Contrôle du 26/10/2016

Exercice 1 :
Soit k un corps. On considère le morphisme d'anneaux

$$\varphi \ : \ k[Y,T] \ \to \ k[X] \tag{1}$$

défini par $\varphi(P(Y,T)) = P(X^2, X^3)$. Notons A l'image de φ.

1. A est-il intègre ?
2. Donner une expression explicite des éléments de A et en déduire que $A \neq k[X]$;
3. Calculer les inversibles de A ;
4. Montrer que X^2 et X^3 sont irréductibles dans A ;
5. En déduire que A n'est pas factoriel.

Exercice 2 :

1. Montrer que le polynôme $X^3 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$;
2. Montrer que le polynôme $X^4 + X^3 + X - 1$ n'a pas de racines dans $\mathbb{F}_3$;
3. Déduire des points précédents que $P = X^4 + 4X^3 + 3X^2 + 7X - 4 \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$.

Exercice 3 :
Soit A l'anneau $A = \mathbb{Z}[i\sqrt{3}]$, dont les éléments sont les réels qui s'écrivent (forcement de manière unique) comme $a + bi\sqrt{3}$, avec $a, b \in \mathbb{Z}$.

Notons également par B l'anneau $B = \mathbb{Z}[j]$ où j est la racine cubique complexe primitive de l'unité $j = \frac{-1+i\sqrt{3}}{2}$. Les éléments de B s'écrivent de manière unique comme $a + bj$, avec $a, b \in \mathbb{Z}$.

Nous allons accepter le fait que B est Euclidien. Soit p un nombre premier de $\mathbb{N}$.

1. Montrer que j est racine de $X^2 + X + 1$.
2. Montrer que si $p \neq 2, 3$ s'écrit sous la forme $p = a^2 + 3b^2$, avec $a, b \in \mathbb{Z}$, alors $p \equiv 1 \pmod 3$.

On suppose désormais que $p \neq 2, 3$ et que $p \equiv 1 \pmod 3$. Nous rappelons que le groupe $\mathbb{F}_p^\times$ des inversibles du corps $\mathbb{F}_p$ est cyclique (isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$). **T.S.V.P.**

3. Montrer que $\mathbb{F}_p^\times$ admet un élément d'ordre 3.
4. Utiliser l'élément d'ordre 3 de $\mathbb{F}_p^\times$ pour montrer que le polynôme $X^2 + X + 1$ admet une racine dans $\mathbb{F}_p$.
5. Montrer que A est contenu dans B, et montrer qu'un élément $\alpha = x + jy$ de B est dans A si et seulement si y est pair.
6. Montrer que si α est dans B alors au moins un élément dans l'ensemble $\{\alpha, j\alpha, j^2\alpha\}$ est dans A.
7. Montrer que p est la norme d'un élément de A si et seulement si c'est la norme d'un élément de B. [1]
8. Montrer que A n'est pas factoriel en écrivant deux factorisations de 4.
9. Montrer que B est intègre.
10. Montrer que les anneaux quotients $\mathbb{F}_p[X]/(X^2+X+1)$ et $B/(p)$ sont isomorphes.
11. En déduire que p est réductible dans B.
12. Montrer que p est de la forme $p = N(x)$, avec $x \in B$.
13. Montrer que p s'écrit donc sous la forme $p = a^2 + 3b^2$ avec $a, b \in \mathbb{Z}$.

1. Comme d'habitude, on définit la norme d'un nombre complexe comme $N(a+ib) = a^2+b^2$. C'est aussi donné par $N(a + ib) = (a + ib)(a - ib)$.

Solution du CC

Exercice 1 :

1. A est intègre car c'est un sous-anneau d'un anneau intègre.

2. Tout élément de A s'écrit comme une somme finie du type $\sum_{n,m\geq 0} a_{n,m}X^{2n+3m}$. Or, $n, m \geq 0$ donc $2n+3m$ est soit nul soit ≥ 2. Cela montre que X n'est pas dans l'image et $A \neq k[X]$.

3. Si $f \in A$ est inversible, il l'est aussi dans $k[X]$. Donc $f \in k$ est une constante non nulle. D'autre part les éléments de k sont tous dans A et l'inverse dans A d'une constante est une constante, donc $A^\times = k^\times$.

4. Supposons par l'absurde que $X^3 = fg$ dans A, avec $f, g \notin A^\times$. Par le point précédent cela signifie que f, g ne sont pas constants, et donc cela est aussi une décomposition de X dans $k[X]$. Comme $k[X]$ est factoriel, on doit avoir $f = cX^2$ et $g = c^{-1}X$, pour une constante c convenable. Cela est absurde car $X \notin A$.

Le même raisonnement pour X^2 donne $f = cX$ et $g = c^{-1}X$ ce qui est également absurde.

5. Dans A on a $X^6 = (X^2)^3 = (X^3)^2$. Ce qui montre que A ne peut pas être factoriel, car X^2 et X^3 ne sont pas associés ($X^2 \neq aX^3$ pour tout $a \in A^\times = k^\times$).

