Un anneau principal non euclidien

Références : Perrin, *Cours d'algèbre*, partie II.5

Théorème.

On note $\alpha = \dfrac{1+i\sqrt{19}}{2}$ et $A = \mathbb{Z}[\alpha]$, alors A est un anneau principal, non-euclidien.

Démonstration. **Étape 1 :** α est racine de $P = T^2 - T + 5$, car $\alpha + \overline{\alpha} = 1$ et $\alpha\overline{\alpha} = 5$.
Ainsi, $A = \left\{a + b\alpha \middle| (a,b) \in \mathbb{Z}^2\right\}$ est un sous-anneau de $\mathbb{C}$. [1]
Donc A est intègre ; et comme $\overline{\alpha} = 1 - \alpha$, A est stable par conjugaison.
Pour $z = a + b\alpha \in A$, on définit la norme :

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

Alors $N(z) \in \mathbb{N}$ (en réduisant avec la méthode de Gauss), et $N(zz') = N(z)N(z')$.
De plus, $N(z) = 0 \Rightarrow \left(a + \dfrac{b}{2}\right)^2 + \dfrac{19}{4}b^2 = 0 \Rightarrow a = b = 0 \Rightarrow z = 0$.
Soit $z \in A^\times$, alors $N(z)N\left(z^{-1}\right) = 1$ donc $N(z) = 1$.
Alors $\left(a + \dfrac{b}{2}\right)^2 + \underbrace{\dfrac{19}{4}}_{>1} b^2 = 1$, donc $b = 0$ et $a = \pm 1$. Ainsi, $A^\times = \{\pm 1\}$.

Étape 2 : Supposons A euclidien, alors $\exists x \in A \backslash A^\times, \pi_{A/(x)}|_{A^\times \cup \{0\}}$ est surjective.
En particulier, $A/(x)$ est un corps (car des inversibles sont envoyés sur des inversibles) et $\#A/(x) \leqslant 3$, donc $A/(x) = K$, où $K \simeq \mathbb{F}_2$ ou $\mathbb{F}_3$.
On en déduit l'existence d'un morphisme d'anneaux surjectif $\varphi : A \to K$.
Alors $\beta = \varphi(\alpha)$ vérifie $\beta^2 - \beta + 5 = 0$.
Mais cette équation ne possède de solution ni dans $\mathbb{F}_2$, ni dans $\mathbb{F}_3$. [2]
On aboutit à une contradiction, et A n'est donc pas euclidien.

Étape 3 : On introduit une pseudo-division euclidienne.

Lemme.

Soient $a, b \in A\backslash\{0\}$.
Alors il existe $(q,r) \in A^2$, tels que :

1. $N(r) < N(b)$;
2. $a = bq + r$ ou $2a = bq + r$.

Démonstration. Soit $x = \dfrac{a}{b} \in \mathbb{C}$, qu'on écrit aussi $x = u + v\alpha$, où $u, v \in \mathbb{Q}$. On note $n = \lfloor v \rfloor$.

— Supposons que $v \notin \left]n + \dfrac{1}{3}, n + \dfrac{2}{3}\right[$; soient s et t les plus proches entiers de u et v.
Ainsi, $|s - u| \leqslant \dfrac{1}{2}$ et $|t - v| \leqslant \dfrac{1}{3}$.
On pose $q = s + t\alpha \in A$ et :

$$N(x-q) = (s-u)^2 + (s-u)(t-v) + 5(t-v)^2 \leqslant \frac{1}{4} + \frac{1}{6} + \frac{5}{9} = \frac{9+6+20}{36} = \frac{35}{36} < 1.$$

On pose $r = a - bq = b(x-q)$ et on a $N(r) < N(b)$.

1. Car A est un sous-groupe de $\mathbb{C}$, contient 1 et est stable par multiplication.
2. Cela se démontre facilement en cherchant de façon exhaustive.

— Supposons désormais que $v \in \left]n+\frac{1}{3}, n+\frac{2}{3}\right[$, alors $2x = 2u + 2v\alpha$ et $2v \in \left]2n+\frac{2}{3}, 2n+1+\frac{1}{3}\right[$ et on est ramené au cas précédent : on peut écrire $2a = bq + r$, avec $N(r) < N(b)$.

□

Étape 4 : Montrons que A est principal.

On a : $A \simeq \mathbb{Z}[T]/(P)$, donc $A/(2) \underset{3}{\simeq} \mathbb{Z}[T]/(2,P) \underset{4}{\simeq} \mathbb{F}_2[T]/(P)$.

