Anneaux de polynômes sur un corps

Solutions

Exercice 1 – On applique l'algorithme d'Euclide : les identités

$$X^3 + X + 1 = (X+1)(X^2 + X + 1) + X \quad \text{et} \quad X^2 + X + 1 = X(X+1) + 1,$$

amènent aux relations

$$\begin{aligned} 1 &= X^2 + X + 1 + X(X+1) = \\ &= X^2 + X + 1 + (X^3 + X + 1 + (X+1)(X^2 + X + 1))(X+1) = \\ &= X^2(X^2 + X + 1) + (X+1)(X^3 + X + 1). \end{aligned}$$

Exercice 2 – Soit $f \in K[X]$ un polynôme de de degré 2 ou 3. Tout d'abord, si f est irréductible, il n'a pas de racine dans K. En effet, si l'on avait $f(a) = 0$, avec $a \in K$, le polynôme f serait divisible par $X - a$, contredisant son irréductibilité. Réciproquement, supposons que f ne possède pas de racine dans K et soit $f = gh$ une factorisation, avec $g, h \in K[X]$ et $\deg(g) \leq \deg(h)$. Les relations $\deg(g) + \deg(h) = \deg(f) \leq 3$ amènent à l'inégalité $\deg(g) \leq 1$. Si l'on avait $\deg(g) = 1$, soit $g = aX + b$, avec $a, b \in K$ et $a \neq 0$, l'élément $-a^{-1}b \in K$ serait une racine de f, ce qui est exclu. On a donc $\deg(g) = 0$ et le polynôme f est irréductible.

Exercice 3 –

1. Un polynôme unitaire de degré 2 à coefficients dans K s'écrivant de manière unique comme $f = X^2 + aX + b$, il en existe p^2.
2. D'après l'exercice précédent, un polynôme $f \in K[X]$ de degré 2 est réductible si et seulement s'il possède une racine dans K, soit $f(a) = 0$ avec $a \in K$. Dans ce cas, on obtient la factorisation $f = (X-a)g$, avec $g \in K[X]$ de degré 1 et, le polynôme f étant unitaire, on en d'eduit l'identité $g = X - b$, avec $b \in K$. Finalement, on a la relation $a = b$ si et seulement si a est une racine double de f.
3. Le point précédent affirme que si un polynôme unitaire $f \in K[X]$ de degré 2 est réductible, il s'écrit de manière unique comme $f = (X-a)(X-b)$, avec $a, b \in K$ et $a \neq b$, ou $f = (x-a)^2$, avec $a \in K$. Dans le premier cas, on obtient $\frac{1}{2}p(p-1)$ polynômes (ce qui revient à choisir un sous-ensemble de cardinal 2 de K), et dans le second cas on a p polynômes (qui correspondent au choix de l'élément $a \in K$). Il s'en suit qu'il existe

$$p^2 - \frac{1}{2}p(p-1) - p = \frac{1}{2}p(p-1)$$

polynômes unitaires, irréductibles, de degré 2 dans $K[X]$. Da manière explicite, il existe un unique polynôme unitaire, irréductible, de degré 2 dans $\mathbb{Z}/2\mathbb{Z}[X]$, égal à X^2+X+1. De même, les trois polynômes unitaires, irréductibles, de degré 2 de $\mathbb{Z}/3\mathbb{Z}[X]$ sont X^2+1, X^2+X+2 et X^2+2X+2.

Exercice 4 – Posons

$$(\cos(\theta)+sin(\theta)X)^n=(X^2+1)q+r,$$

avec $q, r=u+vX\in K[X]$. En évaluant les deux termes de cette égalité en i, on obtient les identités

$$(\cos(\theta)+i\sin(\theta))^n=\cos(n\theta)+i\sin(n\theta)=u+iv,$$

d'où les relations $u=\cos(n\theta)$ et $v=\sin(n\theta)$, ou encore $r=\cos(n\theta)+\sin(n\theta)X$.

