DM2 — Solution

Exercice 1. Soit A un anneau (commutatif unitaire) et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$.

a) Montrer que P est nilpotent si et seulement si pour tout $i \in \mathbb{N}$, a_i est nilpotent.

b) Soit x un élément nilpotent de A. Montrer que $1 + x$ est inversible.

c) Montrer que P est inversible dans $A[X]$ si et seulement si a_0 est inversible et pour tout $i \geq 1$, a_i est nilpotent.

Indice : si $Q = \sum_{i=0}^{m} b_i X^i$ est un inverse de P, on pourra commencer par montrer que que pour tout $r \geq 0$, $a_n^{r+1} b_{m-r} = 0$.

d) Montrer qu'un élément x de A appartient à tous les idéaux maximaux de A si et seulement si pour tout $a \in A$, $1 - ax$ est inversible.

e) Montrer que P est dans l'intersection de tous les idéaux maximaux si et seulement si P est nilpotent (c'est-à-dire, dans $A[X]$, le radical de Jacobson est égal au nilradical).

Solution. a) Si a_i est nilpotent dans A pour tout i, il l'est aussi dans $A[X]$ et donc P, qui appartient à l'idéal de $A[X]$ engendré par les a_i l'est aussi (puisque les éléments nilpotents forment un idéal).

Réciproquement, on raisonne par récurrence sur le degré de P (c'est évident si P est un polynôme constant). Si $P^k = 0$, alors le coefficient en X^{nk} dans P^k, qui est a_n^k, doit être nul. Donc a_n est nilpotent. Donc $Q = P - a_n X^n$ est aussi nilpotent et $\deg Q < \deg P$. Donc les coefficients de Q sont nilpotents, or ce sont les coefficients de P (à l'exception de a_n). D'où le résultat.

b) Si $x^n = 0$, on pose $x' = \sum_{i=0}^{n-1} (-x)^i$ et on vérifie que $x'(1 + x) = 1$.

c) Si a_0 est inversible et a_i nilpotent pour $i \geq 1$, alors $P = a_0(1 + a_0^{-1} \sum_{i=1}^{n} a_i X^i)$. D'après a), $a_0^{-1} \sum_{i=1}^{n} a_i X^i$ est nilpotent, donc $(1 + a_0^{-1} \sum_{i=1}^{n} a_i X^i)$ est inversible d'après b), et donc P est inversible comme produit d'inversibles.

Réciproquement, soit $Q = \sum_{i=0}^{m} b_i X^i$ un inverse de P. Alors $1 = a_0 b_0$, donc a_0 et b_0 est inversible. Montrons par récurrence sur r que $a_n^{r+1} b_{m-r} = 0$.

Pour $r = 0$, il suffit de regarder le coefficient de X^{m+n} dans $PQ = 1$.

Pour $r \geq 1$ alors le coefficient de X^{m+n-r} dans $PQ = 1$ est $0 = a_n b_{m-r} + \sum_{k=0}^{r-1} a_k b_{m-k}$. En multipliant par a_n^r et puisque $0 = a_n^k b_{m-k} | a_k b_{m-k} a_n^r$ pour $k \leq r - 1$, il ne reste plus que $0 = a_n^{r+1} b_{m-r}$, comme voulu.

En prenant, $r = m$, on obtient $a_n^{m+1} b_0 = 0$, et donc a_n est nilpotent puisque b_0 est inversible.

Donc $P - a_n X^n$ est aussi inversible (par la question b)), et de degré strictement inférieur à P. Par récurrence sur le degré de P, on en déduit que $a_i = 0$ pour $1 \leq i \leq n - 1$.

d) Supposons que x appartienne à tous les idéaux maximaux de A. Si $1 - ax$ n'est pas inversible, $(1 - ax)$ est un idéal propre, donc contenu dans un idéal maximal $\mathfrak{m}$. Alors $1 = (1 - ax) + ax \in \mathfrak{m}$ comme combinaison linéaire d'éléments de $\mathfrak{m}$. D'où une contradiction.

