

Étude de l'anneau $\mathbb{Z} \left[\frac{1+i\sqrt{19}}{2} \right]$

Leçons : 122

[Per], partie II.5

Théorème

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

Démonstration :

Étape 1 : α est racine de $P = T^2 - T + 5$, car $\alpha + \bar{\alpha} = 1$ et $\alpha\bar{\alpha} = 5$.

Ainsi, $A = \{a + b\alpha \mid (a, b) \in \mathbb{Z}^2\}$ est un sous-anneau de \mathbb{C} .¹

Donc A est intègre ; et comme $\bar{\alpha} = 1 - \alpha$, A est stable par conjugaison.

Pour $z = a + b\alpha \in A$, on définit la norme :

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

Alors $N(z) \in \mathbb{N}$, et $N(zz') = N(z)N(z')$.

De plus, $N(z) = 0 \Rightarrow \left(a + \frac{b}{2}\right)^2 + \frac{19}{4}b^2 = 0 \Rightarrow a = b = 0 \Rightarrow z = 0$.

Soit $z \in A^\times$, alors $N(z)N(z^{-1}) = 1$ donc $N(z) = 1$.

Alors $\underbrace{\left(a + \frac{b}{2}\right)^2}_{>1} + \frac{19}{4}b^2 = 1$, donc $b = 0$ et $a = \pm 1$. Ainsi, $A^\times = \{\pm 1\}$.

Étape 2 : Supposons A euclidien, alors $\exists x \in A \setminus A^\times, \pi_{A/(x)}|_{A^\times \cup \{0\}}$ est surjective.²

En particulier, $A/(x)$ est un corps et $\#A/(x) \leq 3$, 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 $\varphi : A \rightarrow K$.

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 .³

On aboutit à une contradiction, et A n'est donc pas euclidien.

Étape 3 : On introduit une "pseudo-division euclidienne".

Lemme

Soient $a, b \in A \setminus \{0\}$.

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 $x = \frac{a}{b} = \frac{ab}{N(b)} \in \mathbb{C}$, qu'on écrit aussi $x = u + v\alpha$, où $u, v \in \mathbb{Q}$. On note $n = \lfloor v \rfloor$.

– Supposons que $v \notin \left]n + \frac{1}{3}, n + \frac{2}{3}\right]$; soient s et t les plus proches entiers de u et v .

Ainsi, $|s - u| \leq \frac{1}{2}$ et $|t - v| \leq \frac{1}{3}$.

On pose $q = s + t\alpha \in A$ et :

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

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. La démonstration est dans le rappel sur les anneaux, en page ??.
3. 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 $A/(2) \simeq \mathbb{Z}[T]/(2, P) \simeq \mathbb{F}_2[T]/(P)$.

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 $a \in I \setminus \{0\}$ de norme $N(a)$ minimale.

Soit $x \in I \setminus (a)$;

→ 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 $x = aq'$ 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. ■

Références

[Per] D. PERRIN – *Cours d'algèbre*, Ellipses, 1996.

4. Notons $\pi_P : \mathbb{Z}[T] \rightarrow \mathbb{Z}[T]/(P)$ et $\pi_{\bar{2}} : \mathbb{Z}[T]/(P) \rightarrow (\mathbb{Z}[T]/(P))/(\bar{2})$ les projections canoniques.

$\text{Ker } \pi_{\bar{2}} \circ \pi_P = \{f \in \mathbb{Z}[T] \mid \exists u \in \mathbb{Z}[T], \bar{f} = \bar{2}u\} = \{f \in \mathbb{Z}[T] \mid \exists u, v \in \mathbb{Z}[T], f = 2u + Pv\} = (2, P)$.

Ainsi $\pi_{\bar{2}} \circ \pi_P$ induit un isomorphisme $\mathbb{Z}[T]/(2, P) \simeq (\mathbb{Z}[T]/(P))/(\bar{2}) \simeq A/(2)$.

5. Notons $\pi_2 : \mathbb{Z}[T] \rightarrow \mathbb{Z}[T]/(2)$ et $\pi_{\bar{P}} : \mathbb{Z}[T]/(2) \rightarrow (\mathbb{Z}[T]/(2))/(\bar{P})$ les projections canoniques.

$\text{Ker } \pi_{\bar{P}} \circ \pi_2 = \{f \in \mathbb{Z}[T] \mid \exists u \in \mathbb{Z}[T], \bar{f} = \bar{P}u\} = \{f \in \mathbb{Z}[T] \mid \exists u, v \in \mathbb{Z}[T], f = Pu + 2v\} = (2, P)$.

Ainsi $\pi_{\bar{P}} \circ \pi_2$ induit un isomorphisme $\mathbb{Z}[T]/(2, P) \simeq (\mathbb{Z}[T]/(2))/(\bar{P}) \simeq \mathbb{F}_2[T]/(P)$.