Exercice 5 –

1. En posant $f=(X-a)(X-b)q+r$, avec $q, r=u+vX\in K[X]$, et en évaluant en a, puis en b, on obtient le système linéaire

$$\begin{cases} u+av=f(a), \\ \\ u+bv=f(b), \end{cases}$$

   ce qui amène aux expressions $u=\frac{af(b)-bf(a)}{a-b}$ et $v=\frac{f(a)-f(b)}{a-b}$.
2. En posant $f=(X-a)^2q+r$, avec $q, r=u+vX\in K[X]$, on a l'identité

$$f'=(X-a)^2q'+2(X-a)q+v.$$

   En évaluant les deux termes de cette dernière égalité en a, on en déduit l'expression $v=f'(a)$, et, en évaluant une fois de plus en a, la première égalité amène à la relation $u=f(a)-af'(a)$.

Exercice 6– Notons d le pgcd de f et g et considérons une idéntité de Bézout $uf+vg=d$, avec $u, v\in K[X]$. En évaluant chacun des termes de cette égalité en une racine commune $a\in L$ de f et g, on obtient alors la relation $d(a)=0$, ce qui implique que d, qui est non nul, n'est pas un polynôme constant. Il s'en suit que d est un diviseur de f de degré supérieur ou égal à 1, ce qui implique qu'il est associé à f (car f est irréductible), d'où le résultat.

Exercice 7– On peut supposer $f\in\mathbb{R}[X]$ unitaire. On remarquera si $z\in\mathbb{C}$ est une racine de f, il en est de même pour $\bar{z}$ (le conjugué de z) et leur multiplicités coïncident. Pour toute racine z de f, notons e_z sa mutiplicité. Si $\mathcal{R}$ (respectivement $\mathcal{C}$) désigne l'ensemble des racines réelles de f (resp. l'ensemble des racines non réelles de f à partie imaginaire strictement positive), on obtient les identités

$$f=\prod_{z\in\mathcal{R}}(X-z)^{e_z}\prod_{z\in\mathcal{C}}(X-z)^{e_z}(X-\bar{z})^{e_z}=\prod_{z\in\mathcal{R}}(X-z)^{e_z}\prod_{z\in\mathcal{C}}(X^2-2\mathrm{Re}(z)X+N(z))^{e_z},$$

où l'on a posé $\mathrm{Re}(z)=\frac{1}{2}(z+\bar{z})\in\mathbb{R}$ et $N(z)=z\bar{z}\in\mathbb{R}$. Il suffit finalement de remarquer que pour tout $z\in\mathcal{R}$, le polynôme $X-z$ est irréductible (car de degré 1) et pour

tout $z \in \mathcal{C}$, il en est de même pour $X^2 + \mathrm{Re}(z)X + N(z)$ (car ce dernier ne possède pas de racine réelle, cf. l'exercice 2). Les racines complexes du polynôme $X^8 - 1$ étant $1, -1, i, -i, \frac{\sqrt{2}}{2}(1+i), \frac{\sqrt{2}}{2}(1-i), \frac{\sqrt{2}}{2}(-1+i)$ et $\frac{\sqrt{2}}{2}(-1-i)$, la méthode décrite ci-dessus amène à l'identité

$$X^8 - 1 = (X-1)(X+1)(X^2+1)(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1).$$

Exercice 8 – Pour $p = 2$, on a les identités $X^2 + 3X + 4 = X(X+1)$. Pour $p = 3$, le polynôme ne possède pas de racine dans $\mathbb{Z}/3\mathbb{Z}$ et l'exercice 2 affirme qu'il est irréductible. Pour $p = 5$, on a les relations $X^2 + 3X + 4 = (X-1)^2 - 2$ et (la classe de) 2 n'étant pas un carré dans $\mathbb{Z}/5\mathbb{Z}$, le polynôme est irréductible. Pour $p = 7$, on obtient l'identité $X^2 + 3X + 4 = (X-2)^2$. Finalement, pour $p = 11$, on a les identités

$$X^2 + 3X + 4 = X^2 - 8X + 4 = (X-4)^2 - 12 = (X-4)^2 - 1 = (X-5)(X-3).$$

On remarquera que pour $p \neq 2$, afin de résoudre une équation du second degré, on peut utiliser la méthode usuelle (par le calcul du discriminant). Dans le cas présent, on a $\Delta = 3^2 - 4 \cdot 1 \cdot 4 = -7$, qui est un carré dans $\mathbb{Z}/p\mathbb{Z}$ pour $p \in \{7, 11\}$ et ne l'est pas pour $p \in \{3, 5\}$.

