Entrega 2: Divisibilitat i dominis euclidians

Arnau Mas

18 de maig 2018

Considerem l'anell $\mathbb{Z}[\sqrt{-3}] := \mathbb{Z} + \sqrt{-3}\,\mathbb{Z} \subseteq \mathbb{C}$ amb la suma i producte de $\mathbb{C}$. Hi podem definir l'aplicació

$$\begin{aligned} N\colon \mathbb{Z}[\sqrt{-3}] &\longrightarrow \mathbb{N} \\ z = a + b\sqrt{-3} &\longmapsto a^2 + 3b^2. \end{aligned}$$

Comprovem que N és una norma, és a dir, que és definida estrictament positiva i que és multiplicativa. És clar que per tot $z \in \mathbb{Z}[\sqrt{-3}]$ es té $N(z) \geq 0$. També és clar que $N(0) = 0$. Finalment, si $N(z) = 0$ hem de poder concloure $z = 0$. Si $z = a + b\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ i $N(z) = 0$ tenim $a^2 + 3b^2 = 0$, però com que $a^2, b^2 > 0$ si $a, b > 0$ ha de ser $a = b = 0$ i per tant $z = 0$.

Per veure que N és multiplicativa observem que $N(z) = z\bar{z}$ per tot $z \in \mathbb{Z}[\sqrt{-3}]$. Efectivament, si $z = a + b\sqrt{-3}$ tenim

$$z\bar{z} = (a + \sqrt{-3}b)(a - \sqrt{-3}b) = a^2 + 3b^2 = N(z).$$

Per tant, per tot $z, w \in \mathbb{Z}[\sqrt{-3}]$ tenim

$$N(zw) = zw\bar{z}\bar{w} = z\bar{z}w\bar{w} = N(z)N(w).$$

— ∗ —

Considerem $u \in \mathbb{Z}[\sqrt{-3}]$ una unitat. Per tant existeix $u^{-1} \in \mathbb{Z}[\sqrt{-3}]$ tal que $uu^{-1} = 1$. Fent servir que la norma és multiplicativa i que $N(1) = 1$ tenim

$$1 = N(1) = N(uu^{-1}) = N(u)N(u^{-1}).$$

Per tant ha de ser $N(u) = 1$ o $N(u) = -1$ ja que $u \neq 0$. Però com que $N(u) > 0$ concloem $N(u) = 1$.

I si $z \in \mathbb{Z}[\sqrt{-3}]$ compleix $N(z) = 1$ tenim $z\bar{z} = 1$ i per tant z és una unitat amb $z^{-1} = \bar{z}$.

Per determinar $\mathbb{Z}[\sqrt{-3}]^\times$ només cal que determinem tots els $z \in \mathbb{Z}[\sqrt{-3}]$ tals que $N(z) = 1$. És a dir, hem de trobar totes les solucions de $a^2 + 3b^2 = 1$ amb $a, b \in \mathbb{Z}$. Observem que ha de ser $b = 0$ ja que si $b \neq 0$ aleshores $b^2 \geq 1$ i per tant $a^2 + 3b^2 \geq 3$. Per tant les úniques possibles opcions són $a = 1$ o $a = -1$. Així doncs les unitats de $\mathbb{Z}[\sqrt{-3}]$ són

$$\mathbb{Z}[\sqrt{-3}]^\times = \{1, -1\}.$$

— * —

Considerem $z \in \mathbb{Z}[\sqrt{-3}]$ amb $N(z) = 4$. Observem primer que $z \neq 0$ ja que $N(z) \neq 0$. Si existeixen $\alpha, \beta \in \mathbb{Z}[\sqrt{-3}]$ tals que $z = \alpha\beta$ aleshores hem de tenir $N(\alpha)N(\beta) = N(\alpha\beta) = 4$. És a dir, $N(\alpha), N(\beta) \mid 4$. Per tant els únics valors possibles per $N(\alpha)$ i $N(\beta)$ són 1, 2 o 4. Els valors que pot pendre la norma, però, estan molt restringits per a valors petits. De fet, la norma d'un element no pot ser mai 2. En efecte, si $z = a + \sqrt{-3}b \in \mathbb{Z}[\sqrt{-3}]$ complís $N(z) = 2$ tindriem $a^2 + 3b^2 = 2$. Però això és impossible ja que si $b \neq 0$ aleshores $b^2 > 1$ i per tant $N(z) = a^2 + 3b^2 \geq 3$. I si $b = 0$ aleshores a^2 no pot ser 2 si $a \in \mathbb{Z}$.

El que tenim és que o bé $N(\alpha) = 1$ o bé $N(\alpha) = 4$. En el primer cas α és una unitat, per l'apartat anterior. I en el segon ha de ser $N(\beta) = 1$ i per tant ara és β la que és una unitat. Sigui com sigui, acabem de provar que si z descomposa en producte de dos factors, almenys un dels dos sempre és una unitat, i per tant z és irreductible.

— * —

Considerem $z = 2$ i $w = 1 + \sqrt{-3}$. Tenim $N(z) = N(w) = 4$ i per tant, per l'apartat anterior, els dos són irreductibles.

