$\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ [Pea] p 55

On note $\alpha := \frac{1+i\sqrt{19}}{2}$

$A := \mathbb{Z}[\alpha] = \{a+b\alpha \mid a,b \in \mathbb{Z}\}$

$N : A \longrightarrow \mathbb{N}$

$z = a+b\alpha \mapsto z\bar{z} = a^2+ab+5b^2$

Prop (pseudo div eucl) : Soit $a,b \in A\setminus\{0\}$.
Il existe alors $q,r \in A$ tq $a = bq+r$ ou $2a = bq+r$ avec $N(r) < N(b)$.

Rém :
On considère $x = \frac{a}{b}$ que l'on écrit $x = u+v\alpha$ avec $u,v \in \mathbb{Q}$

$\left(x = \frac{a}{b} = \frac{a\bar{b}}{b\bar{b}} = \frac{1}{N(b)}\, a\bar{b}$ mais A est stable par conj donc $a\bar{b} \in A\right)$

1er cas : $v \notin \left]\lfloor v \rfloor + \frac{1}{3}, \lfloor v \rfloor + \frac{2}{3}\right[$.

Alors, les entiers s et t les + proches de u et v resp^t vérifient $|s-u| \leq \frac{1}{2}$ et $|t-v| \leq \frac{1}{3}$.

Par suite, $q := s+t\alpha$ vérifie $N(x-q) = (u-s)^2+(u-s)(v-t)+5(v-t)^2$

$\leq \frac{1}{4}+\frac{1}{6}+\frac{5}{9}$

< 1

donc $r := a-bq = b(x-q)$ vérifie $N(r) < N(b)$ et donc q,r conviennent.

2ème cas : $v \in \left]\lfloor v \rfloor + \frac{1}{3}, \lfloor v \rfloor + \frac{2}{3}\right[$.

Alors, $2v \in \left]2\lfloor v \rfloor + \frac{2}{3}, 2\lfloor v \rfloor + 1 + \frac{1}{3}\right[$ donc $2v \notin \left]\lfloor 2v \rfloor + \frac{1}{3}, \lfloor 2v \rfloor + \frac{2}{3}\right[$

$\left(\text{si } v \in \left[\lfloor v \rfloor, \lfloor v \rfloor + \frac{1}{2}\right[, \lfloor 2v \rfloor = 2\lfloor v \rfloor \text{ et si } v \in \left[\lfloor v \rfloor + \frac{1}{2}, \lfloor v \rfloor + 1\right[, \lfloor 2v \rfloor = 2\lfloor v \rfloor + 1\right)$

et donc il existe $q, r \in A$ tq $2a = bq + r$ avec $N(r) < N(b)$
moyennant le 1er cas (on considère $2x = \frac{2a}{b} = 2u + 2v\alpha$)

Prop : A est un anneau principal.

Dém :
Soit I un idéal de A.
OPS $I \neq \{0\}$ (sinon, $I = (0)$) donc il existe $a \in I \setminus \{0\}$ tq $N(a)$ soit minimal.
Par l'abs, on supp que $I \neq (a)$.
Il existe alors $x \in I \setminus (a)$.
On effectue la pseudo div eucl de x par a :
Si $x = aq + r$, $r = 0$ par minimalité de $N(a)$ ($r \in I$ et $N(r) < N(a)$) donc $x \in (a)$ ↯
Par suite, $2x = aq + r$ mais $r = 0$ par min de $N(a)$ donc $aq \in (2)$.
Rq : (2) est max.
En effet, $A/(2) \simeq \mathbb{Z}[T]/(2, T^2 - T + 5)$
($\mathbb{Z}[T] \xrightarrow{\text{évalenα}} A \xrightarrow{\text{proj}} A/(2)$ est un morph surj de noyau $(2, T^2 - T + 5)$
et $\mathbb{Z}[T]/(2, T^2 - T + 5) \simeq (\mathbb{Z}/2\mathbb{Z})[T]/(T^2 + T + 1)$
($\mathbb{Z}[T] \xrightarrow{\text{réd}} (\mathbb{Z}/2\mathbb{Z})[T] \xrightarrow{\text{proj}} (\mathbb{Z}/2\mathbb{Z})[T]/(T^2 + T + 1)$ est un morph surj de noyau $(2, T^2 - T + 5)$)
donc $A/(2) \simeq (\mathbb{Z}/2\mathbb{Z})[T]/(T^2 + T + 1)$ mais $T^2 + T + 1$ est irréd ds l'anneau principal $(\mathbb{Z}/2\mathbb{Z})[T]$ donc $(T^2 + T + 1)$ est max et donc le quotient est un corps d'où la rq.

Eq, (2) est 1^{er} donc $a \in (2)$ ou $q \in (2)$.
Si $q \in (2)$, $q = 2q'$ donc $2x = 2aq'$ et donc $x \in (a)$ ↯.
Par suite, $a \in (2)$ donc $a = 2a'$ et $x = a'q$.
Il suffit de mq $a' \in I$ ce qui contredira la min de $N(a)$.
Or, $A = (2, q)$ ((2) est max et ne contient pas q)
donc $1 = \lambda 2 + \mu q$ et donc $a' = \lambda 2a' + \mu a'q = \lambda a + \mu x \in I$