1. Soit A un anneau local[1]. Lorsque M est un A-module de type fini, on appelle (très logiquement) *famille génératrice minimale* un ensemble d'éléments de M qui engendrent celui-ci (en tant que A-module) et dont aucun sous-ensemble strict n'engendre M. Montrer que toutes les familles génératrices minimales de M ont le même cardinal (fini). (Indication : si $\mathfrak{m}$ est l'idéal maximal de A, on considérera $\tilde{M} = M/\mathfrak{m}M$ l'espace vectoriel résiduel sur le corps $k = A/\mathfrak{m}$. On appliquera le lemme de Nakayama.) Donner un contre-exemple à cette affirmation lorsque A n'est pas un anneau local.

Corrigé. Tout d'abord, on constate que $\tilde{M} = M/\mathfrak{m}M = M \otimes_A k$ est bien, de façon naturelle, un espace vectoriel sur le corps résiduel $k = A/\mathfrak{m}$ de A. Comme M est de type fini, il en va de même de $\tilde{M}$, c'est-à-dire que $\tilde{M}$ est un espace vectoriel de dimension finie. Appelons n cette dimension. On va montrer que toute famille génératrice minimale de M est de cardinal n.

Soit $(x_i)_{i\in I}$ une famille génératrice de M (il n'est pas besoin de supposer I fini). Notons $\tilde{x}_i \in \tilde{M}$ la classe de x_i modulo $\mathfrak{m}M$. La famille $(\tilde{x}_i)_{i\in I}$ engendre l'espace vectoriel $\tilde{M}$, donc il existe $J \subseteq I$ de cardinal n tel que $(\tilde{x}_i)_{i\in J}$ en soit une base. Montrons que $(x_i)_{i\in J}$ engendre encore M. Pour cela, soit N le quotient de M par son sous-module engendré par les x_i avec $i \in J$: il s'agit de prouver que $N = 0$. Or N est un A-module de type fini (comme quotient du A-module de type fini M), et on a $N = \mathfrak{m}N$ puisque tout élément $\bar{y} \in N$ provient d'un élément $y \in M$ qui a une réduction $\tilde{y} \in \tilde{M}$ qui est combinaison linéaire (à coefficients dans k) des $\tilde{x}_i$ pour $i \in J$ donc quitte à modifier y par une combinaison linéaire des x_i avec $i \in J$ (donc sans changer sa classe $\bar{y} \in N$) on peut supposer $\tilde{y} = 0$ c'est-à-dire $y \in \mathfrak{m}M$ et donc $\bar{y} \in \mathfrak{m}N$. Le lemme de Nakayama donne alors $N = 0$, ce qui signifie exactement que les x_i où $i \in J$ engendrent M.

On vient de montrer que toute famille génératrice contient une sous-famille génératrice à n éléments, et celle-ci est manifestement minimale (car il n'est pas possible pour moins de n éléments x_i d'avoir des résidus $\tilde{x}_i$ qui engendrent $\tilde{M}$, lequel est de dimension n). En particulier, toute famille génératrice minimale est de cardinal n.

Si A n'est pas un anneau local, on peut trouver des contre-exemples : sur $A = \mathbb{Z}$, pour $M = A$ le $\mathbb{Z}$-module libre de rang 1 (donc certainement de type fini) les deux parties $\{1\}$ et $\{2, 3\}$ sont génératrices minimales, mais elles n'ont pas le même cardinal. (Il est même facile de voir qu'il existe des familles génératrices minimales arbitrairement grandes.) ✓

2. Soit d un entier relatif sans facteur carré. On cherche à déterminer la clôture intégrale $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ de $\mathbb{Z}$ dans le corps $\mathbb{Q}(\sqrt{d})$ (autrement dit l'anneau des entiers du corps de nombres $\mathbb{Q}(\sqrt{d})$). Soit $\sigma\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ l'unique élément non trivial de $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$, groupe de Galois de l'extension (donc $\sigma\colon \sqrt{d} \mapsto -\sqrt{d}$).

(1) Montrer que $x \in \mathbb{Q}(\sqrt{d})$ est entier (sur $\mathbb{Z}$) si et seulement si la trace $\mathrm{tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x) = x + \sigma(x)$ et la norme $N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x) = x \cdot \sigma(x)$ sont des entiers (relatifs). (Indication : quel est le polynôme minimal de x sur $\mathbb{Q}$?)

