Un anneau principal non-euclidien

Un développement un peu classique est le théorème suivant :

Théorème 1. On pose $a := \frac{1}{2}(1 + i\sqrt{19})$. L'anneau $A := \mathbb{Z}[a]$ n'est pas euclidien et est principal.

On en trouve par exemple une preuve dans le Cours d'Algèbre de Perrin. Je trouve cependant que la preuve du fait que A n'est pas euclidien tombe un peu du ciel. L'objectif de ce document est de tenter d'éclairer un peu cette démonstration. Ma source principale est l'article suivant, dans lequel on pourra trouver d'autres résultats intéressants.

On prouvera même que cet anneau n'est pas euclidien en un sens plus général que la définition habituelle. On a pour cela besoin de la notion d'ordinaux, que je ne définirai pas ici. Si vous ne savez pas ce que c'est, remplacer les ordinaux par des entiers ou $\mathbb{N}$, ça devrait faire l'affaire. Commençons.

Définition 1. Un anneau intègre A est dit euclidien (en un sens généralisé) s'il existe un ordinal α et une application $\varphi : A \setminus \{0\} \to \alpha$ tels que pour tout $a, b \in A$, $a \neq 0$, il existe $q, r \in A$ tels que $b = aq + r$ et ($r = 0$ ou $\varphi(r) < \varphi(a)$).

On retombe sur la définition usuelle d'euclidien en autorisant uniquement $\mathbb{N}$ au lieu d'un ordinal quelconque. Les propriétés usuelles des anneaux euclidiens restent valables dans ce cadre plus général. Par exemple, ils sont principaux.

Définition 2. Soit A un anneau intègre. On définit par récurrence ordinale des parties de A de la manière suivante :

- $A_0 = \{0\} \cup A^*$
- $A_\gamma = \bigcup_{\beta<\gamma} A_\beta \cup \{a \in A | \forall b \in A, \exists q \in A, \exists r \in \bigcup_{\beta<\gamma} A_\beta, b = aq + r\}$
- (Si on se restreint aux entiers, on aurait pu définir : $A_{n+1} = A_n \cup \{a \in A | \forall b \in A, \exists q \in A, \exists r \in A_n, b = aq + r\}$).

Autrement dit, on commence à l'étape 0 par prendre 0 et tous les inversibles. Puis, à chaque étape, on rajoute les éléments a par lesquels on peut faire toutes les divisions euclidiennes ($b = aq + r$) avec des restes r déjà ajoutés ($r \in \bigcup_{\beta<\gamma} A_\beta$).

Proposition 1. Soit A un anneau intègre. Alors A est euclidien si et seulement s'il existe un ordinal α tel que $A = A_\alpha$. Dans ce cas, $\varphi : a \mapsto \min\{\gamma | a \in A_\gamma\}$ est un stathme sur A, et est le plus petit stathme sur A.

Démonstration. S'il existe α tel que $A = A_\alpha$, alors φ est bien défini. Montrons que c'est un stathme.

Soit $a \in A \setminus \{0\}$, $b \in A$. Essayons de faire la division euclidienne de b par a. Si $\varphi(a) = 0$, alors a est inversible, donc $b = aa^{-1}b + 0$. Si $\varphi(a) \neq 0$: on a $a \in A_{\varphi(a)} \setminus \bigcup_{\beta<\varphi(a)} A_\beta$ par minimalité de $\varphi(a)$, donc, par définition de $A_{\varphi(a)}$, il existe $q \in A$ et $r \in \bigcup_{\beta<\varphi(a)} A_\beta$ tel que $b = aq + r$. Comme $r \in \bigcup_{\beta<\varphi(a)} A_\beta$, on a $\varphi(r) < \varphi(a)$, ce qu'on souhaitait. Donc φ est bien un stathme.

Réciproquement, supposons que A est euclidien, et soit ψ un stathme. Soit $a \in A \setminus \{0\}$. On va montrer par récurrence sur $\psi(a)$ que $a \in A_{\psi(a)}$, ce qui impliquera qu'il existe γ tel que $A = A_\gamma$ et que $\varphi(a) \leq \psi(a)$.

Si $\psi(a) = 0$: la division euclidienne de 1 par a entraîne que a est inversible, donc $a \in A_0$.

Supposons $\psi(a) \neq 0$ et la propriété établie pour tout r tel que $\psi(r) < \psi(a)$. Alors pour tout $b \in A$, il existe q, r tel que $r = 0$ ou $\psi(r) < \psi(a)$ (donc $r \in A_{\psi(r)} \subseteq \bigcup_{\beta<\psi(a)} A_\beta$) tel que $b = aq + r$. Ainsi, a satisfait la définition de $A_{\psi(a)}$, donc $a \in A_{\psi(a)}$. □

Remarque 1. Pour $A = \mathbb{K}[X]$ avec $\mathbb{K}$ un corps, le stathme minimal obtenu est le degré. Pour $A = \mathbb{Z}$, on n'obtient pas la valeur absolue, mais $x \mapsto \lfloor \log_2(|x|) \rfloor$.

Cette caractérisation donne une manière de démontrer qu'un anneau n'est pas euclidien : on étudie les "couches" successives $A_0, A_1, \ldots$ Si on a $A_\beta = A_{\beta+1} \neq A$ pour un certain β, alors $A_\gamma = A_\beta \neq A$ pour tout $\gamma > \beta$, ce qui montrera que A n'est pas euclidien. Dans le cas qui nous intéresse ici, on a le résultat suivant :

Proposition 2. Avec $A = \mathbb{Z}[a]$, on a $A_0 = A_1 \neq A$, donc A n'est pas euclidien.

Démonstration. Tout d'abord, les inversibles de A sont -1 et 1, donc $A_0 = \{0, 1, -1\}$.

Soit $x \in A_1 \setminus A_0$. Par définition de A_1, tout élément de A est, modulo x, nul ou inversible. Autrement dit, $A/(x)$ est un corps et l'application canonique $A_0 \to A/(x)$ est surjective. Ainsi, $A/(x)$ est de cardinal 2 ou 3, donc isomorphe à $\mathbb{F}_2$ ou $\mathbb{F}_3$. Or a est racine de $X^2 - X + 5$, donc son image mod x aussi. Mais il n'y a pas de racine de $X^2 - X + 5$ dans $\mathbb{F}_2$ ou $\mathbb{F}_3$, absurde.

Donc $A_0 = A_1$, et A n'est pas euclidien. □

Sources :

- Transfinitely valued Euclidean domains have arbitrary indecomposable order type - Chris J. Conidis, Pace P. Nielsen and Vandy Tombs - https://arxiv.org/abs/1703.02631
- Cours d'algèbre - D. Perrin