1. On appelle *idéal premier minimal* d'un anneau A un idéal premier qui n'en contient strictement aucun autre. Par exemple, si A est intègre, l'idéal nul (0) est l'unique idéal premier minimal.

(1) Montrer que si $(\mathfrak{p}_\iota)$ est une famille (non vide) totalement ordonnée d'idéaux premiers de A, alors l'intersection $\bigcap_\iota \mathfrak{p}_\iota$ est encore un idéal premier. En déduire que dans un anneau quelconque il existe toujours au moins un idéal premier minimal. Mieux : montrer que tout idéal premier contient un idéal premier minimal.

(2) Montrer que si A est noethérien, ses idéaux premiers minimaux sont en nombre fini (on pourra, par exemple, supposer que la propriété est fausse et considérer un idéal maximal pour l'inclusion parmi les idéaux I tels que l'anneau quotient A/I ait une infinité de premiers minimaux : I ne peut pas être premier...).

(3) Soit A noethérien, et $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ ses idéaux premiers minimaux (on vient de voir qu'ils sont en nombre fini). Montrer que la dimension (de Krull) de A est le maximum des dimensions des $A/\mathfrak{p}_i$.

Corrigé. (1) Supposons que $x, y \in A$ vérifient $x, y \notin \bigcap_\iota \mathfrak{p}_\iota$. Alors il existe ι tel que $x \notin \mathfrak{p}_\iota$ et ι' tel que $y \notin \mathfrak{p}_{\iota'}$, mais quitte à remplacer $\mathfrak{p}_\iota$ et $\mathfrak{p}_{\iota'}$ par le plus petit des deux on peut supposer que $\iota' = \iota$, soit $x, y \notin \mathfrak{p}_\iota$. Puisque $\mathfrak{p}_\iota$ est premier, $xy \notin \mathfrak{p}_\iota$, donc $xy \notin \bigcap_\iota \mathfrak{p}_\iota$. Ceci prouve que $\bigcap_\iota \mathfrak{p}_\iota$ est un idéal premier.

L'ensemble $\operatorname{Spec} A$ des idéaux premiers de A, partiellement ordonné par l'inclusion, vérifie alors les hypothèses du lemme de Zorn : toute partie totalement ordonnée a un minorant. Il s'ensuit qu'il existe un idéal premier minimal.

Si $\mathfrak{p}$ est un idéal premier quelconque de A, le localisé $A_\mathfrak{p}$ (dans lequel on a inversé tous les éléments n'appartenant pas à $\mathfrak{p}$) a des idéaux premiers en correspondance naturelle avec ceux de A qui sont contenus dans $\mathfrak{p}$ (entre autres puisque $A_\mathfrak{p}/\mathfrak{q}A_\mathfrak{p} \cong (A/\mathfrak{q})_{\bar{\mathfrak{p}}}$ si $\mathfrak{q} \subseteq \mathfrak{p}$). Comme on vient de voir que ce localisé $A_\mathfrak{p}$ avait au moins un idéal premier minimal, c'est que $\mathfrak{p}$, dans A, contient un idéal premier minimal.

(2) Comme suggéré par l'énoncé, si A a un nombre infini d'idéaux premiers minimaux, soit I un idéal maximal pour l'inclusion parmi ceux tels que l'anneau quotient A/I ait une infinité de premiers minimaux : l'existence de I est garantie par la propriété noethérienne (et par le fait qu'on a supposé que (0) vérifiait la propriété). Manifestement, I ne peut pas être premier, puisque les anneaux intègres ont un unique idéal premier minimal (à savoir (0)). Soient donc x et y dans A tels que $x, y \notin I$ mais $xy \in I$. Les idéaux premiers minimaux de A/I s'identifient de façon évidente aux idéaux premiers de A contenant I et minimaux pour cette propriété (pour simplifier, appelons « minimaux sur I » de tels idéaux). Or si $\mathfrak{p}$ est un idéal premier contenant I (et notamment un idéal premier minimal sur I), comme il contient xy, il doit contenir soit x soit y ; mais un idéal premier minimal sur I qui contient x (resp. y) est manifestement minimal sur $I + (x)$ (resp. $I + (y)$). Donc les idéaux premiers minimaux sur I sont tous minimaux sur $I + (x)$ ou $I + (y)$. Mais par maximalité de I, ceux-ci sont en nombre fini : on a trouvé une contradiction.