(2) En déduire que $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ vaut $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ si $d \equiv 1 \pmod 4$ et $\mathbb{Z}[\sqrt{d}]$ sinon.

Corrigé. (1) Montrons d'abord le « seulement si » : si x est entier sur $\mathbb{Z}$ il est clair que $\sigma(x)$ l'est aussi, donc $x + \sigma(x)$ et $x \cdot \sigma(x)$ le sont. Comme ce sont des rationnels (puisqu'ils sont invariants par σ), dire qu'ils sont entiers sur $\mathbb{Z}$ signifie exactement (car $\mathbb{Z}$ est intégralement clos) qu'ils sont des entiers relatifs.

([1]) On rappelle qu'un anneau (commutatif) est dit *local* lorsque l'ensemble de ses éléments non inversibles forme un idéal $\mathfrak{m}$, qui est alors l'unique idéal maximal de A (un idéal maximal $\mathfrak{m}$ est un idéal strict maximal pour l'inclusion — ou, de façon équivalente, tel que $A/\mathfrak{m}$ est un corps).

Montrons à présent le « si » : on a $0 = (x-x)\,(x-\sigma(x)) = x^2 - (x+\sigma(x))\,x + (x\cdot\sigma(x)) = x^2 - \mathrm{tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x)\,x + N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x)$, c'est-à-dire que x est racine du polynôme unitaire $P(t) = t^2 - \mathrm{tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x)\,t + N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x)$, qui est à coefficients entiers par hypothèse. Or cela signifie exactement que x est entier sur $\mathbb{Z}$.

(Le polynôme minimal de $x \in \mathbb{Q}(\sqrt{d})$ sur $\mathbb{Q}$ est $P(t) = t^2 - \mathrm{tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x)\,t + N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x)$, sauf naturellement si $x \in \mathbb{Q}$ auquel cas son polynôme minimal est $P(t) = t - x$. Le polynôme caractéristique est toujours celui de degré 2.)

(2) Soit $x = \alpha + \beta\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, où $\alpha, \beta \in \mathbb{Q}$. Dire que $\mathrm{tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x) \in \mathbb{Z}$ signifie $2\alpha \in \mathbb{Z}$ (i.e., soit $\alpha \in \mathbb{Z}$ soit $\alpha \in \frac{1}{2} + \mathbb{Z}$), et dire que $N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x) \in \mathbb{Z}$ signifie $\alpha^2 - d\beta^2 \in \mathbb{Z}$. Manifestement, $\sqrt{d}$ est toujours dans $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$: on en déduit $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} \supseteq \mathbb{Z}[\sqrt{d}]$. Considérons maintenant $\alpha + \beta\sqrt{d} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ avec $\alpha \in \mathbb{Z}$: alors quitte à soustraire $\alpha \in \mathbb{Z}$ on peut supposer $\alpha = 0$, et dans ce cas $d\beta^2 \in \mathbb{Z}$ ce qui, puisque $\beta \in \mathbb{Q}$ et que d est sans facteur carré, implique $\beta \in \mathbb{Z}$. D'autre part considérons $\alpha + \beta\sqrt{d} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ avec $\alpha \in \frac{1}{2} + \mathbb{Z}$ et de nouveau, quitte à translater par un entier relatif, on peut supposer $\alpha = \frac{1}{2}$: on a alors $\frac{1}{4} - d\beta^2 \in \mathbb{Z}$ avec $\beta \in \mathbb{Q}$, soit $1 - d\,(2\beta)^2 \in 4\mathbb{Z}$, ce qui implique d'une part $2\beta \in \mathbb{Z}$ et $\beta \notin \mathbb{Z}$ et d'autre part $d \equiv 1 \pmod 4$; et réciproquement si on a ces conditions alors $\alpha + \beta\sqrt{d} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Bref, si $d \equiv 1 \pmod 4$ on a $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ et sinon $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$. ✓

3. Les deux questions suivantes sont indépendantes.

(1) Soit A la partie de $\mathbb{C}[t]$ formée des polynômes dont le coefficient de degré 1 (ou, si on préfère, la dérivée à l'origine) est nul : montrer que A est une sous-$\mathbb{C}$-algèbre de $\mathbb{C}[t]$, montrer qu'elle est de type fini sur $\mathbb{C}$, et montrer qu'elle n'est pas intégralement close.

