Pierre Lissy

April 29, 2010

On note $\alpha := (1 + i^s qrt(19))/2$. D'abord, montrons que A n'est pas euclidien. Pour cela, utilisons un lemme.

Lemme 1. *On considère un anneau euclidien. Alors il existe un x non inversible tel que la restricition de la projection canonique sur $A/(x)$ à $A* \cup 0$ soit surjective.*

Proof. si A est un corps, 0 convient. Sinon, on choisit parmi les éléments de A non nuls et non inversibles un élément de valuation minimale. Si $a \in A$, alors on a par division euclidienne $a = xq + r$ avec $v(r) < 0$ ou $r = 0$. Mais comme x est de valuation minimale, soit r est inversible, soit $r = 0$. Ainsi, modulo x, tout élément de A est bien inversible ou nul. □

On en déduit le fait que $Z[\alpha]$ est non euclidien. En effet, on remarque que cet anneau est stable par conjugaison puisque $\bar{a}lpha = -\alpha + 1$. On s'intéresse alors à la norme arithmétique sur cette anneau: $N(z = a + b\alpha) = z\bar{z} = a^2 + ab + 5b^2$. Elle nous permet de trouver les inversibles. En effet, un inversible est tel que $N(zz^{-1}) = 1$, ce qui implique que $N(z)$ est inversible dans l'anneau Z. Ainsi on a par positivité nécessairement $N(z) = 1$, et on voit trivialement que ceci implique b=0 et $a = 1$ pu -1. Ces éléments étant clairemetn inversibles, c'est l'ensemble des inversibles. A partir de là, on conclut en raisonnant par l'absurde. Supposons qu'on est un morphisme surjectif de notre ensemble sur $A/(x)$. Comme A n'est pas un corps ici, $A/(x)$ est isomorphe à Z_2 ou Z_3. A fortiori o na un morphisme surjectif de A dans Z_2 ou Z_3. Mais on a que α vérifie dans A l'équation $\alpha^2 - \alpha + 5 = 0$, en passant ceci dans Z_2 on obtient qu'il existerait une solution de $X^2 + X + 1 = 0$ ce qui est faux, et modulo 3 de $X^2 - X - 1 = 0$, ce qui est aussi faux.

Montrons maintenant le caractère principale.

Lemme 2 (Division pseudo euclidienne)**.** *On considère deux éléments non nuls a et b. Alors il existe q et r tels que*

1. *$r = 0$ ou $N(r) < N(b)$*
2. *$a = bq + r$ ou $2a = bq + r$*

Proof. Posons x l'élement de $\mathbb{C}$ égal $a/b = a\bar{b}/|b|^2$. On l'écrit sous la forme $u + \alpha v$ avec u et v des rationnels. On pose n la partie entière de v. De deux choses l'une.

1. v n'est pas dans $(n + 1/3, n + 2/3)$. Notons s et t les entiers les plus proches de u et v. Alors $|s - u| \leqslant 1/2$ et $|s - t| \leqslant 1/3$. Donc si l'on psoe $q = s + t\alpha$, on a $q = \in A$ et donc $N(x-q) = (s-u)^2+(s-u)(t-v)+5(t-v)^2 \leqslant 1/4+1/12+5/9 = (20+12+3)/36 = 35/36 < 1$. D'où $N(a - qb) < N(b)$, ce qui est le résultat voulu.

2. v est dans cet intervalle. On remarque alors que si m est la partie entière de $2v$, il n'est pas dans $(n + 1/3, n + 2/3)$, on est ramené au cas précédent: $2a = bq + r$ avec les conditions voulues

□

Lemme 3. *L'idéal (2) est maximal. En effet, par théorème d'isomorphisme des anneaux, on A d'abord $Z[\alpha] \simeq Z[T]/(T^2 - T + 5)$. Ensuite, en considérant $\varphi : a + b\alpha \mapsto a + bX + (2, X^2 - X + 5)$,on a $Z[\alpha]/(2) \simeq Z[T]/(2, T^2 - T + 5)$ puis enfin en considérant le morphisme $P \in Z_2[X] \mapsto P + (2, T^2 + T + 1)$ on voit que $A/(2) \simeq Z_2/(T^2 + T + 1)$. Or comme le polynôme $T^2 + T + 1$ est irréductible le membrede droite est un corps donc celui d gauche auss, ie (2) est maximal.*

On peut maintenant conclure. Soit I un idéal et a un élément de I de norme minimale (par mi les éléments non nuls). Si $I = (a)$ alors c'est fini, sinon effectuons la pseudo-division de $x \in I/\{(a)\}$. $x = aq + r$ est impossible car comme a est de norme minimale ceci implique $r = 0$ et a divise x, ce qui est faux par hypothèse. O na donc$2x = aq + r$ et pour la même raison $r = 0$, ainsi $2x = aq$,ie $aq \in (2)$. Mais l'idéal (2) est maximal donc $a \in (2)$ ou $q \in (2)$. Dans ce dernier cas on a $q = 2q'$ et par intégrité $x = aq'$, faux par hypothèse. Donc $a \in (2)$, on a donc $a = 2a'$ et $x = a'q$. ontrons que $a' \in I$. En effet, comme (2) est maximal l'anneau engendré par 2 et q vaut A tout entier. O na donc une relatio nde Bézout $2\lambda + q\mu = 1$. D'où $a' = 2\lambda a' + \mu q a' = \lambda a + \mu x$.