(3) On vient de voir que tout idéal premier de A contient un des $\mathfrak{p}_i$; en particulier, si $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \subsetneq \cdots \subsetneq \mathfrak{q}_d$ est une chaîne d'idéaux premiers de A, elle contient nécessairement un des $\mathfrak{p}_i$ (au sens où chaque $\mathfrak{q}_j$ le contient), donc s'identifie à une chaîne d'idéaux premiers de $A/\mathfrak{p}_i$, et réciproquement. Ceci démontre ce qu'on voulait. ✓

2. Soit A un anneau noethérien, et $x \in A$ qui ne soit pas inversible. Montrer que tout idéal premier $\mathfrak{p} \subsetneq (x)$ est minimal (cf. l'exercice précédent) : on pourra, pour commencer, se ramener à A intègre, puis constater que $\mathfrak{p} = x\mathfrak{p}$ et appliquer (un corollaire de) Cayley-Hamilton.

Corrigé. Supposons par l'absurde qu'il y ait $\mathfrak{q} \subsetneq \mathfrak{p} \subsetneq (x)$ avec $\mathfrak{q}$ premier : quitte à quotienter par $\mathfrak{q}$ on peut supposer se ramener à $\mathfrak{q} = (0)$, c'est-à-dire supposer que A est intègre. Tout élément $y \in \mathfrak{p}$ s'écrit xz par hypothèse, et comme $x \not\in \mathfrak{p}$ et que $\mathfrak{p}$ est premier, on a $z \in \mathfrak{p}$: ceci montre $\mathfrak{p} = x\mathfrak{p}$. On sait alors (en appliquant Cayley-Hamilton à l'endomorphisme identité sur le module de type fini $\mathfrak{p}$) qu'il existe $b \in (x)$ tel que $(1-b)\mathfrak{p} = 0$. Mais par intégrité de A, on doit avoir $b = 1$, ce qui contredit le fait que x n'est pas inversible. ✓

3 (longueur d'un module). Si A est un anneau, on appelle *simple* un A-module non nul qui n'admet pas d'autre sous-module que 0 et lui-même : de façon équivalente, il s'agit d'un module isomorphe à $A/\mathfrak{m}$ avec $\mathfrak{m}$ un idéal maximal de A. On appelle *suite de composition* ou *suite de Jordan-Hölder* d'un A-module M une suite $0 = M_0 \subset M_1 \subset \cdots \subset M_\ell = M$ avec chaque M_{i+1}/M_i simple.

(1) Montrer que la longueur d'une suite de composition est indépendante du choix de celle-ci. (Procéder par récurrence sur la longueur d'une suite de composition, de façon analogue au théorème de Jordan-Hölder pour les groupes.)

On peut donc définir la *longueur* d'un A-module M comme la longueur de n'importe quelle suite de composition (avec $\ell(M) = \infty$ si une suite de composition n'existe pas).

(2) Si $A = k$ est un corps, quelle est la longueur d'un k-espace vectoriel vu comme A-module ? Si $A = \mathbb{Z}$, quelle est la longueur du $\mathbb{Z}$-module $\mathbb{Z}/4\mathbb{Z}$?

(3) Montrer que si M est un A-module et $M' \subseteq M$ un sous-module, alors M admet une suite de composition si et seulement si M' et M/M' en admettent, et qu'alors on a $\ell(M) = \ell(M') + \ell(M/M')$.

(4) Si A est un anneau local[1] noethérien d'idéal maximal $\mathfrak{m}$, montrer que pour tout d le A-module $A/\mathfrak{m}^d$ a une longueur finie, i.e., admet une suite de composition. (Indication : montrer que c'est le cas de $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ pour chaque entier i en le considérant comme un espace vectoriel sur $k = A/\mathfrak{m}$.)

(5) Soit A un anneau noethérien tel que tout idéal premier de A soit maximal : montrer que A a une longueur finie (i.e., admet une suite de composition) comme A-module. (Indication : considérer un idéal I maximal pour la propriété que A/I soit un A-module de longueur infinie, et montrer que I est premier.)

