Jose Antonio Lorencio Abril

Abril 2020

2.6.2. Sea D un dominio y sea K su cuerpo de fracciones. Supongamos que existe una aplicación $\delta : K \setminus \{0\} \to \mathbb{Q}$ que conserva productos y tal que $\delta(D) \subset \mathbb{Z}^{\geq 0}$. Demostrar que la restricción de δ a D es una función euclídea en D si y solo si para todo $x \in K \setminus D$ existe $y \in D$ tal que $\delta(x - y) < 1$.

' $\implies$ ' La restricción, que voy a llamar d, es una función euclídea si verifica $DE1$ y $DE2$.

Dado $x \in K \setminus D$, entonces podemos escribir $x = \frac{a}{b}$, con $b \neq 1, 0$, y $b \nmid a$, *coprimos*. De esta forma $\delta(x) = \delta\left(\frac{a}{b}\right)$ y sea $k = \delta(1)$.

Ahora bien, $\delta(1) = \delta(1 \cdot 1) = \delta(1)\delta(1) = \delta(1)^2 \implies \delta(1) \in \{-1, 0, 1\}$.

No puede ser -1, ya que $1 \in D \implies \delta(1) = d(1) \in \mathbb{Z}^{\geq 0}$. Por tanto, $k = \delta(1) \in \{0, 1\}$.

Pero, si $k = 0$ y se conserva el producto, entonces $d(a) = d(a1) = d(a)d(1) = 0$. Luego $d(a) = 0,\ \forall a \in D$. Por lo que no puede verificarse DE2.

Es decir, $k = 1$.

¿Será $\delta\left(\frac{a}{b}\right) = \frac{\delta(a)}{\delta(b)} = \frac{d(a)}{d(b)}$?

$$\frac{a}{b} = a \cdot b^{-1} \overset{\delta \text{ conserva productos}}{\Longrightarrow} \delta\left(\frac{a}{b}\right) = \delta(a \cdot b^{-1}) = \delta(a) \cdot \delta(b^{-1}) = d(a)\delta(b^{-1})$$

Por otro lado, tenemos que
$b \cdot b^{-1} = 1 \implies \delta(b)\delta(b^{-1}) = \delta(b \cdot b^{-1}) = \delta(1) = 1 \implies \delta(b^{-1}) = \frac{1}{\delta(b)} = \frac{1}{d(b)}$

Entonces, queda que

$$\delta(x) = \delta\left(\frac{a}{b}\right) = \frac{d(a)}{d(b)}$$

Por $DE2$, existen $q, r \in D$ tales que $a = bq + r$ y o bien $r = 0$ o bien $d(r) < d(b)$.

Sabemos que $r \neq 0$, pues entonces la fracción sería simplificable. Por tanto, $d(r) < d(b)$.

Y se tiene que $bq = a - r$.

De aquí deducimos que tomando $y = q$, obtenemos que

$$\delta\left(\frac{a}{b} - q\right) = \delta\left(\frac{a - bq}{b}\right) = \delta\left(\frac{a - a + r}{b}\right) = \delta\left(\frac{r}{b}\right) = \frac{d(r)}{d(b)} < 1$$

Y tenemos el resultado.

$' \Longleftarrow '$

Nótese que excluyo el caso de δ idénticamente nula, en este caso no nos proporciona una función euclídea.

DE1: Sean $a, b \in D$, tales que $a|b$, entonces ¿$d(a) \leq d(b)$?

Como d conserva el producto, entonces, tenemos que $b = ac$, entonces $d(b) = d(ac) = d(a)d(c)$.

Si fuera $d(c) = 0$, entonces tendríamos, en K, que $1 = \delta(1) = \delta(cc^{-1}) = \delta(c)\delta(c^{-1}) = d(c)\delta(c^{-1}) = 0\#$
Esto es una contradicción, por lo que debe ser $d(c) \geq 1 \implies d(a) \leq d(b)\checkmark$

DE2: Sean $a, b \in D$ con $b \neq 0$.

Entonces, existe $y \in D$ tal que $\delta\left(\frac{a}{b} - y\right) < 1$. Entonces, tenemos que

$$\delta\left(\frac{a - by}{b}\right) = k\frac{\delta(a - by)}{\delta(b)} < 1$$

$$\delta(a - by) < \delta(b)$$

Tomando $r = a - by$, $q = y$, tenemos que

$$a = yb + a - by = yb + r$$

Si $r = 0$, entonces $a = yb \implies b|a$.

Si $r \neq 0$, hemos visto que $d(r) = \delta(r) < \delta(b) = d(b)$. $\checkmark$

2.6.3. Usar el problema anterior para decidir qué números naturales m la aplicación $d(x) = |x|^2$ define una función euclídea en $\mathbb{Z}\left[\sqrt{-m}\right]$.

El cuerpo de fracciones es $\mathbb{Q}\left[\sqrt{-m}\right]$ por el ejemplo 2.36.