Si $1 - ax$ est inversible pour tout a. Soit $\mathfrak{m}$ un idéal maximal de A ne contenant pas x. Alors l'image $\bar{x}$ de x dans $A/\mathfrak{m}$ est non nul donc inversible, d'inverse $\bar{x}'$. Alors $1 - xx' \in \mathfrak{m}$ ne peut pas être inversible contrairement à l'hypothèse.

e) Si P est dans tout idéal premier, a fortiori il est dans tout idéal maximal.

Réciproquement, si P est dans tout idéal maximal, alors d'après d), $1 + XP$ est inversible. On déduit donc de c), que les coefficients de P sont nilpotents, donc P est nilpotent d'après a). Il appartient donc à tout idéal premier.

Exercice 2. Soit $n \geq 2$ un entier. Le but de ce problème est de montrer que

$$S_n = X^n - X - 1$$

est irréductible sur $\mathbb{Q}$.

– Montrer que S_n a n racines distinctes dans $\mathbb{C}$.

– Pour tout polynôme $P \in \mathbb{C}[X]$ de degré m tel que $P(0) \neq 0$, on note $z_1, \ldots, z_m$ les racines de P dans $\mathbb{C}$ comptées avec multiplicité et on pose

$$\phi(P) = \sum_{i=1}^{m} \left(z_i - \frac{1}{z_i} \right).$$

Exprimer $\phi(P)$ en fonction des coefficients de P. En déduire la valeur de $\phi(S_n)$.

– Soit z une racine de S_n. Montrer que l'on a

$$2\Re\left(z - \frac{1}{z} \right) > \frac{1}{|z|^2} - 1.$$

On pourra écrire $z = re^{i\theta}$ et exprimer $\cos\theta$ en fonction de r.

– Montrer que si $x_1, \ldots, x_m$ sont m réels positifs tels que $\prod_{i=1}^{m} x_i = 1$, on a

$$\sum_{i=1}^{m} x_i \geq m.$$

– Soit P un diviseur non constant de S_n dans $\mathbb{Z}[X]$. Montrer que $|P(0)| = 1$ et $\phi(P) \geq 1$.

– Conclure.

Solution. a) Une racine double x serait racine de S_n et de sa dérivée $S_n' = nX^{n-1} - 1$. On aurait donc $x^{n-1} = 1/n$, et donc $0 = S_n(x) = x/n - x - 1$, d'où $x = \frac{n}{1-n}$, ce qui est en contradiction avec $x^{n-1} = 1/n$ (comme on peut le remarquer en regardant la norme ou la valuation p-adique pour un p divisant n). S_n a donc bien n racines distinctes dans $\mathbb{C}$ (puisque $\mathbb{C}$ est algébriquement clos).

b) Écrivons $P = \sum_{n=0}^{m} a_n X^n = a_m \prod_{i=1}^{m} (X - z_i)$. En développant et en identifiant le coefficient en X^{m-1}, on trouve

$$a_{m-1} = -a_m \sum_i z_i.$$

De même $a_0 = a_m \prod_i (-z_i)$ et

$$a_1 = a_m \sum_i \prod_{j \neq i} (-z_i) = \sum_i \frac{1}{-z_i} a_m \prod_j (-z_j) = -a_0 \sum_i \frac{1}{z_i}.$$

Donc $\phi(P) = -\frac{a_{m-1}}{a_m} + \frac{a_1}{a_0}$.
En particulier $\phi(S_n) = 1$.

c) Ecrivons $z = re^{i\theta}$. Alors $z - \frac{1}{z} = re^{i\theta} - e^{-i\theta}/r$. Comme $\cos(\theta) = \cos(-\theta)$, on obtient

$$\Re(z - \frac{1}{z}) = (r - 1/r)\cos(\theta).$$

L'énoncé est donc équivalent à montrer que

$$(1 - \frac{1}{r^2})(1 + 2r\cos(\theta)) > 0.$$

Comme S_n est à coefficients réels, $\bar{z}$ est aussi racine de S_n. Donc

$$r^{2n} = z^n \bar{z}^n = (1+z)(1+\bar{z}) = 1 + z + \bar{z} + z\bar{z} = 1 + 2r\cos(\theta) + r^2$$