Corrigé. (1) On suppose que M admet une suite de composition $0 = M_0 \subset M_1 \subset \cdots \subset M_\ell = M$ de longueur ℓ et on cherche à prouver, par récurrence sur ℓ, que toute suite de composition a cette même longueur. Si $\ell = 1$, c'est-à-dire que M est simple, le résultat est clair (et le cas $\ell = 0$ l'est encore plus...). Dans le cas général, soit $0 = N_0 \subset N_1 \subset \cdots \subset N_r = M$ une suite de composition de longueur r. À présent, M/M_1 admet une suite de composition de longueur $\ell - 1$, à savoir $0 = M_1/M_1 \subset \cdots \subset M_i/M_1 \subset M_\ell/M_1 = M/M_1$. Pour ce qui est des N_j, on a soit $N_j \cap M_1 = 0$ soit $N_j \cap M_1 = M_1$, et trivialement N_0 est dans le premier cas et N_r est dans le second. Il existe donc un unique j_0 tel que $N_{j_0} \cap M_1 = 0$ et $N_{j_0+1} \cap M_1 = M_1$: alors N_{j_0} s'envoie naturellement dans N_{j_0+1}/M_1, et ce morphisme est injectif (puisque son noyau est $N_{j_0} \cap M_1 = 0$), mais aussi surjectif puisque $(N_{j_0+1}/M_1)/\bar{N}_{j_0} = (N_{j_0+1}/N_{j_0})/\bar{M}_1$ et que $\bar{M}_1$ (l'image de l'injection de M_1 dans N_{j_0+1}/N_{j_0}) n'est pas nulle dans le module simple N_{j_0+1}/N_{j_0}. Ainsi, $N_{j_0} \cong N_{j_0+1}/M_1$, et on a une suite de composition de longueur $r-1$ de M/M_1, à savoir $0 = N_0 \subset \cdots \subset N_{j_0} \subset N_{j_0+2}/M_1 \subset \cdots \subset N_r/M_1 = M/M_1$. Par hypothèse de récurrence, $r - 1 = \ell - 1$ donc $r = \ell$.

(2) Si k est un corps, les k-modules simples sont les espaces vectoriels de dimension 1,

(1) On rappelle qu'un anneau local est, par définition, un anneau ayant un unique idéal maximal $\mathfrak{m}$ (ou, ce qui revient au même, un idéal $\mathfrak{m}$ tel que tout élément du complémentaire de $\mathfrak{m}$ soit inversible).

donc la longueur d'un k-espace vectoriel est simplement sa dimension. Si $A = \mathbb{Z}$, le $\mathbb{Z}$-module $\mathbb{Z}/4\mathbb{Z}$ a la longueur 2 puisque $0 \subset \mathbb{Z}/2\mathbb{Z} \subset \mathbb{Z}/4\mathbb{Z}$ en est une suite de composition.

(3) Si M admet une suite de composition $0 = M_0 \subset \cdots \subset M_\ell = M$ alors tout sous-module M' de M en admet aussi une, puisque la suite des $M_i \cap M'$, soit $0 = M_0 \cap M' \subseteq \cdots \subseteq M_\ell \cap M' = M'$, si elle n'est pas une suite de composition, a des quotients successifs $(M_{i+1} \cap M')/(M_i \cap M') \subseteq M_{i+1}/M_i$ qui sont soit simples soit nuls — et dans ce dernier cas on peut les supprimer pour obtenir une suite de composition. De même, si $M'' = M/M'$ est un quotient de M, en prenant l'image d'une suite de composition de M par la surjection canonique on obtient une suite de sous-modules de M'' qui, une fois supprimées les redondances, donne une suite de composition.

Réciproquement, si M' et $M'' = M/M'$ admettent des suites de composition, disons $0 = M'_0 \subset \cdots \subset M'_{\ell'} = M'$ et $0 = M''_0 \subset \cdots \subset M''_{\ell''} = M''$, alors on obtient une suite de composition de M en les concaténant de la façon suivante : si $i \leq \ell'$, on pose $M_i = M'_i$, et si $i \geq \ell'$ on appelle M_i l'image réciproque de $M''_{i-\ell'}$ par la surjection canonique $M \twoheadrightarrow M''$ (ces deux définitions donnent bien $M_{\ell'} = M'$. Il est facile de voir que $0 = M_0 \subset \cdots \subset M_{\ell'+\ell''} = M$ est bien une suite de composition de M, donc on a prouvé $\ell(M) = \ell' + \ell''$.