Dado $x \in \mathbb{Q}\left[\sqrt{-m}\right]$ tenemos que $x = \frac{a}{b} + \frac{c}{d}\sqrt{-m}$.

Entonces

$$d(x) = \left(\frac{a}{b} + \frac{c}{d}\sqrt{-m}\right)\left(\frac{a}{b} - \frac{c}{d}\sqrt{-m}\right) = \frac{a^2}{b^2} + \frac{c^2}{d^2}m$$

Si tomamos $y = y_1 + y_2\sqrt{-m}$, con y_1 el entero más cercano a $\frac{a}{b}$ e y_2 el entero más cercano a $\frac{c}{d}$, entonces tendremos que $\left|\frac{a}{b} - y_1\right| \leq \frac{1}{2}$, $\quad \left|\frac{c}{d} - y_2\right| \leq \frac{1}{2}$, por lo que

$$d(x-y) = d\left(\left(\frac{a}{b} - y_1\right) + \left(\frac{c}{d} - y_2\right)\sqrt{-m}\right) = \left|\frac{a}{b} - y_1\right|^2 + \left|\frac{c}{d} - y_2\right|^2 m \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 m = \frac{1}{4} + \frac{m}{4} \leq \frac{m+1}{4}$$

Y $\mathbb{Z}\left[\sqrt{-m}\right]$ admitirá a d como función euclídea si y solo si

$$\frac{m+1}{4} < 1 \iff m + 1 < 4 \iff m < 3$$

Es decir, $m \in \{1, 2\}$.

2.6.4 Sea m un entero libre de cuadrados, es decir no es divisible por el cuadrado de ningún otro entero. Sea

$$\boldsymbol{A_m = \left\{\frac{a+b\sqrt{m}}{2} : a \equiv b \ mod \ 2\right\}}$$

Demostrar que A_m es un subanillo de los números complejos si y solo si $m \equiv 1 \ mod \ 4$. Usar el problema 2.6.2 para decidir para qué números primos p, A_{-p} es un subanillo de los números complejos y la función $d(x) = |x|^2$ define una función euclídea en A_{-p}.

- ¿$1 \in A_m$?

$$1 = \frac{2+0\sqrt{m}}{2}, \ 2 \equiv 0 \mod 2 \checkmark$$

- Suma

  Sean $a, b \in A_m$, entonces

$$\frac{a_1+a_2\sqrt{m}}{2} + \frac{b_1+b_2\sqrt{m}}{2} = \frac{(a_1+b_1)+(a_2+b_2)\sqrt{m}}{2}$$

  Y

$$\begin{array}{l} a_1 \equiv a_2 \mod 2 \\ b_1 \equiv b_2 \mod 2 \end{array} \implies a_1+b_1 \equiv a_2+b_2 \mod 2 \checkmark$$

- Producto

  Sean $a, b \in A_m$, entonces

$$\left(\frac{a_1+a_2\sqrt{m}}{2}\right)\left(\frac{b_1+b_2\sqrt{m}}{2}\right) = \frac{a_1b_1+a_1b_2\sqrt{m}+a_2b_1\sqrt{m}+ma_2b_2}{4} =$$

$$= \frac{(a_1b_1+ma_2b_2)+(a_1b_2+a_2b_1)\sqrt{m}}{4}$$

  Sabemos que $a_1 - a_2 = 2k \iff a_1 = 2k + a_2$, e igual pasa con los b. Entonces es

$$\frac{((2k+a_2)(2j+b_2)+ma_2b_2)+((2k+a_2)b_2+a_2(2j+b_2))\sqrt{m}}{4} =$$

$$= \frac{(4jk+2kb_2+2ja_2+a_2b_2+ma_2b_2)+(2kb_2+a_2b_2+2ja_2+a_2b_2)\sqrt{m}}{4} =$$

$$= \frac{(4jk+2kb_2+2ja_2+(m+1)a_2b_2)+(2kb_2+2a_2b_2+2ja_2)\sqrt{m}}{4} =$$

  El sumando de la derecha es divisible por 2, y queremos que el de la izquierda también lo sea, para simplificar el denominador. Para ello ha de ser $m+1$ un número par. Por lo que m es impar y por tanto congruente módulo 4 con 1 o con -1. Vamos a suponer que es así y seguimos:

$$\frac{\left(2jk+kb_2+ja_2+\frac{m+1}{2}a_2b_2\right)+(kb_2+a_2b_2+ja_2)\sqrt{m}}{2}$$

  Ahora queremos que el primer sumando sea congruente módulo dos con el segundo:

$$2jk \equiv 0 \mod 2$$

El kb_2 y el ja_2 son congruentes consigo mismos. Por lo que solo resta ver que

$$\frac{m+1}{2}a_2b_2 \equiv a_2b_2 \mod 2 \iff \frac{m+1}{2}a_2b_2 - a_2b_2 = 2n \iff \left(\frac{m+1}{2}-1\right)a_2b_2 = 2n \iff$$

$$\iff \left(\frac{m+1-2}{2}\right)a_2b_2 = 2n \iff (m-1)\,a_2b_2 = 4n \iff (m-1)\,a_2b_2 \equiv 0 \mod 4$$

