Un anneau principal non euclidien

30 juin 2013

Lemme. *Soit (A, ν) un anneau euclidien. Il existe $x \in A$ tel que $x \notin A^\times$ tel que la restriction à $A^\times \cup \{0\}$ de la projection canonique de A sur $A/(x)$ soit surjective.*

Démonstration. Si A est un corps, $x = 0$ convient. Sinon, parmi les éléments de A non nuls et non inversibles, on choisit x tel que $\nu(x)$ soit minimal. Alors, si $a \in A$, on a $a = xq + r$ avec $r = 0$ ou $\nu(r) < \nu(x)$, donc $a \equiv r[x]$. Mais si $r \neq 0$, comme $\nu(r) < \nu(x)$, r est inversible et a est bien égal, modulo x à 0 ou à un élément de $A^\times$. $\square$

Proposition. $A = \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] =: \mathbb{Z}[\alpha]$ *n'est pas un anneau euclidien.*

Démonstration. On pose $\alpha = \frac{1+i\sqrt{19}}{2}$, d'où $\overline{\alpha} = \frac{1-i\sqrt{19}}{2}$ et α vérifie l'équation $\alpha^2 - \alpha + 5 = 0$. En effet, on a $\alpha + \overline{\alpha} = 1$et $\alpha\overline{\alpha} = 5$ d'où $\alpha^2 + \alpha\overline{\alpha} = \alpha$ et $\alpha^2 - \alpha + 5 = 0$. On remarque que $A = [a + b\alpha \mid a, b \in \mathbb{Z}]$. L'anneau $\mathbb{Z}[\alpha]$ est un sous-anneau de $\mathbb{C}$ et est donc intègre. De plus, A est stable par conjugaion car $\overline{\alpha} = 1 - \alpha$. On a $A^\times = \{\pm 1\}$. En effet, si $z \in A^\times$, il existe $z' \in A$ tel que $zz' = 1$ d'où $|z|\,|z'| = 1$ et $|z|^2 = 1$. Or, $|z|^2 = |a + b\alpha|^2 = \left(a + \frac{b}{2}\right)^2 + \left(b\frac{\sqrt{19}}{2}\right)^2 = a^2 + ab + 5b^2$ avec $a, b \in \mathbb{Z}$. Or, Si $b \neq 0$, $\left(b\frac{\sqrt{19}}{2}\right)^2 > 1$ donc $|z| > 1$. Ainsi, $b = 0$ et $a = \pm 1$ et $A^\times = \{\pm 1\}$.

Il en résulte que A n'est pas eucliien, sinon, en vertu du lemme, il existerait $x \in A$ tel que $A/(x)$ soit un corp à 2 ou 3 éléments. on aurait donc un homomorphisme surjectif $\varphi : A \to K$ avec $K = \mathbb{F}_2$ ou $\mathbb{F}_3$. La restriction de φ à $\mathbb{Z}$ étant la projection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$, on aurait donc un élément $\beta = \varphi(\alpha) \in K$ vérifiant $\beta^2 - \beta + 5 = 0$ dans K. Pour $K = \mathbb{F}_2$, on aurait $\beta^2 + \beta + 1 = 0$, qui n'a pas de solution dans $\mathbb{F}_2$. Pour $K = \mathbb{F}_3$, on aurait $\beta^2 - \beta - 1 = 0$ qui n'a pas de solution dans $\mathbb{F}_3$, d'où une contradiction. $\square$

Proposition. *A est un anneau principal.*

Démonstration. Soit $\mathcal{I}$ un idéal de A différent de $\{0\}$. Soit $y \in \mathcal{I} \setminus \{0\}$ tel que $|y|$ soit minimal. Soit $x \in \mathcal{I}$ non nul. Comme x et $\overline{y}$ apprtiennent à A, leur produit appartient à A et

$$z := \frac{x}{y} = \frac{x\overline{y}}{|y|^2} = \frac{\alpha + \beta\alpha}{\gamma}$$

avec $a, b, c \in \mathbb{Z}$ et $c > 0$. Quitte à les diviser par leur pgcd, nous supposons que a, b, c sont premiers entre eux dans leur ensemble. On souhaite montrer que $x \in (y) = y.A$ donc que $z \in A$, c'est à dire que $c = 1$.

Supposons que $c = 2$. Alors, a ou b est impair. Posons $u = a + b\overline{\alpha}$. On a $z = \frac{\overline{u}}{2}$. On prouv, en examinant les parités possibles de a et b, que l'entier naturel $|u|^2 = a^2 + ab + 5b^2$ est impair, d'où l'existence de $v \in \mathbb{N}$ tel que $|u|^2 = 2v + 1$. Alors,

$$zu - v = \frac{1}{2}|u|^2 - v = \frac{1}{2}$$

Supposons que $\gamma \geq 3$. Le théorème de Bézout fournit $m, n, q \in \mathbb{Z}$ tels que $na + (m+n)b - qc = 1$. Notons p l'entier le plus proche de $\frac{ma - 5nb}{c}$ et posons $u = m + n\alpha$ et $v = p + q\alpha$. On a :

$$\begin{aligned}
zu - v &= \frac{a + b\alpha}{c}(m + n\alpha) - (p + q\alpha) \\
&= \frac{ma + mb\alpha + na\alpha + (\alpha - 5)nb}{c} - (p + q\alpha) \\
&= \frac{ma - 5nb}{c} - p + \frac{na + (m+n)b - qc}{c} \cdot \alpha \\
&= \frac{ma - 5nb}{c} - p + \frac{\alpha}{c} = r + \frac{\alpha}{c}
\end{aligned}$$

où r est un nombre rationnel tel que $|r| \leq \frac{1}{2}$ donc :

$$\begin{aligned}|zu-v|^2 &= \left|r+\frac{\alpha}{c}\right|^2 = \left(r+\frac{\alpha}{c}\right)\left(r+\frac{\overline{\alpha}}{c}\right) = r^2 + r\frac{\alpha+\overline{\alpha}}{c} + \frac{\alpha\overline{\alpha}}{c^2} \\ &= r^2 + \frac{r}{c} + \frac{5}{c^2} \leq \frac{1}{4} + \frac{1}{6} + \frac{5}{9} = \frac{35}{36} < 1\end{aligned}$$

De plus $zu - v \neq 0$, car sinon $\alpha = -Rc$ donc α est réel, ce qui évidemment faux. Dans les deux cas ($c = 2$ ou $c \geq 3$) on a trouvé des éléments u et v de A tels que $zu - v \neq 0$ et $|zu - v| < 1$. Or $ux - vy = y(zu - v)$ donc $ux - vy \neq 0$ et $|ux - vy| = |y|\,|zu - v| < 1$. Comme x et y appartiennent à l'idéal $\mathcal{I}$ et u et v à A, $ux - vy \in I \setminus \{0\}$, don l'inégalité $|ux - vy| < |y|$ contredit la définition de y. Donc $c = 1$, ce qui achève la preuve. $\square$

Leçon concernée :
122 Anneaux principaux. Applications.

Références

[1] Daniel Perrin. Cpours d'algèbre. Ellipses.

[2] Bertrand Hauchecorne. Les Contre-exemples en mathématiques. Ellipses.