(4) D'après la question (3), pour montrer que $A/\mathfrak{m}^d$ est de longueur finie, comme A-module, pour tout i, il suffit de le montrer pour chaque $\mathfrak{m}^i/\mathfrak{m}^{i+1}$. Or celu-ci est un k-espace vectoriel (où $k = A/\mathfrak{m}$) de type fini (puisque c'est un A-module de type fini annulé par $\mathfrak{m}$), c'est-à-dire de dimension finie, c'est-à-dire de longueur finie (comme k-module). Or dire que $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ est de longueur finie comme k-module revient manifestement à dire qu'il l'est comme A-module.

(5) Supposons par l'absurde que A soit un anneau noethérien dont tous les idéaux premiers sont maximaux, et qui n'est pourtant pas de longueur finie (comme module sur lui-même). Il alors des idéaux I (par exemple 0 lui-même) tels que A/I soit un A-module de longueur infinie : soit I maximal vérifiant cette propriété, et $B = A/I$ l'anneau quotient. On va prouver que B est intègre (c'est-à-dire que I est premier). Soient (par l'absurde) x, y deux éléments non nuls de B tels que $xy = 0$: alors $B/(x) = A/(I + (x))$ est un A-module de longueur finie par maximalité de I, et $B/(y)$ aussi ; mais (x) (l'idéal premier de B engendré par x) est l'image de B par l'application A-linéaire de multiplication par x, et le noyau de cette application contient y, c'est-à-dire qu'on a une surjection $B/(y) \twoheadrightarrow (x)$ de A-module, donc (x) est de longueur finie puisque $B/(y)$ l'est : mais si (x) et $B/(x)$ sont de longueur finie, B l'est, et on a trouvé une contradiction. C'est donc que I est premier, et par hypothèse il est maximal : alors $k = A/I$ est un corps donc de longueur finie (exactement 1) comme k-module, mais donc aussi de longueur finie comme A-module : de nouveau, une contradiction. ✓

4 (Hauptidealsatz de Krull). Soit A un anneau local noethérien intègre d'idéal maximal $\mathfrak{m}$. On suppose que, pour un certain $x \in A$, l'idéal $(x) = xA$ a pour radical $\mathfrak{m}$. On se propose de montrer que, dans ces conditions, la dimension (de Krull) de A est 1. Pour cela, on aura besoin de la notion de *longueur* d'un module, introduite à l'exercice précédent.

(1) Expliquer pourquoi il s'agit de prouver que : si $\mathfrak{p}$ est un idéal premier non nul de A, alors $\mathfrak{p} = \mathfrak{m}$, et pourquoi pour cela il suffit de vérifier $x \in \mathfrak{p}$.

(2) Soit $z \in \mathfrak{p} \setminus \{0\}$. En notant $(z) \div x^n = \{t \in A | tx^n \in (z)\}$ (idéal de A), montrer que $((z) \div x^n)/(z) \cong ((x^n) \div z)/(x^n)$.

(3) Pourquoi existe-t-il n_0 tel que $(z) \div x^n = (z) \div x^{n_0}$ pour tout $n \geq n_0$?

(4) Montrer que $A/(x^n)$ est de longueur finie, en utilisant le (5) de l'exercice n°3.

(5) En déduire que si $n \geq n_0$ alors $\ell(A/(x^n)) - \ell(A/((x^n) \div z))$ est constant, où ℓ désigne la longueur.

(6) Montrer que $A/((x^n) \div z) \cong ((x^n) + (z))/(x^n)$.

(7) En déduire que $(x^n) + (z) = (x^{n_0}) + (z)$ si $n \geq n_0$.

(8) Rappeler pourquoi $1 - ux$ est inversible pour tout $u \in A$, et déduire de ce qui précède que $x \in \mathfrak{p}$.

(∞) Si A est un anneau noethérien intègre (plus nécessairement local) et $x \in A$, montrer que si $\mathfrak{p}$ est un idéal premier minimal contenant x (cf. exercice n°1), il n'existe pas de chaînes d'idéaux premiers $(0) \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$, aboutissant à $\mathfrak{p}$, de longueur ≥ 2 (comparer ce résultat à la conclusion de l'exercice 2 !).

