

* $\mathbb{Z}[\frac{1+i\sqrt{5}}{2}]$ est principal non euclidien: résons 122, 127

[Perrin, II.5]

$A = \mathbb{Z}[\alpha]$ est principal non euclidien, où $\alpha = \frac{1+i\sqrt{5}}{2}$

lemme 1:

Si B est un anneau euclidien, alors:

$\exists \pi: B \setminus B^* \rightarrow B^* \cup \{0\} : B^* \cup \{0\} \rightarrow B/(a)$ est surjective.

lemme 2:

On note $N: z \mapsto z\bar{z}$ la norme sur A .

$\forall a, b \in A \setminus \{0\}, \exists q, r \in A$ tq: 1) $r=0$ ou $N(r) < N(b)$

2) $a = bq + r$ ou $\bar{a} = b\bar{q} + \bar{r}$

premières remarques sur A :

$$\alpha + \bar{\alpha} = 1, \alpha\bar{\alpha} = 5, \alpha^2 - \alpha + 5 = 0 \rightsquigarrow A \simeq \mathbb{Z}[X]/(X^2 - X + 5)$$

$$\forall z \in A^* \Leftrightarrow N(z) = 1 \Leftrightarrow z = \pm 1 \quad (\text{car } N(a+ib) = a^2 + ab + 5b^2)$$

preuve du lemme 2:

Si B est un corps, $x=0$ convient.

Sinon, on choisit $x \in B \setminus B^* \cup \{0\}$ de valuation $v(x)$ minimal.

Soit $y \in B$, on peut écrire $y = qx + r$ avec $r=0$ ou $v(r) < v(x)$. Or, si $v(r) < v(x)$, alors, par minimalité de $v(x)$: $r \in B^*$.

$$\text{Ainsi: } y - qx = r \in B^* \cup \{0\}$$

□

preuve que A est non euclidien:

Supposons A euclidien. Soit α donné par le lemme 1

la projection canonique $\pi: A \rightarrow A/(\alpha)$ vérifie $\pi(A^* U(\alpha)) = A/(\alpha)$. Or, π envoie les éléments inversibles sur des éléments inversibles et donc $A/(\alpha)$ est un corps. Or, $A^* U(\alpha) = \{-1; 0; 1\}$ et donc:

$$|A/(\alpha)| \leq 3 \leadsto A/(\alpha) = K = \mathbb{F}_2 \text{ ou } \mathbb{F}_3$$

On a donc un morph. surjectif: $\pi: A = \mathbb{Z}[X] \rightarrow K$ et $\pi|_{\mathbb{Z}}$ est forcément la proj. can. $\mathbb{Z} \rightarrow \mathbb{F}_2$ ou $\mathbb{F}_3$ (car $1 \mapsto 1$). Ainsi, $\pi(\alpha)$ est une racine de $\pi(X^2 - X + 5) = \overline{X^2 - X + 5}$ dans K .

$$\text{Dans } \mathbb{F}_2: \overline{X^2 - X + 5} = X^2 + X + 1 \leadsto \text{pas de racine. } \nexists$$

$$\text{Dans } \mathbb{F}_3: \overline{X^2 - X + 5} = X^2 + 2X + 2 \leadsto \text{pas de racine. } \nexists$$

Ceci contredit donc notre hypothèse initiale.

preuve du lemme 2:

Notons $\frac{a}{b} = u + \alpha v$ avec $u, v \in \mathbb{Q}(\mathbb{R})$. Notons m un entier le plus proche de u et n un entier le plus proche de v .

$$\leadsto \frac{a}{b} = \underbrace{m + \alpha n}_{=: q \in A} + s + \alpha t \quad \text{avec} \quad |s|, |t| \leq \frac{1}{2}$$

$$\text{On a donc } a = bq + \underbrace{b(s + \alpha t)}_{=: r \in A} \quad \text{et} \quad N(r) = N(b) |s + \alpha t|^2 = (s^2 + st + 5t^2) N(b)$$

$$\bullet \text{ Si } |t| \leq \frac{1}{3}: |s + \alpha t|^2 \leq \frac{1}{4} + \frac{1}{6} + \frac{5}{9} = \frac{9+6+20}{36} = \frac{35}{36} < 1$$

