Un anneau vraiment passionnant.

Théorème. *L'anneau*

$$\mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right] = \left\{z = a + b\frac{1+i\sqrt{19}}{2} \in \mathbf{C},\ a, b \in \mathbf{Z}\right\}$$

est principal mais non euclidien.

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

Preuve. Si A est un corps, $x = 0$ convient. Sinon, parmi les éléments de A non nuls et non inversibles, on choisit x de stathme minimal. Alors, si $a \in A$, on écrit $a = xq + r$ avec $r = 0$ ou $\nu(r) < \nu(x)$. Si $r \neq 0$, alors r est inversible par définition de x. Finalement, modulo (x), a est égal à 0 ou à un élément inversible. □

Appliquons ce résultat. On va noter $\alpha = \mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ et $\overline{\alpha}$ son conjugué. Remarquons que :

$$\alpha + \overline{\alpha} = 1 \quad \text{et} \quad \alpha\overline{\alpha} = 5$$

donc α vérifie l'équation $\alpha^2 - \alpha + 5 = 0$. En tant que sous-anneau de $\mathbf{C}$, $\mathbf{Z}[\alpha]$ est intègre et stable par conjugaison puisque $\overline{\alpha} = 1 - \alpha$. On définit pour $z \in \mathbf{Z}[\alpha]$ ce qu'on appellera *norme* :

$$N(z) = z\overline{z} = a^2 + ab + 5b^2 \in \mathbf{N}.$$

L'objectif est le calcul des inversibles. Soit $z \in \mathbf{Z}[\alpha]^\times$, alors :

$$1 = N(1) = N(zz^{-1}) = N(z)N(z^{-1})$$

donc $N(z) = 1$ (c'est un inversible de $\mathbf{N} \subset \mathbf{Z}$) et on a la relation :

$$a^2 + ab + 5b^2 = 1 \ \text{ où } \ z = a + b\alpha.$$

Or, on voit que :

$$b^2 + a^2 + ab \geq b^2 + a^2 - |ab| \geq (|b| - |a|)^2 \geq 0$$

donc

$$1 = a^2 + ab + 5b^2 \geq 4b^2$$

de sorte que $b = 0$ et $a = \pm 1$. Finalement, $\mathbf{Z}[\alpha]^\times = \{\pm 1\}$.

Si cet anneau était euclidien, il existerait $x \in \mathbf{Z}[\alpha]$ tel que $\mathbf{Z}[\alpha]/(x)$ soit un corps à 2 ou 3 éléments. D'où un homomorphisme :

$$\varphi : \mathbf{Z}[\alpha] \longrightarrow \mathbf{K} \ \text{ avec } \ \mathbf{K} = \mathbf{F}_2 \ \text{ ou } \ \mathbf{K} = \mathbf{F}_3$$

dont la restriction à $\mathbf{Z}$ est la projection canonique. Alors $\beta = \varphi(\alpha)$ vérifie $\beta^2 - \beta + 5 = 0$ dans $\mathbf{K}$. Que ce soit dans $\mathbf{F}_2$ ou dans $\mathbf{F}_3$, il n'y a pas de solution. C'est absurde.

Proposition. *Soient $a, b \in \mathbf{Z}[\alpha] \notin \{0\}$. Il existe $q, r \in \mathbf{Z}[\alpha]$ avec :*

(i) $r = 0$ *ou* $N(r) < N(b)$

(ii) $a = bq + r$ *ou* $2a = bq + r$.

Preuve. Soit $x = \frac{a}{b} = \frac{a\bar{b}}{b\bar{b}} \in \mathbf{C}$ que l'on écrit $x = u + v\alpha$ avec $u, v \in \mathbf{Q}$. On note $n = \lfloor v \rfloor$. On distingue :

1. Si $v \notin]n + 1/3, n + 2/3[$, alors, soient s et t les entiers les plus proches de u et v respectivement, on a en posant $q = s + t\alpha$:
$$N(x - q) = (s - u)^2 + (s - u)(t - v) + 5(t - v)^2 \leq \frac{1}{4} + \frac{1}{2} \times \frac{1}{3} + \frac{5}{9} = \frac{35}{36} < 1.$$
et on a le résultat voulu en posant $r = a - bq = b(x - q)$.
2. Dans l'autre cas, on note que $2v \in]2n + 2/3, 2n + 1 + 1/3[$. Ainsi, en posant $m = \lfloor 2v \rfloor$, on a $2v \notin]m + 1/3, m + 2/3[$ et on est ramené au cas précédent : on a $2a = bq + r$ avec $N(r) < N(b)$.

□

On montre maintenant que $\mathbf{Z}[\alpha]$ est principal. On commence par voir que l'idéal (2) est maximal car
$$\mathbf{Z}[\alpha] \simeq \mathbf{Z}[T]/(T^2 - T + 5)$$
donc en vertu du théorème d'isomorphisme :
$$\mathbf{Z}[\alpha]/(2) \simeq (\mathbf{Z}/2\mathbf{Z})[T]/(T^2 + T + 1)$$
et la conclusion puisque $T^2 + T + 1$ est irréductible sur $\mathbf{F}_2$.

Ensuite, on prend $I \neq \{0\}$ un idéal de $\mathbf{Z}[\alpha]$ et $a \in I$ non nul de norme minimale. Si $I = (a)$ c'est fini, sinon prenons $x \in I \notin (a)$. On écrit la pseudo division euclidienne :

(i) Si $x = aq + r$ avec $N(r) < N(a)$ on a $r = 0$ et $x \in (a)$ c'est absurde.

(ii) Si $2x = aq + r$ avec $N(r) < N(a)$ on a $r = 0$ et $2x = aq$. Comme (2) est maximal donc premier, on a $a \in (2)$ ou $q \in (2)$. Le deuxième cas est impossible car il entrainerait $x \in (a)$. Donc $a = 2a'$ et $x = a'q \in (a')$. Mais (2) est maximal et ne contient pas q donc $(2, q) = \mathbf{Z}[\alpha]$ de sorte qu'on peut écrire
$$\lambda 2 + \mu q = 1 \quad \lambda, \mu \in \mathbf{Z}[\alpha].$$
On en déduit :
$$a' = \lambda 2a' + \mu q a' = \lambda a + \mu x$$
donc $a' \in I$ et on a une contradiction car $N(a') < N(2a') = N(a)$.

Référence. D. Perrin, *Cours d'Algèbre*