(2) Soit A la partie de $\mathbb{C}[x,y]$ formée des polynômes n'ayant que des monômes de degré total pair (ou, si on préfère, vérifiant $p(-x,-y) = p(x,y)$) : montrer que A est une sous-$\mathbb{C}$-algèbre de $\mathbb{C}[x,y]$, montrer qu'elle est de type fini sur $\mathbb{C}$, et montrer qu'elle est intégralement close. Montrer cependant que A n'est pas un anneau factoriel.

Corrigé. (1) Manifestement, A est un sous-$\mathbb{C}$-espace vectoriel de $\mathbb{C}[t]$, contenant 1 : il s'agit donc de voir qu'elle est stable par multiplication. Or si $p, q \in \mathbb{C}[t]$ vérifient $p'(0) = 0$ et $q'(0) = 0$ alors $(pq)' = p'q + pq'$ s'annule aussi en 0. Ceci prouve que A est une sous-$\mathbb{C}$-algèbre de $\mathbb{C}[t]$. Pour s'assurer qu'elle est de type fini, on constate que $A = \mathbb{C}[t^2, t^3]$ (autrement dit, A est engendré, comme $\mathbb{C}$-algèbre, par t^2 et t^3) : c'est clair car $t^2, t^3 \in A$ et tout monôme t^n de degré n différent de 1 est produit d'une certaine puissance de t^2 et d'une certaine puissance de t^3 (il s'ensuit que toute somme de tels monômes, bref, tout élément de A, est dans $\mathbb{C}[t^2, t^3]$). Maintenant, A est un anneau intègre (comme sous-anneau de $\mathbb{C}[t]$ qui est intègre) donc on peut parler de son corps des fractions $K = \mathbb{C}(t^2, t^3)$, qu'on peut voir comme un sous-corps de $\mathbb{C}(t)$ (puisque A est un sous-anneau de $\mathbb{C}[t]$), et comme $t = (t^3)/(t^2)$ on voit que $t \in K$ donc manifestement $K = \mathbb{C}(t)$: c'est-à-dire que A a le même corps des fractions $\mathbb{C}(t)$ que $\mathbb{C}[t]$. Enfin, $t \in K$ est racine du polynôme unitaire $P(u) = u^2 - t^2 \in A[u]$, donc t est entier sur A, et comme $t \notin A$ on en déduit que A n'est pas intégralement clos.

(2) Tout d'abord, il y a bien équivalence entre dire que $p(-x,-y) = p(x,y)$ et dire que p n'a que des monômes de degré total pair : une implication est évidente, et quant à l'autre on voit facilement (à l'aide d'un développement à l'origine) que les monômes du plus petit degré impair s'annulent. Manifestement, A est un sous-$\mathbb{C}$-espace vectoriel de $\mathbb{C}[x,y]$, contenant 1 : il s'agit donc de voir qu'elle est stable par multiplication. Or si $p, q \in \mathbb{C}[x,y]$ vérifient $p(-x,-y) = p(x,y)$ et $q(-x,-y) = q(x,y)$ alors pq le vérifie aussi. Ceci prouve que A est une sous-$\mathbb{C}$-algèbre de $\mathbb{C}[x,y]$. Pour s'assurer qu'elle est de type fini, on constate que $A = \mathbb{C}[x^2, xy, y^2]$ (autrement dit, A est engendré, comme $\mathbb{C}$-algèbre, par x^2, xy et y^2) : c'est clair car