Corrigé. (1) Montrer que la dimension est 1 signifie qu'il n'y a pas de chaînes d'idéaux premiers de longueur ≥ 2. Mais comme toute chaîne d'idéaux premiers doit avoir pour extrémités l'unique idéal premier minimal (0) et l'unique idéal maximal $\mathfrak{m}$, il s'agit de montrer qu'on ne peut pas intercaler de $(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$, c'est-à-dire, montrer que tout idéal premier non nul $\mathfrak{p}$ de A est égal à $\mathfrak{m}$. Or si $x \in \mathfrak{p}$, on a $\mathfrak{p} \supseteq (x)$ donc $\mathfrak{p} \supseteq \sqrt{(x)}$ (puisque $\mathfrak{p}$ est premier), c'est-à-dire $\mathfrak{p} = \mathfrak{m}$ comme souhaité.

(2) Si $rx^n = sz$ alors r et s se déterminent mutuellement puisque A est intègre. Cette flèche $r \mapsto s$ détermine un isomorphisme $(z) \div x^n \xrightarrow{\sim} (x^n) \div z$, et par passage au quotient $((z) \div x^n)/(z) \xrightarrow{\sim} ((x^n) \div z)/(x^n)$.

(3) L'anneau A est noethérien et la suite d'idéaux $((z) \div x^n)$ est croissante, donc elle stationne.

(4) Un idéal premier de l'anneau $A/(x^n)$ correspond à un idéal premier de A contenant x^n, mais un tel idéal doit contenir $\sqrt{(x^n)} = \mathfrak{m}$, donc c'est $\mathfrak{m}$. Autrement dit, tout idéal premier de $A/(x^n)$ est maximal : ainsi, d'après la question (5) de l'exercice n°3, $A/(x^n)$ est de longueur finie comme module sur lui-même, donc aussi comme module sur A (une suite de composition comme $A/(x^n)$-module est aussi une suite de composition comme A-module).

(5) De la suite exacte courte $0 \to ((x^n) \div z)/(x^n) \to A/(x^n) \to A/((x^n) \div z) \to 0$ et de l'additivité des longueurs (question (3) de l'exercice précédent) on déduit que $\ell(((x^n) \div z)/(x^n)) = \ell(A/(x^n)) - \ell(A/((x^n) \div z))$, d'après (2) c'est encore $\ell(((z) \div x^n)/(z))$, et d'après (3) la quantité en question est constante pour $n \geq n_0$.

(6) L'application $t \mapsto tz$ définit un isomorphisme $A/((x^n) \div z) \xrightarrow{\sim} ((x^n) + (z))/(x^n)$.

(7) D'après (5) et (6) mis ensemble, $\ell(A/(x^n)) - \ell(((x^n)+(z))/(x^n))$ est constant pour $n \geq n_0$. Mais, de nouveau d'après l'additivité des longueurs, c'est $\ell(A/((x^n) + (z)))$. Donc, de nouveau, $\ell((((x^n) + (z)))/((x^{n_0}) + (z))) = 0$ pour tout $n \geq n_0$. Donc $(((x^n) + (z)))/((x^{n_0}) + (z)) = 0$. Donc $(x^n) + (z) = (x^{n_0}) + (z)$. En particulier, on peut écrire $x^{n_0} = ux^{n_0+1} + vz$, c'est-à-dire $x^{n_0}(1 - ux) \in (z)$.

(8) On a $x \in \mathfrak{m}$, donc $ux \in \mathfrak{m}$, c'est-à-dire que $1 - ux$ est inversible. On en déduit $x^{n_0} \in (z) \subseteq \mathfrak{p}$, donc $x \in \mathfrak{p}$, ce qui conclut.

(∞) L'anneau localisé $A_{\mathfrak{p}}$ est local intègre, avec pour idéal maximal $\mathfrak{p}A_{\mathfrak{p}}$, donc on peut lui appliquer ce qui précède ! Une chaîne d'idéaux premiers $(0) \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$ de longueur ≥ 2 donnerait une chaîne correspondante dans $A_{\mathfrak{p}}$, or on vient de voir que celui-ci était de dimension ≤ 1. ✓

5. Soit A la sous-algèbre de $k[x_1, \ldots, x_n]$ formée des polynômes dont tous les monômes sont de degré multiple de r. Quelle est la dimension (de Krull) de A ?

Corrigé. L'anneau $k[x_1, \ldots, x_n]$ est entier sur A : en effet, chaque x_i vérifie l'équation de dépendance intégrale $(x_i)^r = (x_i^r)$ (cet élément est dans A). Donc la dimension de A est celle de $k[x_1, \ldots, x_n]$, c'est-à-dire n. ✓