Université Claude Bernard Lyon 1

MASTER M1G

Algèbre

Correction de l'examen du 8 janvier 2016

Exercice 1

On va regarder ce polynôme P comme un polynôme sur l'anneau factoriel $A[X]$, où $A := \mathbb{C}[Y]$. Comme A est factoriel, il suffit de montrer que P est de contenu 1 et irréductible sur $\mathbb{K}[X]$, avec $\mathbb{K} := \mathbb{C}(Y)$. Son contenu est égal à $PGCD(1, Y^2 - 1) = 1$.

Maintenant, pour montrer que P est irréductible sur $\mathbb{K}[X]$, il suffit de voir qu'il n'a pas de racine dans $\mathbb{K}$, puisqu'il est de degré 2. Or, P est unitaire, donc, toute racine dans $\mathbb{K}$ est une racine dans A (car A est factoriel). Supposons par l'absurde que $Q \in \mathbb{C}[Y]$ soit une racine de P. On aurait $Q(Y)^2 = 1 - Y^2$. Donc, Q serait un polynôme de degré 1 ; de la forme $aY + b$, avec $a, b \in \mathbb{C}$. Par identification, l'égalité donne alors

$$a^2 = -1,\ 2ab = 0,\ b^2 = 1,$$

ce qui est vite vu comme absurde, en caractéristique différente de 2.

Exercice 2. *Question de cours*

Soit α une racine de P dans une extension algébrique de $\mathbb{K}$. Comme P est irréductible, on sait que $[\mathbb{K}(\alpha) : \mathbb{K}] = n$. Si on montre que $[\mathbb{L}(\alpha) : \mathbb{L}] = n$, alors, P sera irréductible sur $\mathbb{L}$. Effectivement, on aura que le polynôme minimal de α sur $\mathbb{L}$ sera de degré n et divisera P, et donc, ce polynôme minimal sera égal à P. On obtient que P sera bien irréductible.

D'après le raisonnement qui précède, on a déjà l'inégalité $[\mathbb{L}(\alpha) : \mathbb{L}] \leq \deg(P) = n$.

Montrons l'inégalité inverse. Posons $[\mathbb{L}(\alpha) : \mathbb{K}(\alpha)] =: x$ et $[\mathbb{L}(\alpha) : \mathbb{L}] = y$. Par le théorème de la base téléscopique, on a

$$xn = [\mathbb{L}(\alpha) : \mathbb{K}] = ym.$$

Comme n et m sont premiers entre eux, n divise y, ce qui prouve l'inégalité inverse, comme désiré.

Exercice 3.

1. L'évaluation en $X = i\sqrt{3}$ donne un morphisme surjectif d'anneaux de $\mathbb{Z}[X]$ vers A qui a pour noyau l'idéal $(X^2 + 3)\mathbb{Z}[X]$. Effectivement, si l'on note K ce noyau, on a bien évidemment $(X^2 + 3)\mathbb{Z}[X] \subset K$. Réciproquement, comme $(X^2 + 3)$ est irréductible sur $\mathbb{Q}$, c'est le polynôme minimal de $i\sqrt{3}$ sur $\mathbb{Q}$. Donc, $K \subset \mathbb{Z}[X] \cap (X^2 + 3)\mathbb{Q}[X]$. Montrons donc que $\mathbb{Z}[X] \cap (X^2 + 3)\mathbb{Q}[X] \subset (X^2 + 3)\mathbb{Z}[X]$. Soit P dans $\mathbb{Z}[X]$ qui se décompose en $P = (X^2+3)R$, avec $R \in \mathbb{Q}[X]$. Alors, $R = \frac{a}{b}R_0$, avec $R_0 \in \mathbb{Z}[X]$ de contenu 1, et $a, b \in \mathbb{Z}$. On a donc $bP = a(X^2 + 3)R_0$, et, en prenant le contenu, il vient $bc(P) = a$. Donc b divise a et $R \in \mathbb{Z}[X]$, comme voulu.

   On vient de montrer l'isomorphisme $\mathbb{Z}[i\sqrt{3}] \simeq \mathbb{Z}[X]/(X^2 + 3)$. Maintenant, posons $B = \mathbb{Z}[X]$, $I = (X^2 + 3)$, $J = (X^2 + 3, 2)$. En utilisant l'isomorphisme naturel $(B/I)/(J/I) \simeq B/J$, il vient que $\mathbb{Z}[i\sqrt{3}]/(2) \simeq \mathbb{Z}[X]/(X^2 + 3, 2)$. De même, on obtient $\mathbb{F}_2[X]/(X^2 + 3) \simeq \mathbb{Z}[X]/(X^2 + 3, 2)$. Or, sur le corps $\mathbb{F}_2$, $X^2 + 3 = X^2 + 1 = (X + 1)^2$, qui n'est donc pas irréductible. Donc, l'anneau $\mathbb{F}_2[X]/(X^2 + 3)$ n'est pas intègre, et ainsi, $A/(2)$, qui lui est isomorphe, n'est pas intègre.

2. Il vient de la question ci-dessus que 2 n'est pas premier dans A. Or, 2 est irréductible. Pour le voir, on suppose $2 = ab$, avec a et b non inversibles (donc de norme > 1). Alors, en prenant la norme, on voit que $4 = N(a)N(b)$. Donc $N(a) = N(b) = 2$. Or, $x^2 + 3y^2 = 2$ n'a pas de solutions entières (par exemple, réduire modulo 3), et donc 2 est irréductible. Dans un anneau factoriel, tout irréductible est premier ; l'anneau A n'est pas factoriel.