$x^2, xy, y^2 \in A$ et tout monôme $x^d y^{2n-d}$ de degré $2n$ est produit de puissances de ces monômes (il s'ensuit que toute somme de tels monômes, bref, tout élément de A, est dans $\mathbb{C}[x^2, xy, y^2]$). Maintenant, A est un anneau intègre (comme sous-anneau de $\mathbb{C}[x, y]$ qui est intègre) donc on peut parler de son corps des fractions $K = \mathbb{C}(x^2, xy, y^2)$, qu'on peut voir comme un sous-corps de $\mathbb{C}(x, y)$ (puisque A est un sous-anneau de $\mathbb{C}[x, y]$), et même du sous-corps K_0 du corps des fractions rationnelles $h \in \mathbb{C}(x, y)$ vérifiant $h(-x, -y) = h(x, y)$. Inversement, si $h \in K_0$ est une fraction rationnelle en les indéterminées x, y qui vérifie $h(-x, -y) = h(x, y)$ alors en écrivant $h = p/q$ où $p, q \in \mathbb{C}[x, y]$, on a soit $p(-x, -y) = p(x, y)$ et de même pour q (donc immédiatement $p/q \in K$) soit $p(-x, -y) = -p(x, y)$ et de même pour q et dans ce cas quitte à multiplier p et q par x on est ramené à $p/q \in K$: bref, K_0, le corps des fractions rationnelles vérifiant $h(-x, -y) = h(x, y)$, est le corps $K = \mathbb{C}(x^2, xy, y^2)$ des fractions de A. (On peut également remarquer que l'extension $\mathbb{C}(x, y)/\mathbb{C}(x^2, xy, y^2)$ est galoisienne de groupe de Galois $\mathbb{Z}/2\mathbb{Z}$ dont l'unique élément non trivial est $\sigma\colon h(x, y) \mapsto h(-x, -y)$.) Enfin, si $h \in K$ est entier sur A alors en particulier il est entier sur $\mathbb{C}[x, y]$ donc il appartient à $\mathbb{C}[x, y]$ (car $\mathbb{C}[x, y]$ est intégralement clos, étant factoriel), donc $h \in K \cap \mathbb{C}[x, y]$, c'est-à-dire que h est un polynôme à deux indéterminées vérifiant $h(-x, -y) = h(x, y)$, et ceci montre $h \in A$. Donc A est bien intégralement clos. Pour finir, A n'est pas factoriel car les trois éléments x^2, xy, y^2 sont irréductibles mais le carré de l'un est égal au produit des deux autres, $(xy)^2 = (x^2)(y^2)$, ce qui contredit l'unicité de la décomposition en facteurs irréductibles. ✓

4. (1) On rappelle que le radical (de Jacobson) $\operatorname{rad} A$ d'un anneau (commutatif) A est l'intersection de tous ses idéaux maximaux. Montrer que $x \in A$ est dans $\operatorname{rad} A$ si et seulement si pour tout $a \in A$ on a $1 + ax \in A^\times$ (où $A^\times$ désigne le groupe des unités — c'est-à-dire les éléments inversibles de A).

(2) On appelle nilradical $\operatorname{Nil} A$ d'un anneau (commutatif) A l'intersection de tous ses idéaux premiers[2]. Montrer que $\operatorname{Nil} A$ est l'ensemble des éléments nilpotents de A. (Indication : on pourra être amené à considérer, donné $x \in A$ non nilpotent, un élément maximal pour l'inclusion parmi les idéaux ne contenant aucune puissance de x — et montrer que cet idéal est premier.)

(3) Manifestement, $\operatorname{Nil} A \subseteq \operatorname{rad} A$ pour tout anneau (commutatif) A (pourquoi ?). Montrer que si A est un anneau *artinien*, c'est-à-dire que toute suite d'idéaux décroissante pour l'inclusion stationne, alors il y a égalité. (Indication : si $\mathfrak{R} = \operatorname{rad} A$, on considérera la suite décroissante $\mathfrak{R}^k$ des puissances de l'idéal $\mathfrak{R}$ et on appliquera le lemme de Nakayama. Pour simplifier, on pourra admettre le résultat suivant : tout anneau artinien est noethérien.)

(4) Montrer que si A est un anneau (commutatif) quelconque alors $\operatorname{rad}(A[t]) = \operatorname{Nil}(A[t]) = (\operatorname{Nil} A)[t]$. (On montrera d'abord que $(A/\operatorname{Nil} A)[t]$ est réduit, puis on utilisera les critères prouvés en (1) et (2).)

Corrigé. (1) Supposons par l'absurde que $x \in \operatorname{rad} A$ et que pour un certain $a \in A$ l'élément $1 + ax$ n'est pas une unité : alors $1 + ax$ engendre un idéal strict de A qui est donc contenu dans un idéal maximal $\mathfrak{m}$. Comme $x \in \operatorname{rad} A \subseteq \mathfrak{m}$ on a $ax \in \mathfrak{m}$ donc $1 = (1 + ax) - (ax) \in \mathfrak{m}$, ce qui est une contradiction.

