUBREIL - JACOTIN, *Lecons d'algèbre Moderne, Dunod (1961), París.*

Departamento de Matemáticas y Estadística
Universidad Nacional de Colombia
Bogotá, Colombia, S.A.

(Recibido en septiembre de 1970)