Exercice 9 –

1. Fixons un élément x de A. En munissant A de sa structure naturelle de K-espace vectoriel, l'application $\phi : A \to A$ définie par la relation $\phi(y) = xy$ est linéaire. Elle est injective si et seulement si $\ker(\phi)$ est nul, ce qui revient à affirmer que x n'est pas un diviseur de 0. Le K-espace vectoriel A étant de dimension finie, le théorème du rang affirme que cette dernière condition est équivalente à la surjectivité de ϕ. Montrons maintenant que ϕ est surjective si et seulement s'il existe $y \in A$ tel que $\phi(y) = 1$, ce qui se traduit par l'inversibilité de x. Une implication étant immédiate, si $\phi(y) = 1$ on en déduit que, pour tout $z \in A$, on a les identités

   $$\phi(yz) = xyz = \phi(y)z = z,$$

   et donc z appartient à l'image de ϕ, d'où l'assertion.
2. Il suffit de considérer l'anneau $\mathbb{Z}$, car tout entier $n > 1$ n'est ni inversible, ni diviseur de 0.

Exercice 10 – On a la factorisation $X^3 - X^2 = X^2(X-1)$. Un élément $x \in A$ possède un unique représentant du type $f = a + bX + cX^2$, avec $a, b, c \in \mathbb{C}$.

— L'élément x est inversible si et seulement si le polynôme f est premier avec $X^3 - X^2$, ce qui revient à affirmer que X et $X-1$ ne divisent pas f, ou encore que $f(0)$ et $f(1)$ sont non nuls. On obtient donc les relations $a \neq 0$ et $a + b + c \neq 0$.

— L'élément x est nilpotent si et seulement s'il existe un entier $n > 0$ tel que le polynôme $X^3 - X^2$ divise f^n, ce qui implique que X et $X-1$ divisent f, d'où les relations $a = a + b + c = 0$. Dans ce cas, le polynôme f est divisible par $X(X-1)$ (car les polynômes X et $X-1$ sont premiers entre eux), ce qui amène à l'identité $x^2 = 0$.

— Finalement, d'après l'exercice précédent, l'élément x est un diviseur de 0 si et seulement s'il n'est pas inversible, ce qui se traduit par les conditions $a = 0$ ou $a + b + c = 0$.

Exercice 11 –

1. En procédant par l'absurde, supposons que $\sqrt{p} = \frac{n}{m}$ est rationnel, où n et m sont deux entiers premiers entre eux. On obtient alors l'identité $n^2 = pm^2$ et l'entier n est donc divisible par p, soit $n = pu$, avec p entier, ce qui amène à la relation $p^2u^2 = m^2$, ou encore $m^2 = pu^2$, et l'entier m est lui aussi divisible par p, ce qui contredit la coprimalité de n et m.
2. Supposons d'avoir deux écritures $x = a + b\sqrt{p} = a' + b'\sqrt{p}$, avec $a, a', b, b' \in \mathbb{Q}$. En posant $u = a - a' \in \mathbb{Q}$ et $v = b - b' \in \mathbb{Q}$, on obtient l'identité $u + v\sqrt{p} = 0$. Si l'on avait $v \neq 0$, on en déduirait les relations $\sqrt{p} = -uv^{-1} \in \mathbb{Q}$, ce qui est exclu. On a donc $v = 0$ et, par conséquent, $u = -v\sqrt{p} = 0$, d'où $a = a'$ et $b = b'$.
3. Étant donnés deux éléments $x = a + b\sqrt{p}$ et $y = a' + b'\sqrt{p}$ de $\mathbb{Q}(\sqrt{p})$, les relations

$$\begin{cases} x + y = a + b\sqrt{p} + a' + b'\sqrt{p} = (a + a') + (b + b')\sqrt{p} \in \mathbb{Q}(\sqrt{p}), \\ \\ xy = (a + b\sqrt{p})(a' + b'\sqrt{p}) = (aa' - pbb') + (ab' + ba')\sqrt{p} \in \mathbb{Q}(\sqrt{p}) \end{cases}$$