. On est donc ramené à prouvé que

$$(1 - \frac{1}{r^2})(r^{2n} - r^2) > 0.$$

Or si $r < 1$, $(1 - \frac{1}{r^2}) < 0$ et $(r^{2n} - r^2) < 0$, d'où l'inégalité voulue.
Si $r > 1$, $(1 - \frac{1}{r^2}) > 0$ et $(r^{2n} - r^2) > 0$, d'où l'inégalité voulue.
Si $r = 1$, l'expression de $\cos(\theta)$ nous donne $\cos(\theta) = -\frac{1}{2}$ et donc $z = j$ ou $\bar{j}$ est une racine 3$^{\text{e}}$ de 1, de polynôme minimal $X^2 + X + 1$ sur $\mathbb{Q}$. En posant k le reste de la division euclidienne de n par 3, on en déduit que z est racine de $X^k - X - 1$, qui n'est pas multiple de $X^2 + X + 1$, d'où une contradiction.

d) Par convexité de l'exponentielle $\exp(\frac{1}{m}\sum_{i=1}^{m} y_i) \leq \frac{1}{m}\sum_{i=1}^{m} \exp(y_i)$. En appliquant cette inégalité à $y_i = \log x_i$ et puisque $\sum_i \log x_i = 0$ par hypothèse, on obtient $1 \leq\leq \frac{1}{m}\sum_{i=1}^{m} x_i$ comme voulu.

e) Supposons $S_n = PQ$ avec $P, Q \in \mathbb{Z}[X]$. Quitte à multiplier P par -1, on peut supposer P unitaire. Alors $-1 = S_n(0) = P(0)Q(0)$, donc $P(0)$ est inversible dans $\mathbb{Z}$ et donc $P(0) = 1$ ou -1.
Comme P est unitaire et $P(0)$ est inversible, $\phi(P) \in \mathbb{Z}$.
Notons $(x_j)_{j=1}^k$ la famille des racines de P (ce sont aussi des racines de S_n. On a

$$2\phi(P) = 2\Re(\phi(P)) = 2\sum_j \Re(x_j - \frac{1}{x_j}) > \sum_j (\frac{1}{|x_j}^2 - 1)$$

On a $\prod_{j=1}|x_j| = |P(0)| = 1$ et donc $\prod_j \frac{1}{|x_j}^2 = 1$. D'après la question précédente, on en déduit que $\sum_j (\frac{1}{|x_j}^2 \geq m$.
On obtient alors $\Phi(P) > 0$, et donc $\Phi(P) \geq 1$ puisque $\phi(P) \in \mathbb{Z}$.

f) Si S_n est réductible dans $\mathbb{Q}[X]$, il l'est aussi dans $\mathbb{Z}[X]$. Soient donc P et Q comme dans la question précédente.
On a alors $\phi(S_n) = \phi(P) + \phi(Q) \geq 2$, ce qui contredit la question 2.

Exercice 3. Soit A un anneau noethérien et G un groupe fini opérant sur A par automorphismes d'anneaux. On note $A^G = \{a \in A : \forall g \in G, ga = a\}$. Vérifier que A^G est un sous-anneau de A.
On suppose que le cardinal de G est inversible dans A et on défini $p : A \to A$ par

$$p(a) = \frac{1}{\text{card}(G)} \sum_{g \in G} ga.$$

a) Montrer que pour tout $g \in G$, on a $g \circ p = p \circ g = p$.
b) Montrer que p est A^G-linéaire et que $p \circ p = p$.
c) Montrer que l'image de p est A^G.
d) Soit I un idéal de A^G et IA l'idéal de A engendré par I. Montre que $p(IA) = I$.
e) Montrer que A^G est noethérien.