Réciproquement, supposons $x \notin \mathfrak{m}$ pour un certain idéal maximal $\mathfrak{m}$ de A. Alors $A/\mathfrak{m}$ est un corps (car il n'a aucun idéal strict autre que $\{0\}$), donc il existe $\bar{a} \in A/\mathfrak{m}$ tel que $\bar{a} \cdot \bar{x} = -1$, ce qui donne $1 + ax \in \mathfrak{m}$ (où a est un relèvement quelconque de $\bar{a}$) donc $1 + ax$ n'est pas une unité.

[2] Un idéal (strict) $\mathfrak{p}$ est dit premier lorsque $A/\mathfrak{p}$ est un anneau intègre, ou, de façon équivalente, lorsque $xy \in \mathfrak{p}$ implique $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$.

(2) Si $x \in A$ est nilpotent, disons $x^n = 0$, alors pour tout idéal premier $\mathfrak{p}$ de A on a $x \in \mathfrak{p}$ (cela se voit en utilisant la propriété $(xy \in \mathfrak{p}) \implies (x \in \mathfrak{p}) \vee (y \in \mathfrak{p})$ et une récurrence immédiate sur n). Donc $x \in \operatorname{Nil} A$.

Réciproquement, supposons que $x \in A$ n'est pas nilpotent. Alors il existe des idéaux disjoints de $\{x^n : n \in \mathbb{N}\}$ (par exemple, l'idéal nul vérifie cette condition). Soit $\mathfrak{p}$ un idéal maximal pour l'inclusion parmi ceux-ci (on applique ici le lemme de Zorn). Montrons que $\mathfrak{p}$ est premier. Pour cela, supposons $y \notin \mathfrak{p}$ et $z \notin \mathfrak{p}$: alors par maximalité de $\mathfrak{p}$, il existe une puissance x^m de x telle que $x^m = ay + p$ avec $a \in A$ et $p \in \mathfrak{p}$ (en effet, l'idéal $(y) + \mathfrak{p} = \{ay + p : a \in A, p \in \mathfrak{p}\}$, engendré par $\mathfrak{p}$ et y, n'est pas disjoint de l'ensemble des puissances de x), et de même il existe une puissance x^n de x qui s'écrit $x^n = bz + q$ avec $b \in A$ et $q \in \mathfrak{p}$. On a alors $x^{mn} = abxy + r$ avec $r = ayq + bzp + pq \in \mathfrak{p}$, donc $xy \notin \mathfrak{p}$. On a donc montré que $\mathfrak{p}$ est premier, et comme $x \notin \mathfrak{p}$, on a $x \notin \operatorname{Nil} A$.

(3) On a $\operatorname{Nil} A \subseteq \operatorname{rad} A$ car tout idéal maximal est premier.

Supposons maintenant A artinien. Soit $\mathfrak{R} = \operatorname{rad} A$, et considérons la suite $\mathfrak{R}^k$ des puissances successives de l'idéal $\mathfrak{R}$. Comme A est artinien, cette suite doit stationner, disons $\mathfrak{R}^k = \mathfrak{R}^{k+1}$: appelons $\mathfrak{R}^\infty = \mathfrak{R}^N$ la valeur à laquelle elle stationne. Si on admet que tout anneau artinien est noethérien, alors $\mathfrak{R}$, étant un sous-module du module de type fini A sur l'anneau noethérien A, est de type fini, donc le lemme de Nakayama permet de conclure de $\mathfrak{R}^\infty = \mathfrak{R} \cdot \mathfrak{R}^\infty$ qu'on a $\mathfrak{R}^\infty = 0$: donc le produit de N éléments quelconques de $\mathfrak{R}$ est nul, et en particulier tout élément de $\mathfrak{R}$ est nilpotent ce qui prouve $\mathfrak{R} \subseteq \operatorname{Nil} A$, d'où l'égalité.

