9. Dominios de ideales principales

9.1. Definición y propiedades fundamentales

Existen caracterizaciones (véase Números, Grupos y Anillos, página 246) que aconsejan definir el siguiente concepto en el ambiente de los dominios de integridad.

Definición 9.1 (Dominio de ideales principales)**.**
Dado un dominio de integridad A.

A es un dominio de ideales principales si todo ideal de A es principal, esto es, $\forall I < A.\exists x \in A.I = \langle x \rangle$.

Teorema 9.1 (Teorema de Bézout)**.**
Dado un dominio de ideales principales A.

1. $\forall a, b \in A \exists d = (a, b)$.
2. $\exists u, v \in A.d = au + bv$.

A cualquier pareja u, v que verifique la segunda ecuación se les llama coeficientes de Bézout.

Demostración. Dados $a, b \in A$, consideremos $< a, b >= \{ax + by : x, y \in A\}$ este es el ideal generado por a y b, esto es, el menor ideal que los contiene. En efecto, como $a, b \in < a, b >$ sabemos que $< a, b >$ no es vacío. También es claro que $< a, b >$ es un ideal ya que $ax+by+ax'+by' = a(x+x')+b(y+y') \in I$ y $c(ax + by) = a(xc) + b(yc) \in I$.

Utilizamos que A es un dominio de ideales principales y obtenemos que debe existir $d \in A. < a, b >=< d >$ y por tanto $d = au + bv$ para convenientes $u, v \in A$. Por tanto, hemos deducido la segunda propiedad.

Por lo anterior, $d|a \wedge d|b$ y si $c \in A$ verifica que $c|a \wedge c|b$ entonces $c|au + bv$ de donde $c|d$. Esto nos dice que $d = (a, b)$ □

Ejemplo 9.1: Por los ejemplos anteriores como en $\mathbb{Z}[\sqrt{-5}]$ no existe el máximo común divisor de cualesquiera dos elementos tampoco puede ser un dominio de ideales principales.

Proposición 9.2 (Todo DE es un DIP)**.**
Todo dominio euclídeo es un dominio de ideales principales donde cada ideal está generado por el elemento con valor mínimo de la función euclídea.

Demostración. Si ϕ es la función euclídea asociada al dominio y consideremos un ideal cualquiera $I \neq \{0\}$. El conjunto $\phi(I - \{0\})$ es un subconjunto no vacío de números naturales y por tanto tiene mínimo. Sea b este mínimo. Demostraremos que $I =< b >$.

$\subseteq$) Dado que $b \in I \implies < b > \subseteq I$.
$\supseteq$) Dado $a \in I - \{0\}$ tenemos que $\phi(a) \geq \phi(b)$. Por estar en un dominio euclídeo, $a = bq + r$ con $r = 0 \vee \phi(r) < \phi(b)$. Si $r = 0$ hemos acabado ya que entonces $a = bq \in < b >$ y por tanto $I \subseteq < b >$. Si $r \neq 0$ entonces necesariamente $\phi(r) < \phi(b)$. Pero esto contradice que b sea el elemento de valor mínimo del conjunto anterior, ya que $r = a - bq \in I$ y $\phi(r) < \phi(b)$. □

9.2. Mínimo común múltiplo. Retículos de divisibilidad e ideales.

Definición 9.2 (Mínimo cómun múltiplo)**.**
Sea A un dominio de integridad y $a, b \in A$. Decimos que m es su mínimo común múltiplo si se verifican las siguientes condiciones:

- $a|m \wedge b|m$
- $a|c \wedge b|c \implies m|c$

Lo denotaremos por $m = mcm(a, b) = [a, b]$

Notemos que un mínimo común múltiplo es único salvo asociados.

Proposición 9.3 (Propiedades del mínimo común múltiplo)**.**
1. $[a, b] = [b, a]$
2. $[a, b] = b \iff a|b$
3. $[a, 0] = 0 \wedge [a, 1] = a$
4. $[[a, b], c] = [a, b, c] = [a, [b, c]]$
5. $[ac, bc] = [a, b]c$
6. Si existe $[a, b]$ *entonces existe* (a, b) *y además* $[a, b](a, b) = ab$.

Demostración. □

Curiosamente, la existencia de máximo común divisor no garantiza la existencia de mínimo común múltiplo.