Volem provar que 1 és un màxim comú divisor de z i w. És clar que z i w no són associats ja que les úniques unitats de $\mathbb{Z}[\sqrt{-3}]$ són 1 i -1. També és evident que 1 és divisor comú de z i w. Hem de veure que qualsevol altre divisor comú de z i w és una unitat. Considerem, doncs, $d \in \mathbb{Z}[\sqrt{-3}]$ un divisor comú de z i w. És a dir, podem escriure $z = \alpha d$ i $w = \beta d$ per alguns $\alpha, \beta \in \mathbb{Z}[\sqrt{-3}]$. Com que z i w són irreductibles hi ha dues possibilitats: o bé d és una unitat o bé α i β són unitats. En el primer cas ja hem acabat. I si el segon fos cert tindriem que z i w són associats, però això sabem que no és veritat. Per tant d ha de ser una unitat i concloem que 1 és un màxim comú divisor de z i w.

Si z i w compleixen una identitat de Bézout vol dir que existeixen $\lambda, \mu \in \mathbb{Z}[\sqrt{-3}]$ tals que

$$\lambda z + \mu w = 1.$$

Posem $\lambda = \lambda_1 + \lambda_2\sqrt{-3}$ i $\mu = \mu_1 + \mu_2\sqrt{-3}$. Estem dient, doncs, que

$$2\lambda_1 + \mu_1 - 3\mu_2 + (2\lambda_2 + \mu_1 + \mu_2)\sqrt{-3} = 1.$$

Per tant ha de ser $2\lambda_2 + \mu_1 + \mu_2 = 0$ i $2\lambda_1 + \mu_1 - 3\mu_2 = 1$. Restant trobem

$$2(\lambda_1 - \lambda_2) - 4\mu_2 = 1.$$

Però aleshores λ_1, μ_1 i μ_2 no poden existir ja que tant $2(\lambda_1 - \lambda_2)$ com $4\mu_2$ serien parells i -1 no és parell. Per tant z i w no satisfan una identitat de Bézout.

— * —

Tenim que $zw = 2(1 + \sqrt{-3}) = 2 + 2\sqrt{-3}$ és un múltiple comú de z i w. També ho és $z^2 = w\bar{w} = 4$ i $N(z^2) = N(w\bar{w}) = 16$. Si z i w tinguessin un mínim comú múltiple m hauria de passar, per definició, $m \mid 4$ i $m \mid (2 + 2\sqrt{-3})$. Això ens diu $N(m) \mid 16$. Com hem comentat abans, la norma d'un element de $\mathbb{Z}[\sqrt{-3}]$ no pot ser 2, per tant $N(m) \neq 8$ ja que si fos així i escribim $4 = am$ aleshores $N(a) = 2$: una contradicció. A més, com que, per definició, $z \mid m$ i $w \mid m$ hem de tenir $N(m) \geq 4$. Les úniques opcions possibles, doncs, són $N(m) = 16$ i $N(m) = 4$.

Si $N(m)$ fos 16 aleshores tindriem que m és associat tant a z^2 com a $w\bar{w}$ —com que $m \mid z^2 = 4$ tenim $m = 4b$ per $b \in \mathbb{Z}[\sqrt{-3}]$, però aleshores $N(b) = 1$ i b és una unitat; i de la mateixa manera comprovem que m i $w\bar{w}$ serien associats—, però això sabem que no és el cas ja que $w\bar{w}$ i z^2 no són associats.

I si $N(m)$ fos 4 aleshores, per un apartat anterior, m seria irreductible; en contradicció amb la hipotesi que $z \mid m$ i $w \mid m$ —i amb que z i w no són associats. Així doncs concloem que m no pot existir i que z i w no tenen mínim comú múltiple.

— ∗ —

Hem de veure que $2w$ i $2z$ no tenen màxim comú divisor. Tenim $2w = zw = 2+2\sqrt{-3}$ i $2z = z^2 = w\bar{w} = 4$. És clar que $z = 2$ és un divisor comú de $2z$ i $2w$, així com w. Així, si d és un màxim comú divisor de $2w$ i $2z$ hem de tenir $z \mid d$ i $w \mid d$. A més $d \mid 2w$ i $d \mid 2z$. Això ens restringeix molt $N(d)$: concretament, $4 \mid N(d)$ i $N(d) \mid 16$. Seguint el mateix argument que a l'apartat anterior, no és possible que $N(d) = 8$. Si $N(d) = 4$ és irreductible, la qual cosa implicaria que tant z com w són associats a d i per tant associats entre si, però sabem que no és el cas. I si $N(d) = 16$ podriem concloure que $2w$ i $2z$ són associats, que també sabem que no és el cas. Així doncs, d no pot existir i per tant $2z$ i $2w$ no tenen màxim comú divisor.

— ∗ —

Tenim
$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$
Ja hem vist que tant 2 com $1+\sqrt{-3}$ són irreductibles no associats. També és irreductible $1-\sqrt{-3}$ ja que $N(1-\sqrt{-3}) = 4$. I 2 tampox no és associat a $1-\sqrt{-3}$. Per tant acabem d'escriure 4 com a producte d'irreductibles de dues maneres diferents. Això ens dóna que $\mathbb{Z}[\sqrt{-3}]$ no és un DFU.