Problème.

A.

1. On suppose, par l'absurde, que $\alpha \in \mathbb{Q}$. Alors $\alpha = \frac{a}{b}$, avec a et b entiers, et donc $2b^2p = a^2$. Comme p est impair (il est congru à -3 modulo 8), il est différent de 2. Donc, la p-valuation du membre de gauche est impaire, alors que la p-valuation du membre de droite est paire. Absurde.
2. Tout élément de C s'écrit sous la forme $P(\alpha)$, avec $P \in \mathbb{Z}[X]$. Comme X^2-2p est unitaire, la division euclidienne de P par X^2-2p reste dans $\mathbb{Z}[X]$. Donc, $P = (X^2-2p)Q(X)+(aX+b)$, avec $a, b \in \mathbb{Z}$. Ce qui implique l'existence, en évaluant en α.
   Montrons l'unicité. Si $a + b\alpha = a' + b'\alpha$, alors $(b' - b)\alpha = a - a'$. Or, α n'est pas rationnel, donc forcément, $b' = b$ et $a' = a$.
3. Tout élément de K s'écrit donc sous la forme $\frac{a+b\alpha}{a'+b'\alpha}$, avec $a, a', b, b' \in \mathbb{Z}$. En multipliant par la forme conjuguée, il vient
$$\frac{a + b\alpha}{a' + b'\alpha} = \frac{(a + b\alpha)(a' - b'\alpha)}{a'^2 - 2pb'^2},$$
   qui se met clairement sous la forme voulue $x + y\alpha$, avec $x, y \in \mathbb{Q}$.
   L'unicité est analogue à la question précédente.
4. (a) On pose $k = x + y\alpha$, et $k' = x' + y'\alpha$. Le membre de gauche vaut $|(xx' + 2pyy')^2 - 2p(xy' + x'y)^2|$. Le membre de droite vaut $|(x^2 - 2py^2)(x'^2 - 2py'^2)|$. On voit que ces deux termes sont égaux.
   (b) On pose $c = a + b\alpha$, avec $a, b \in \mathbb{Z}$. Il vient que $N(c) = |a^2 - 2pb^2| \in \mathbb{N}$.
   Si $N(c) = 0$, alors $a^2 - 2pb^2 = 0$, ce qui implique $(a - b\alpha)(a + b\alpha) = 0$, et donc $a = b = 0$ car α est irrationnel.
   (c) Si u est inversible, alors $uu' = 1$ pour un u' de C. En prenant la norme, et en utilisant les deux items qui précèdent, il vient $N(u) = 1$. Réciproquement, si $u = a + b\alpha \in C$ est de norme 1, alors $\pm 1 = (a + b\alpha)(a - b\alpha)$, et donc u est inversible dans C.

B.

1. Comme C est principal, il est factoriel. Donc, on peut toujours décomposer k en une fraction d'éléments de C sans facteurs premiers communs.
2. Comme C est principal, l'idéal engendré par γ et β est principal : $(\gamma, \beta) = (\delta)$, pour un δ de C. Or, δ divise γ et β, par hypothèses. Donc, δ est unitaire ; il peut être pris égal à 1, et on a ainsi l'existence de u et v.
3. Si $k \notin C$, alors β n'est pas unitaire, et donc $N(\beta) > 1$. On a, de plus, $u\gamma - v\beta = 1$, donc $\beta(uk - v) = 1$. En prenant la norme, il vient donc $N(uk - v) < 1$.
   Montrons l'inégalité $N(uk - v) > 0$. Par l'absurde, on aurait $N(uk - v) = 0$ et donc $uk - v = 0$, c'est-à-dire $u\gamma - v\beta = 0$, d'où $1 = 0$. Absurde.

C.

1. On a clairement $k \in \mathbb{K}$. Supposons $k \in C$, alors $\frac{\alpha}{2} = a + b\alpha$, avec $a, b \in \mathbb{Z}$, ce qui est en contradiction avec l'unicité prouvée en A.3.
2. On voit par un calcul simple, que $ku - v = (py - z) + \alpha(\frac{x}{2} - t)$. Sa norme vaut donc
$$N(ku - v) = |(py - z)^2 - 2p(\frac{x}{2} - t)^2| = \frac{1}{2}|2(py - z)^2 - p(x - 2t)^2|.$$
D'où le résultat.
3. L'inégalité précédente force l'égalité $|2(py - z)^2 - p(x - 2t)^2| = 1$ et donc, $2(py - z)^2 - p(x - 2t)^2 = \pm 1$. En réduisant modulo p, on obtient bien l'égalité souhaitée.

D.

1. On a
$$\left(\frac{-2}{p}\right) = (-2)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} 2^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p^2-1}{8}}.$$
2. Comme, par hypothèses, p est congru à -3 modulo 8, il vient $p = -3 + 8a$, avec $a \in \mathbb{Z}$. Donc, $\frac{p-1}{2} = -2 + 4a$ est pair, et $\frac{p^2-1}{8} = 1 - 6a + 8a^2$ est impair.
Il vient donc
$$\left(\frac{2}{p}\right) = -1, \left(\frac{-2}{p}\right) = -1.$$
En conclusion, 2 et -2 ne sont pas des carrés modulo p.
3. Si C était principal, on aurait que $\bar{2}\bar{z}^2 = \pm\bar{1}$, et donc soit $\bar{2}$, soit $-\bar{2}$ serait un carré (le carré de $\frac{1}{\bar{z}}$). Absurde. Donc, C n'est pas principal.