Ejemplo 9.2:

Proposición 9.4 (Existencia de mcd implica la de mcm)**.**
Sea A un dominio de integridad.

Si existe el máximo común divisor de cualquier par de elementoss entonces existe el mínimo común múltiplo de cualquier par, esto es, $\forall a, b \in A \exists (a, b) \implies \forall a, b \in A \exists [a, b]$.

Demostración. Sean $a, b \in A \setminus \{0\}$ y $d = (a, b)$. Como $d|a, b$ también $d|ab$ y como no podía ser de otro modo eligiremos $m = \frac{ab}{d}$ como candidato a ser $[a, b]$.

1. Como $m = \frac{ab}{d} = a\frac{b}{d} = ab_1 \wedge m = \frac{ab}{d} = \frac{a}{d}b = a_1 b$ es claro que $a|m \wedge b|m$.
2. Sea $m_1 \in A$ tal que $a|m_1 \wedge b|m_1$. Queremos ver que $m|m_1$. Para ello tomo $k = (m, m_1)$ que existe por las hipótesis y elijo $d_1 = \frac{m}{k} \in A$.

   Como $a|m \wedge a|m_1$ se tiene que $a|k$ y análogamente $b|k$. Sea $k = au = bv$. Tenemos:

   $$m = a_1 b = kd_1 = bvd_1 \implies a_1 = vd_1 \implies a = da_1 = vdd_1$$

   $$m = b_1 a = kd_1 = aud_1 \implies b_1 = ud_1 \implies b = db_1 = ud_1 d$$

   Por tanto,

   $$dd_1|a, b \implies dd_1|d1 \implies d_1|1 \implies d_1 \in U(A)$$

   Como $m = kd_1$ tenemos que $m = (m, m_1)$ luego $m|m_1$ como queríamos.

□

Corolario 9.5 (Existencia del mínimo común múltiplo en DIP)**.**
En cualquier dominio de ideales principales (en particular, en los dominios euclídeos), existe el mínimo común múltiplo de cualquiera dos elementos.

Demostración. En efecto, en un DIP por el teorema de Bézout existe el máximo común divisor de cualquier par de elementos y como un DIP es un dominio de integridad se tiene por la proposición anterior que existe el mínimo común múltiplo de cualquier par de elementos.

Cualquier dominio euclídeo es un dominio de ideales principales. □

Corolario 9.6 (Retículo de divisibilidad)**.**
Sea D un dominio de ideales principales y sea $(,),[,]$ el máximo común divisor y el mínimo común múltiplo respectivamente. Entonces $(D,(,),[,])$ es un retículo.

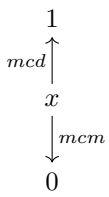
Demostración. Elijamos $[,]$ como ínfimo y $(,)$ como supremo.

Por lo anterior, estas operaciones son internas en D.

Claramente, se verifican las propiedades conmutativa, asociativa y la propiedad de idempotencia. Faltaría demostrar la propiedad de absorción que diría $[x,(x,y)]=x$ y $(x,[x,y])=x$.

Por otro lado, el máximo del retículo es el 1 del dominio y el mínimo del retículo es el 0 del dominio.

En consecuencia, $(a,1)=1,(a,0)=a$. También el 0 del dominio es el mínimo del retículo, y en particular, $[a,0]=0,[x,1]=x$. □



Pregunta: ¿este retículo es distributivo, es complementado? ¿Es el 1 el máximo y el 0 el mínimo o hay maximales (las unidades) y minimales? Aquí solo hace falta que sea distributivo y complementado para ser un álgebra de Boole.

Corolario 9.7 (Retículo de ideales de un DIP)**.**
Sea A un dominio de ideales principales consideremos el retículo de ideales ordenado por la inclusión las operaciones supremo e ínfimo y producto están definidas para este en términos del máximo común divisor y del mínimo común múltiplo. Más precisamente, para todo $a,b\in A$:

1. $\langle a\rangle+\langle b\rangle=\langle(a,b)\rangle$
2. $\langle a\rangle\cap\langle b\rangle=\langle[a,b]\rangle$
3. $\langle a\rangle\cdot\langle b\rangle=\langle ab\rangle$

Demostración.
1. Es consecuencia del teorema de Bézout.
2. Se deriva desde la definición.
3. Se deriva desde la definición.

□