Solution. (i) On calcule

$$g \circ p(a) = g\left(\frac{1}{\text{card}(G)} \sum_{h \in G} ha\right) = \frac{1}{\text{card}(G)} \sum_{h \in G} (gh)a = \frac{1}{\text{card}(G)} \sum_{gh \in G} gha = p(a).$$

De même on a

$$p \circ g(a) = \frac{1}{\text{card}(G)} \sum_{h \in G} h(ga) = \frac{1}{\text{card}(G)} \sum_{h \in G} (hg)a = \frac{1}{\text{card}(G)} \sum_{hg \in G} (hg)a = p(a).$$

(ii) On calcule

$$p \circ p = \frac{1}{\text{card}(G)} \sum_{g \in G} g \circ p = \frac{1}{\text{card}(G)} \sum_{g \in G} p = \frac{1}{\text{card}(G)} \text{ card}(G)\ p = p.$$

Si $\lambda \in A^G$ est invariant par le groupe G, alors on a

$$p(\lambda a) = \frac{1}{\text{card}(G)} \sum_{g \in G} g(\lambda a) = \frac{1}{\text{card}(G)} \sum_{g \in G} \lambda g(a) = \lambda \frac{1}{\text{card}(G)} \sum_{g \in G} ga = \lambda p(a).$$

Le projecteur p est donc bien A^G linéaire.
(iii) Soit $\lambda \in A^G$, on a alors

$$p(\lambda) = \frac{1}{\text{card}(G)} \sum_{g \in G} g(\lambda) = \frac{1}{\text{card}(G)} \sum_{g \in G} \lambda = \lambda \frac{1}{\text{card}(G)} \text{ card(G)} = \lambda.$$

ce qui prouve que A^G est contenu dans l'image de p. Par ailleurs, si $x \in \text{Im}\, p$, alors on a $x = p(y)$ et pour tout $g \in G$, on a

$$g(x) = g(p(y)) = g \circ p(y) = p(y) = x$$

donc $x \in A^G$.
(iv) Comme $I \subset A^G$ et que p est l'identité sur A^G, on a $p(I) = I$. Or on a $I \subset IA$ donc $I \subset p(IA)$.

Soit maintenant $x \in IA$, on peut alors écrire $x = \sum_i a_i x_i$ avec $a_i \in A$ et $x_i \in I$. Mais alors comme p est A^G linéaire, on a

$$p(x) = \sum_i x_i p(a_i)$$

et $x_i \in I$ et $p(a_i) \in A^G$, on a donc $p(x) \in I$ car I est un idéal de A^G.
(v) Première méthode : soit $(I_n)_n$ une suite croissante d'idéaux de A^G et montrons que (I_n) est stationnaire. La suite $(I_n A)_n$ est une suite croissante d'idéaux de A donc est stationnaire par noethérianité de A. Donc la suite $(p(I_n A))_n$ est stationnaire, or comme $p(I_n A) = I_n$, on obtient le résultat voulu.

Deuxième méthode : soit I un idéal de A^G et montrons qu'il est de type fini. On a vu que $I = p(IA)$ où IA est un idéal de A. Comme A est noethérien, ce dernier idéal est de type fini : $IA = (a_1, \cdots, a_n)$. Mais alors comme I engendre IA, les a_i s'écrivent :

$$a_i = \sum_j x_{i,j} b_{i,j}$$

où la somme est finie avec $b_{i,j} \in I$ et $x_{i,j} \in A$. On voit donc que les $b_{i,j} = p(b_{i,j})$ engendrent IA comme idéal de A. Montrons qu'ils engendrent I comme idéal de A^G.
En effet, si $x \in I$, alors on sait que $x \in p(IA)$ donc $x = p(y)$ avec $y \in IA$. Mais alors on peut écrire $y = \sum_{i,j} y_{i,j} b_{i,j}$ avec $y_{i,j} \in A$. On a alors comme $b_{i,j} \in I \subset A^G$ et que p est A^G-linéaire :

$$x = p(y) = \sum_{i,j} p(y_{i,j} b_{i,j}) = \sum_{i,j} p(y_{i,j}) b_{i,j}.$$

Comme les $p(y_{i,j})$ sont dans A^G, ceci prouve que les $b_{i,j}$ engendrent I comme idéal de A^G.