Expliquons comment faire sans admettre que tout anneau artinien est noethérien. Supposons par l'absurde que $\mathfrak{R}^\infty \neq 0$. Considérons l'ensemble $\mathscr{L}$ des idéaux *de type fini* L tels que $\mathfrak{R}^\infty \cdot L \neq 0$. Manifestement $\mathscr{L}$ n'est pas vide : l'anneau A tout entier appartient à $\mathscr{L}$. Soit maintenant L un élément *minimal* (pour l'inclusion) de $\mathscr{L}$: un tel élément existe puisque A est artinien (donc tout ensemble non vide d'idéaux a un élément minimal). Prouvons maintenant $\mathfrak{R} \cdot L = L$. Pour cela, soit $x \in \mathfrak{R}^\infty \cdot L$ non nul : comme $\mathfrak{R} \cdot \mathfrak{R}^\infty = \mathfrak{R}^\infty$, on peut écrire $x = \sum_i y_i z_i t_i$ où $y_i \in \mathfrak{R}$, $z_i \in \mathfrak{R}^\infty$ et $t_i \in L$; soit alors L' l'ideal (de type fini) engendré par les $y_i t_i$: manifestement, $L' \subseteq L$ et même $L' \subseteq \mathfrak{R} \cdot L$, et par ailleurs $\mathfrak{R}^\infty \cdot L' \neq 0$ (puisqu'il contient x) ; par minimalité de L on a alors $L' = L$ donc $\mathfrak{R} \cdot L = L$ et le lemme de Nakayama donne $L = 0$ ce qui est absurde, d'où la conclusion souhaitée $\mathfrak{R}^\infty = 0$.

(4) Tout d'abord, remarquons que $A/\operatorname{Nil} A$ est un anneau réduit (il n'a pas de nilpotents non nuls car ceux-ci seraient nilpotents dans A donc seraient dans $\operatorname{Nil} A$). Il s'ensuit que $(A/\operatorname{Nil} A)[t]$ est aussi un anneau réduit, et c'est aussi $A[t]/(\operatorname{Nil} A)[t]$. Il s'ensuit que $(\operatorname{Nil} A)[t] \supseteq \operatorname{Nil}(A[t])$, et l'inclusion réciproque est évidente. Par ailleurs, on sait qu'on a toujours $\operatorname{Nil}(A[t]) \subseteq \operatorname{rad}(A[t])$, et on va prouver l'inclusion réciproque. Soit donc $f(t) = c_0 + \cdots + c_n t^n \in \operatorname{rad}(A[t])$: le critère de la question (1) permet d'affirmer que $1 + tf(t) \in A[t]^\times$, c'est-à-dire $1 + c_0 t + \cdots + c_n t^{n+1} \in A[t]^\times$. Soit maintenant $\mathfrak{p}$ un idéal premier : comme $1 + tf(t)$ doit être inversible dans $(A/\mathfrak{p})[t]$ et que les seuls polynômes inversibles sur un anneau intègre (ici $A/\mathfrak{p}$) sont les constantes, on voit que $c_0, \ldots, c_n \in \mathfrak{p}$ (ils sont nuls dans $A/\mathfrak{p}$). Ceci étant vrai pour tout idéal premier $\mathfrak{p}$, on a $c_0, \ldots, c_n \in \operatorname{Nil} A$. ✓

Motivations : L'exercice 1 est la conséquence la plus classique du lemme de Nakayama. L'exercice 2 est un fait fondamental de théorie algébrique des nombres. L'exercice 3 a une interprétation en géométrie algébrique (l'anneau A du (1) est l'anneau des fonctions sur une courbe cubique cuspidale tandis que celui du (2) est l'anneau des fonctions sur un cône quadratique ; on montre donc essentiellement qu'une courbe cuspidale n'est pas normale mais qu'un cône quadratique l'est). L'exercice 4 est important à plusieurs titres : d'une part, si on appelle *anneau de Jacobson* un anneau dans lequel le nilradical coïncide avec le radical de Jacobson, alors la substance algébrique du théorème des zéros de Hilbert (Nullstellensatz) est le fait qu'une algèbre de type fini sur un corps est un anneau de Jacobson ; le (4) est un théorème de Snapper ; d'autre part, il y a des généralisations aux anneaux non nécessairement commutatifs du radical de Jacobson (l'intersection de tous les idéaux maximaux à gauche, qui se trouve être aussi l'intersection de tous les idéaux maximaux à droite) et aussi du nilradical (la somme

de tous les idéaux bilatères nils, c'est-à-dire dont tous les éléments sont nilpotents, est appelée le nilradical supérieur, c'est un idéal bilatère nil, mais il ne contient pas nécessairement tous les éléments nilpotents ; il existe aussi un nilradical inférieur), et le fait est que dans un anneau artinien à gauche (ou à droite) le radical de Jacobson est nilpotent et coïncide avec le nilradical (inférieur ou supérieur).