Donc: $N(r) < N(b)$, ce qui permet de conclure

$$\bullet \text{ Sinon: } |t| > \frac{1}{3}, \text{ et ainsi: } 2t = \pm 1 + t' \text{ avec } |t'| \leq \frac{1}{3}.$$

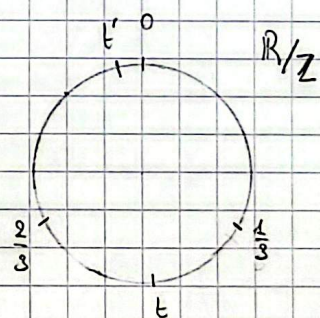
$$\text{Donc: } 2a = bq' + b(s' + \alpha t') \text{ avec } |s'| \leq \frac{1}{2} \text{ et } |t'| \leq \frac{1}{3}$$

$\leadsto$ On est dans le 1^{er} cas et donc: $r' = b(s' + \alpha t')$ vérifie $N(r') < N(b)$. On conclut donc également dans ce cas $\square$.

preuve que A est principal:

• On montre tout d'abord que (2) est maximal dans A.

$$\text{On a } A = \mathbb{Z}[X] \simeq \mathbb{Z}[X] / (X^2 - X + 5)$$



Ainsi, par le 3^e (?) th d'iso :

$$A/(2) \simeq (\mathbb{Z}[X]/(P))/(2) \simeq \mathbb{Z}[X]/(P, 2) \simeq (\mathbb{Z}[X]/(2))/(P) \simeq \mathbb{F}_2[X]/(P)$$

Or, on a déjà vu que $P = X^2 + X + 1$ dans $\mathbb{F}_2[X]$ et n'a donc pas de racine dans $\mathbb{F}_2$. Ainsi, P est irréductible dans $\mathbb{F}_2[X]$ et donc : $\mathbb{F}_2[X]/(P)$ est un corps.

→ $A/(2)$ est un corps → (2) est max. dans A .

• Soit I un idéal non trivial de A .

Soit $\alpha \in I \setminus \{0\}$ tq $N(\alpha)$ soit minimal. Montrons que $I = (\alpha)$.

Supposons que ce ne soit pas le cas, soit $y \in I \setminus (\alpha)$.

Par le lemme 2 : y ou $2y = q\alpha + r$ avec $N(r) < N(\alpha)$.

Or, $y, 2y, q\alpha \in I$ donc $r \in I$. Par minimalité de $N(\alpha)$: $r = 0$.

Donc : $y = q\alpha$ ou $2y = q\alpha$.

Or, par hypothèse : $y \notin (\alpha)$, donc : $2y = q\alpha$. (*)

En particulier : $q\alpha \in (2)$, idéal maximal donc premier, et donc : $q \in (2)$ ou $\alpha \in (2)$.

- Si $q = 2q' \in (2)$, alors, en simplifiant dans (*) (car A intègre) : $y = q'\alpha$, ce qui constitue encore une contradiction.

On en déduit : $\alpha = 2\alpha' \in (2)$ et $q \notin (2)$.

En simplifiant dans (*): $y = q\alpha'$.

Or, $q \notin (2)$ et (2) maximal donc $(2, q) = A$.

Ainsi, $\exists u, v \in A$ tq $1 = 2u + qv$.

On a donc : $vy = vq\alpha' = \alpha' - 2u\alpha' = \alpha' - u\alpha$, et donc : $\alpha' = vy + u\alpha \in I$.

Or : $N(\alpha) = N(2\alpha') = 4N(\alpha')$ donc $N(\alpha') < N(\alpha)$ et $\alpha' \in I \setminus \{0\}$: absurde.

Donc : $I = (\alpha)$.