Como esto debe darse para todo a_2b_2, sucederá si y solo si

$$m-1 \equiv 0 \mod 4 \iff m \equiv 1 \mod 4 \checkmark$$

Segunda parte

La función es

$$\delta\left(\frac{a+b\sqrt{-p}}{2}\right) = \delta\left(\frac{a+bi\sqrt{p}}{2}\right) = \left(\frac{a}{2}+\frac{b\sqrt{p}}{2}i\right)\left(\frac{a}{2}-\frac{b\sqrt{p}}{2}i\right) = \frac{a^2}{4}+\frac{b^2p}{4}$$

Conserva productos pues es la norma cuadrado.

¿Va a los enteros no negativos?

Sabemos que $a \equiv b \mod 2 \iff a-b=2n \iff a=2n+b$, y $-p \equiv 1 \mod 4 \iff p \equiv -1 \mod 4 \iff p+1=4k$ entonces

$$\frac{(2n+b)^2+pb^2}{4} = \frac{4n^2+4nb+b^2+pb^2}{4} = n^2+nb+\frac{(1+p)\,b^2}{4} =$$

$$= n^2+nb+\frac{4kb^2}{4} = n^2+nb+kb^2 \in \mathbb{Z}^{\geq 0}$$

Vamos a ver cuál es su cuerpo de fracciones. Para ello tomamos dos elementos del anillo, hacemos la fracción y operamos:

$$\frac{\frac{a_1+a_2\sqrt{-p}}{2}}{\frac{b_1+b_2\sqrt{-p}}{2}} = \frac{(a_1+a_2\sqrt{-p})\,(b_1-b_2\sqrt{-p})}{(b_1+b_2\sqrt{-p})\,(b_1-b_2\sqrt{-p})} = \frac{a_1b_1+pa_2b_2+(a_2b_1-a_1b_2)\sqrt{-p}}{b_1^2+pb_2^2} =$$

$$= \frac{a_1b_1+pa_2b_2}{b_1^2+pb_2^2}+\frac{a_2b_1-a_1b_2}{b_1^2+pb_2^2}\sqrt{-p}$$

Esto está en $\mathbb{Q}\,[\sqrt{-p}]$.

Veamos si se verifica el recíproco, ¿$\frac{a_1}{a_2}+\frac{b_1}{b_2}\sqrt{-p} \in Q\,(A_{-p})$?

$$\frac{a_1}{a_2} = \frac{\frac{2a_1+0\sqrt{-p}}{2}}{\frac{2a_2+0\sqrt{-p}}{2}} \in Q\,(A_{-p})$$

$$\frac{b_1}{b_2}\sqrt{-p} = \frac{\frac{0+b_1\sqrt{-p}}{2}}{\frac{0+b_2\sqrt{-p}}{2}} \in Q\,(A_{-p})$$

Por tanto, su suma está en $Q\,(A_{-p})$.

Es decir, $Q\,(A_{-p}) = \mathbb{Q}\,[\sqrt{-p}]$.

Dado $x \in \mathbb{Q}\,[\sqrt{-p}] \setminus A_{-p}$

$$x = \frac{a_1}{a_2}+\frac{b_1}{b_2}\sqrt{-p}$$

Si tomamos $y = \frac{a+b\sqrt{-p}}{2} \in A_{-p}$, con b como el entero más cercado a $2\frac{b_1}{b_2}$ y a como el entero más cercano a $2\frac{a_1}{a_2}$ que verifica $a \equiv b \mod 2$, entonces tenemos que $\left|2\frac{a_1}{a_2} - a\right| \leq 1 \iff \left|\frac{a_1}{a_2} - \frac{a}{2}\right| \leq \frac{1}{2}$, $\left|2\frac{b_1}{b_2} - b\right| \leq \frac{1}{2} \iff \left|\frac{b_1}{b_2} - \frac{b}{2}\right| \leq \frac{1}{4}$, y entonces

$$\delta\left(x-y\right) = \left|x-y\right|^2 = \left|\frac{a_1}{a_2} - \frac{a}{2} + \left(\frac{b_1}{b_2} - \frac{b}{2}\right)\sqrt{-p}\right| = \left(\frac{a_1}{a_2} - \frac{a}{2}\right)^2 + p\left(\frac{b_1}{b_2} - \frac{b}{2}\right)^2 \leq \frac{1}{4} + \frac{p}{16}$$

Entonces, ha de ser

$$\frac{4+p}{16} < 1 \iff 4+p < 16 \iff p < 12$$

O sea, que $0 < p < 12$, con p primo y con $p \equiv -1 \mod 4$.

Los únicos que verifican la desigualdad son $\{1, 2, 3, ..., 11\}$, de ellos los primos son $\{2, 3, 5, 7, 11\}$ y de estos, los que cumplen la congruencia son:

$$p \in \{3, 7, 11\}$$