Exercice 2 :

1. Soit $Q = X^3 + X + 1 \in \mathbb{F}_2[X]$. On a $Q(0) = 0 + 0 + 1 = 1$, $Q(1) = 1 + 1 + 1 = 1$. Donc Q n'a pas de racines dans $\mathbb{F}_2$, et ne peut donc pas avoir de facteurs de degré un. Il est nécessairement irréductible dans $\mathbb{F}_2[X]$.

2. Soit $S(X) := X^4 + X^3 + X - 1$. On a alors $S(0) = 0 + 0 + 0 - 1 = -1$, $S(1) = 1 + 1 + 1 - 1 = -1$, $S(-1) = 1 - 1 - 1 - 1 = 1$. Donc S n'a pas de racines dans $\mathbb{F}_3$.

3. On procède par l'absurde. Comme P est unitaire, si $P = AB$ avec $A \in \mathbb{Z}[X]$ alors on peut supposer A et B unitaires. Cela entraine que le degré de cette factorisation est préservé par réduction modulo un idéal quelconque.

Si A est de degré un, on aurait une factorisation $\overline{P} = \overline{A} \cdot \overline{B}$ de la réduction $\overline{P} \in \mathbb{F}_3[X]$ de P dans $\mathbb{F}_3[X]$. Mais $\overline{P} = S$, et comme S n'a pas de racines dans $\mathbb{F}_3$, il n'a pas non plus de facteurs de degré 1. Cela contredit l'existence d'un facteur de degré 1 dans P.

Si A et B ont degré 2, on aurait une factorisation $\overline{P} = \overline{A} \cdot \overline{B}$ de la réduction $\overline{P} \in \mathbb{F}_2[X]$ de P dans $\mathbb{F}_2[X]$. Mais dans $\mathbb{F}_2[X]$ on a $\overline{P} = X^4 + X^2 + X = X(X^3 + X + 1)$. Mais nous avons vu que $X^3 + X + 1$ est irréductible, donc $\overline{P}$ n'a pas de facteurs de degré 2 dans $\mathbb{F}_2[X]$. Cela contredit l'existence de facteurs de degré 2 de P.

Donc P est irréductible.

Exercice 3 :

1. Les racines de l'unité sont les racines du polynôme $X^3-1=(X-1)(X^2+X+1)$. Comme $j \neq 1$, alors j est racine de X^2+X+1.

2. Si $p=a^2+3b^2$, alors son image dans $\mathbb{F}_3$ est a^2, mais les carrés dans $\mathbb{F}_3$ sont $0^2=0$, $1^2=1$, $(-1)^2=1$. Donc $p \equiv 0, 1 \pmod 3$, comme par hypothèse $p \neq 3$, on doit avoir $p \equiv 1 \pmod 3$.

3. On sait que le groupe $\mathbb{F}_p^\times$ est cyclique d'ordre $p-1$. Soit a un générateur. Comme $p \equiv 1 \pmod 3$, alors 3 divise $p-1$. Si $b=a^{\frac{p-1}{3}}$, alors $b^3=1$. L'ordre de b divise 3, c'est donc 1 ou 3. Mais l'ordre de b n'est pas 1 car $b \neq 1$, en effet $a^k \neq 1$ pour tout $k \leq p-1$. Donc l'ordre de b est 3.

4. On a $(X^2+X+1)(X-1)=(X-1)^3$. Les racines de X^2+X+1 sont les racines cubiques de l'unité différentes de l'unité. Or, on a vu que $\mathbb{F}_p^\times$ avait un élément b d'ordre exactement 3, donc b est une racine cubique non triviale de l'unité. Donc b est une racine de X^2+X+1.

5. L'élément $i\sqrt{3}$ appartient à B car $i\sqrt{3}=2j+1$. Pour tout $a+ib\sqrt{3} \in A$ on a alors $a+ib\sqrt{3}=(a+b)+j2b$, donc $A \subseteq B$.

Maintenant, si $x+jy \in B$ est tel que y est pair, alors $x+jy=(x-\frac{y}{2})+\frac{y}{2}i\sqrt{3} \in A$. Réciproquement, si $x+jy \in A$, alors on peut trouver $a, b \in \mathbb{Z}$ tels que $a+ib\sqrt{3}=x+jy$. Par unicité de l'écriture en B cela entraine $x=a+b$ et $y=2b$, donc y est pair.

6. Soit $\alpha=x+jy \in B$. À la question 1 on a vu que j est racine de X^2+X+1, donc $j^2=-j-1$. Donc $j\alpha=-y+j(x-y)$ et $j^2\alpha=(y-x)-jx$.

On utilise la question précédente : si y est pair alors $\alpha \in A$; si x est pair alors $j^2\alpha \in A$; si les deux sont impair, alors $(x-y)$ est pair et $j\alpha \in A$.

