

Remarque du devoir surveillé

I/1° a) Il suffit de montrer que $A(\sqrt{m})$ est un sous-anneau de B .

$A(\sqrt{m}) \neq \emptyset$: stable par $+$ et $(\cdot)$ et par $\times$: $(a+b\alpha)(a'+b'\alpha) = aa' + bb'\alpha^2 + (ab'+a'b)\alpha$

$1 \in A(\sqrt{m})$ c.q.f.d.

b). Il faut l'hypothèse supplémentaire : $A \cap A' = \{0\}$: dans ce cas :

$$a+b\alpha = a'+b'\alpha \Rightarrow \begin{matrix} a=a' \\ b=b' \end{matrix} \text{ car } \begin{matrix} a-a' = (b'-b)\alpha \\ a=a' \end{matrix} \Rightarrow \begin{matrix} a=a' \\ b=b' \end{matrix} \text{ et } (b'-b)^2 m = 0 \Rightarrow (b'-b)^2 = 0 \Rightarrow b=b'$$

2° a). On a : $\overline{u+v} = \bar{u} + \bar{v}$ et $\overline{uv} = \bar{u} \cdot \bar{v}$ puis $u \mapsto \bar{u}$ involutif (donc bijectif).

b). $N(u) = a^2 - b^2 \alpha^2 \in A$. $N(uv) = uv \cdot \bar{u}\bar{v} = u\bar{u} \cdot v\bar{v} = N(u)N(v)$.

c). u inversible $\Rightarrow N(uu^{-1}) = N(u)N(u^{-1}) = 1 \Rightarrow N(u^{-1}) = N(u)^{-1}$ inversible !

Si $N(u)$ est inversible alors : $u \cdot \bar{u} = N(u) \Rightarrow u^{-1} = \bar{u} \cdot (N(u))^{-1}$

(il ne faut pas oublier que B est commutatif).

II 1° a). $u \in \mathbb{Z}(i)^* \Leftrightarrow N(u) \in \mathbb{Z}^* : u = a+ib \cdot N(u) = a^2+b^2 = 1$

donc : $a = \pm 1, b = 0$ ou $b = \pm 1, a = 0$: 4 possibilités

b). Si $\pi = u \cdot v \Rightarrow N(u) = N(u)N(v)$, or, comme $N(u)$ est premier : $\Rightarrow N(u) = 1$ ou $N(v) = 1 \Rightarrow u$ ou v inversibles (I. 2° c).

2° a). On a : $\frac{\pi}{y} = u_0 + i v_0 + (u-u_0) + (v-v_0)i \Rightarrow \pi = (u_0 + i v_0) \cdot y + \underbrace{[(u-u_0) + i(v-v_0)] y}_{= r}$

Or : $r \in \mathbb{Z}(i)$ car : $r = \pi - (u_0 + i v_0) y$.

et d'autre part : $N(r) = N(y) \cdot N[(u-u_0) + i(v-v_0)] = N(y) [(u-u_0)^2 + (v-v_0)^2]$

$(u-u_0)^2 \leq \frac{1}{4}$ et $(v-v_0)^2 \leq \frac{1}{4} \Rightarrow N(r) \leq \frac{1}{2} N(y)$.

On aura unicité car il n'y a qu'un seul entier u_0 tel que $|u-u_0| \leq \frac{1}{2}$ et de même pour v .

$\Leftrightarrow u \neq [u] + \frac{1}{2}$ et $v \neq [v] + \frac{1}{2}$.

Si l'une de ces 2 conditions n'est pas vérifiée, on aura 2 choix ou 4 choix dans le cas le plus favorable : i.e. $u = [u] + \frac{1}{2}, v = [v] + \frac{1}{2}$

b). $\{N(u), u \in \mathbb{Z}, u \neq 0\}$ est un sous-ensemble de $\mathbb{N}$ non vide, il possède donc un plus petit élément : $N(d)$.

Si $u \in \mathbb{Z}$ alors : $u = d\alpha + r$ avec $N(r) \leq \frac{1}{2} N(d)$ donc, $N(r) = 0$

et on peut conclure : $\mathbb{Z} = (d)$. c.q.f.d.

3° a). On a : $5 = (2+i)(2-i)$; $13 = (3+2i)(3-2i)$ et $17 = (4+i)(4-i)$.

b) $\Leftrightarrow$ on a : $p = (a+ib)(a-ib) = u \cdot \bar{u}$ avec $N(u) = p \neq 1$.

$\Rightarrow$: p réductible $\Rightarrow p = (u+iv)(u'+iv') \Rightarrow \begin{cases} u'+iv' = \frac{p}{u+iv} (u-iv) \\ \text{et } p^2 = (u^2+v^2)(u'^2+v'^2) \end{cases}$
donc $u' = \frac{p}{u^2+v^2} u$ $\Leftrightarrow \begin{cases} u'(u^2+v^2) = pu \\ v'(u^2+v^2) = -pv \end{cases}$
 $v' = \frac{-p}{u^2+v^2} v$ donc : $p \mid u^2+v^2$ ou $p \mid u'^2+v'^2$ on suppose $p \mid u^2+v^2$ i.e. $u^2+v^2 = kp$

$u = ku'$
 $v = -kv'$ $\Rightarrow p = k(u'-iv')(u'+iv') = k(u^2+v^2)$.

Conclusion : si $k = 1$, on a bien le résultat.

si $k \neq 1 \Rightarrow u'^2+v'^2 = 1$ or on a supposé $u+iv$ et $u'+iv'$ non inversible : c.q.f.d.