Mais $T^2 - T + 5$ est irréductible sur $\mathbb{F}_2$ car de degré 2 sans racine ; donc $A/(2)$ est un corps et (2) est maximal dans A.
Soit $I \neq (0)$ un idéal de A, et soit $a \in I \backslash \{0\}$ de norme $N(a)$ minimale.
Soit $x \in I \backslash (a)$;

→ Si $x = aq + r$ avec $N(r) < N(a)$ ou $r = 0$, alors comme $r \in I$, par minimalité de $N(a)$, on a $r = 0$. Ainsi $x \in (a)$: contradiction.

→ Ainsi, $2x = aq + r$, et même $2x = aq$ en répétant le procédé qu'on vient à peine de faire.
Comme (2) est maximal, l'idéal (2) est premier, d'où $a \in (2)$ ou $q \in (2)$.
Si $q \in (2)$, alors $q = 2q'$ et $x = aq'$ (par intégrité) donc $x \in (a)$. Contradiction.
Donc $a \in (2)$, c'est à dire : $a = 2a'$.
Comme $q \notin (2)$ et (2) est maximal, on a : $(2, q) = A$, donc $\exists \lambda, \mu \in A, 2\lambda + q\mu = 1$.
Donc $a' = 2\lambda a' + q\mu a' = \lambda a + \mu x \in I$.
Or $0 < N(a') < N(a)$. Contradiction.

Ainsi, $I = (a)$ et A est principal.

□

À présent, prouvons le lemme utilisé.

Lemme.

Soit A un anneau euclidien, alors il existe $x \in A \setminus A^\times$ tel que $\pi_{A/(x)}|_{A^\times \cup \{0\}}$ est surjective.

Démonstration. Si A est un corps, on prend $x = 0$.
Sinon, on prend $x \in A \setminus (A^\times \cup \{0\})$ de stathme minimal parmi les éléments de $A \setminus (A^\times \cup \{0\})$ (existe car le stathme est à valeurs dans $\mathbb{N}$).
Le but est de trouver pour tout $a \in A$, un élément r de $A^\times \cup \{0\}$ tel que $a = r$ dans $A/(x)$. Pour cela on écrit la division euclidienne $a = xq + r$.
Si $r = 0$, c'est bon. Sinon on a $v(r) < v(x)$ donc r est inversible. □

Remarques : • Il est bon de connaître les contre-exemples classiques dans la théorie des anneaux.

— $\mathbb{Z}[i\sqrt{5}]$ est noethérien mais pas factoriel.
— $\mathbb{R}[X_1, X_2, ...]$ est factoriel mais pas noethérien.
— $\mathbb{Z}[X]$ est factoriel non principal.
— $\mathbb{Z}[X]/(2X)$ est noethérien non intègre.

• On peut trouver des rappels très clairs à l'adresse suivante :
`http://www.normalesup.org/~crenard/rappelsAnneaux.pdf`
• On peut montrer le même résultat pour $d = 43$, 67 et 163.

Adapté du travail de Florian Lemonnier.

3. Notons $\pi_P : \mathbb{Z}[T] \to \mathbb{Z}[T]/(P)$ et $\pi_{\overline{2}} : \mathbb{Z}[T]/(P) \to (\mathbb{Z}[T]/(P))/(\overline{2})$ les projections canoniques.
Ker $\pi_{\overline{2}} \circ \pi_P = \left\{f \in \mathbb{Z}[T] \middle| \exists u \in \mathbb{Z}[T], \overline{f} = \overline{2u}\right\} = \{f \in \mathbb{Z}[T] | \exists u, v \in \mathbb{Z}[T], f = 2u + Pv\} = (2, P)$.
Ainsi $\pi_{\overline{2}} \circ \pi_P$ induit un isomorphisme $\mathbb{Z}[T]/(2,P) \simeq (\mathbb{Z}[T]/(P))/(\overline{2}) \simeq A/(2)$.

4. Notons $\pi_2 : \mathbb{Z}[T] \to \mathbb{Z}[T]/(2)$ et $\pi_{\overline{P}} : \mathbb{Z}[T]/(2) \to (\mathbb{Z}[T]/(2))/(\overline{P})$ les projections canoniques.
Ker $\pi_{\overline{P}} \circ \pi_2 = \left\{f \in \mathbb{Z}[T] \middle| \exists u \in \mathbb{Z}[T], \overline{f} = \overline{Pu}\right\} = \{f \in \mathbb{Z}[T] | \exists u, v \in \mathbb{Z}[T], f = Pu + 2v\} = (2, P)$.
Ainsi $\pi_{\overline{P}} \circ \pi_2$ induit un isomorphisme $\mathbb{Z}[T]/(2,P) \simeq (\mathbb{Z}[T]/(2))/(\overline{P}) \simeq \mathbb{F}_2[T]/(P)$.