7. Si p est la norme d'un élément de A il est norme d'un élément de B, car on a vu que $A \subseteq B$. Par ailleurs si $p=N(\alpha)$ avec $\alpha \in B$, alors $p=N(\alpha)=N(j\alpha)=N(j^2\alpha)$, car $N(j)=1$ et la norme est multiplicative. Comme au moins un élément dans l'ensemble $\{\alpha, j\alpha, j^2\alpha\}$ est dans A, on voit que p est norme d'un élément de A.

8. On a $4=2^2=(1+i\sqrt{3})(1-i\sqrt{3})$. Montrons maintenant que 2, $(1+i\sqrt{3})$, et $(1-i\sqrt{3})$ sont irréductibles dans A, et que 2 n'est pas associé à $(1 \pm i\sqrt{3})$.

Calculons d'abord les inversibles de A. Si $\alpha=a+ib\sqrt{3} \in A^\times$ est inversible, alors $N(\alpha)=a^2+3b^2=1$. Donc $\alpha=\pm 1$ et $A^\times=\{\pm 1\}$.

Notons au passage que cela montre aussi que α est inversible dans A si et seulement si $N(\alpha) = 1$.

Si $2 = \alpha\beta$, avec $\alpha, \beta \notin A^\times$, alors $N(\alpha)N(\beta) = N(2) = 4$, et $N(\alpha) = N(\beta) = 2$. Mais l'équation $a^2 + 3b^2 = 2$ n'a pas de solutions entières. Donc 2 est irréductible.

De même, si $(1 + i\sqrt{3}) = \alpha\beta$, avec $\alpha, \beta \notin A^\times$, alors $N(\alpha)N(\beta) = N(1 \pm i\sqrt{3}) = 4$, et $N(\alpha) = N(\beta) = 2$. Mais l'équation $a^2 + 3b^2 = 2$ n'a pas de solutions entières. Donc $1 \pm i\sqrt{3}$ est irréductible.

Il est clair que 2 n'est pas associé à $(1 \pm i\sqrt{3})$ car les inversibles de A sont ± 1.

Donc A n'est pas factoriel.

9. L'anneau B est intègre car c'est un sous-anneau de $\mathbb{C}$.

10. On a $B \cong \mathbb{Z}[X]/(X^2+X+1)$. En effet on a une flèche $\varphi : \mathbb{Z}[X] \to \mathbb{C}$, qui envoie un polynôme P dans $P(j)$. L'image de φ est B. En effet l'image de $a + bX$ est $a + bj$, donc l'image contient B, et d'autre part l'image est le sous-anneau de $\mathbb{C}$ engendré par $\mathbb{Z}$ et j. Ce sous-anneau est contenu dans B car c'est le plus petit sous-anneau de $\mathbb{C}$ contenant $\mathbb{Z}$ et j.

Le noyau contient $X^2 + X + 1$ qui s'annule en j, et si $P(j) = 0$ on peut écrire (division euclidienne généralisée) $P = (X^2 + X + 1)Q(X) + R(X)$ avec $Q, R \in \mathbb{Z}[X]$ et $\deg(R) \leq 1$. Comme $P(j) = 0$ on a $R(j) = 0$ mais cela est impossible car j est irrationnel. Donc $Ker(\varphi) = (X^2 + X + 1)$ et $B = \mathbb{Z}[X]/(X^2 + X + 1)$.

Donc $B/(p) \cong \mathbb{Z}[X]/(p, X^2 + X + 1) \cong \mathbb{F}_p[X]/(X^2 + X + 1)$.

11. Par la question 3, le polynôme $X^2 + X + 1$ se décompose comme produit de deux facteurs de dégrée un dans $\mathbb{F}_p[X]$. En particulier, l'idéal $(X^2 + X + 1)$ n'est pas premier et l'anneau $\mathbb{F}_p[X]/(X^2 + X + 1) \cong B/(p)$ n'est pas intègre.

On en déduit que (p) n'est pas premier dans B. Comme B est Euclidien, tout idéal engendré par un irréductible est un idéal premier. Donc p ne peut pas être irréductible.

12. Comme p est réductible dans B, on peut écrire $p = \alpha\beta$, avec $\alpha, \beta \notin B^\times$. Donc $N(\alpha)N(\beta) = p^2$. Nous souhaitons en déduire que $N(\alpha) = N(\beta) = p$. Pour cela nous devons montrer que $N(\alpha) = 1$ entraine que $\alpha \in B^\times$ est inversible. Mais cela est un fait général : comme α et son conjugué $\overline{\alpha}$ sont dans B, si $N(\alpha) = \alpha\overline{\alpha} = 1$, alors $\overline{\alpha}$ est l'inverse de α.

Comme $\alpha, \beta \notin B^\times$, alors $N(\alpha), N(\beta) \neq 1$, et on doit avoir $N(\alpha) = N(\beta) = p$.

13. Par la question 6 on sait que dans l'ensemble $\{\alpha, j\alpha, j^2\alpha\}$ il y a un élément de A. Comme $N(j) = N(j^2) = 1$ les trois éléments ont norme p, et donc p est la norme d'un élément de A. Si $a + i\sqrt{3}b$ est cet élément, alors $p = a^2 + 3b^2$.