   impliquent que $\mathbb{Q}(\sqrt{p})$ est stable par rapport à la somme et au produit. En particulier, l'inclusion $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p})$ amène aux relations $0, 1, -x \in \mathbb{Q}(\sqrt{p})$. L'ensemble $\mathbb{Q}(\sqrt{p})$ est donc un sous-anneau de $\mathbb{R}$. Soit maintenant $x = a + b\sqrt{p} \in \mathbb{Q}(\sqrt{p})$ un élément non nul. En posant $N(x) = a^2 - pb^2 \in \mathbb{Q}$, on a l'inégalité $N(x) \neq 0$. En effet, dans le cas contraire, si b était non nul, on obtiendrait l'identité $p = a^2b^{-2}$ et $\sqrt{p}$ serait rationnel. On a donc $b = 0$, d'où $a^2 = a^2 - pb^2 = 0$ et finalement $a = 0$, ce qui donne $x = 0$. Dans ce cas, en posant

$$y = aN(x)^{-1} - bN(x)^{-1}\sqrt{p} \in \mathbb{Q}(\sqrt{p}),$$

   on obtient les identités

$$xy = N(x)^{-1}(a + b\sqrt{p})(a - b\sqrt{p}) = N(x)^{-1}(a^2 - pb^2) = 1$$

   et x est inversible. Le sous-anneau $\mathbb{Q}(\sqrt{p})$ de $\mathbb{R}$ est donc un corps.
4. D'après l'exercice 2, le polynôme $X^2 - p \in \mathbb{Q}[X]$ est irréductible, car in ne posséde pas de racine dans $\mathbb{Q}$. De plus, l'exercice 6 affirme que si $f \in \mathbb{Q}[X]$ s'annule en $\sqrt{p}$ alors il est divisible par $X^2 - p$ (et la réciproque est trivialement vérifiée). Le noyau de ϕ étant formé par les polynômes s'annulant en $\sqrt{p}$ on en déduit que c'est l'idéal de $\mathbb{Q}[X]$ engendré par $X^2 - p$. Pour tout polynôme $f \in \mathbb{Q}[X]$, en effectuant la division euclidienne, on obtient l'identité $f = (X^2 - p)q + r$, avec $q, r = a + bX \in \mathbb{Q}[X]$. Il s'en suit que l'élément $\phi(f) = a + b\sqrt{p}$ appartient à $\mathbb{Q}(\sqrt{p})$. Réciproquement, pour tout élément $x = a + b\sqrt{p} \in \mathbb{Q}(\sqrt{p})$, on a l'identité $x = \phi(a + bX)$ et on en déduit que l'image de ϕ coïncide avec $\mathbb{Q}(\sqrt{p})$. Le théorème de factorisation pour les homomorphismes d'anneaux affirme alors que le quotient $\mathbb{Q}[X]/(X^2 - p)$ est isomorphe à $\mathbb{Q}(\sqrt{p})$.
5. Supposons d'avoir un isomorphisme $\sigma : \mathbb{Q}(\sqrt{p}) \to \mathbb{Q}(\sqrt{q})$. On remarquera que l'identité $\sigma(1) = 1$ implique que $\sigma(x) = x$ pour tout $x \in \mathbb{Q}$. Il s'en suit que l'élément $x = \sigma(\sqrt{p}) = a + b\sqrt{q} \in \mathbb{Q}(\sqrt{q})$ vérifie les relations

$$x^2 = a^2 - qb^2 + 2ab\sqrt{q} = \sigma(\sqrt{p})^2 = \sigma(\sqrt{p}^2) = \sigma(p) = p.$$

L'unicité de l'écriture d'un élément de $\mathbb{Q}(\sqrt{q})$ obtenue dans le point 1 implique alors que $2ab = 0$, d'où les identités $a = 0$ ou $b = 0$, qui amènent respectivement aux relations $qb^2 = p$ et $a^2 = p$, toutes deux impossibles.