ALGÈBRE COMMUTATIVE III : CORRIGÉ

Exercice 1 — Soit A un anneau noethérien. Notons que tout ensemble non vide d'idéaux de A admet nécessairement un élément maximal puisqu'il n'existe pas de chaîne strictement croissante d'idéaux dans A...

1) Supposons qu'il existe un idéal de A ne contenant le produit d'aucune famille finie d'idéaux premiers et soit $\mathfrak{I}$ maximal pour cette condition. Comme $\mathfrak{I}$ n'est manifestement pas un idéal premier, il existe $x,y \in \mathrm{A}-\mathfrak{I}$ tels que $xy \in \mathfrak{I}$ et on obtient ainsi une contradiction puisque le produit des idéaux $(\mathfrak{I}+\mathrm{A}x)$ et $(\mathfrak{I}+\mathrm{A}y)$ est contenu dans $\mathfrak{I}$ alors que chacun d'eux contient le produit d'un nombre fini d'idéaux premiers. Tout idéal de A contient donc le produit d'un nombre fini d'idéaux premiers.

Remarque : il découle immédiatement de cette observation qu'un anneau noethérien ne contient qu'un nombre fini d'idéaux premiers minimaux. Il existe en effet des idéaux premiers $\mathfrak{p}_1,\ldots,\mathfrak{p}_n$ dont le produit est contenu (donc égal) à l'idéal nul ; tout idéal premier de A *contient par conséquent ce produit, ce qui implique qu'il contient nécessairement l'un des $\mathfrak{p}_i$ (sinon l'anneau* $\mathrm{A}/\mathfrak{p}$ *contiendrait des éléments non nuls $x_1,\ldots,x_n$ tels que $x_1\ldots x_n = 0$ et ne serait donc pas intègre...) et tout idéal premier* minimal *de* A *est donc l'un des $\mathfrak{p}_i$.*

2) (i) Soit M un A-module non nul et soit $\mathfrak{p}$ un idéal de A de la forme $\mathrm{Ann}(x)$ avec $x \in \mathrm{M}-\{0\}$, maximal pour cette condition. Quels que soient $a,b \in \mathrm{A}$ tels que $ab \in \mathfrak{p}$, $abx = 0$; si $a \notin \mathfrak{p}$, $ax \neq 0$ et $b \in \mathrm{Ann}(ax)$; comme $\mathrm{Ann}(x) \subset \mathrm{Ann}(ax)$, $\mathrm{Ann}(ax) = \mathrm{Ann}(x)$ par maximalité et donc $b \in \mathfrak{p}$. L'ensemble $\mathrm{Ass}_{\mathrm{A}}(\mathrm{M})$ des idéaux premiers associés à un A-module M non nul est donc non vide.

(ii) Si un idéal premier $\mathfrak{p}$ de A est associé à un A-module M, il existe par hypothèse $x \in \mathrm{M}$ tel que $\mathfrak{p} = \mathrm{Ann}(x)$; l'image de x dans $\mathrm{A}_{\mathfrak{p}}$ est alors non nulle et son annulateur est l'idéal premier (maximal) $\mathfrak{p}\mathrm{A}_{\mathfrak{p}}$ de $\mathrm{A}_{\mathfrak{p}}$.

Considérons réciproquement un idéal premier $\mathfrak{p}$ de A tel que $\mathfrak{p}\mathrm{A}_{\mathfrak{p}}$ soit associé à $\mathrm{M}_{\mathfrak{p}}$ et soient $x \in \mathrm{A}$, $s \in \mathrm{A}-\mathfrak{p}$ tels que $\mathfrak{p}\mathrm{A}_{\mathfrak{p}} = \mathrm{Ann}(s^{-1}x)$. On vérifie sans difficulté que l'annulateur de tx dans A est contenu $\mathfrak{p}$ quel que soit $t \in \mathrm{A}-\mathfrak{p}$ et que chaque élément de $\mathfrak{p}$ est contenu dans $\mathrm{Ann}(tx)$ pour un certain $t \in \mathrm{A}-\mathfrak{p}$; il existe donc $s' \in \mathrm{A}-\mathfrak{p}$ tel que $\mathfrak{p} \subset \mathrm{Ann}(tx)$ puisque l'idéal $\mathfrak{p}$ est de type fini et $\mathfrak{p} = \mathrm{Ann}(s'x)$ est ainsi un idéal premier associé à M.

(iii) L'ensemble des éléments a de A tels que l'homothétie $\mathrm{M} \xrightarrow{a\cdot} \mathrm{M}$ ne soit pas injective est précisément la réunion des idéaux $\mathrm{Ann}(x)$ de A lorsque x parcourt $\mathrm{M}-\{x\}$; ayant vérifié à la question 1 que tout élément maximal parmi ces idéaux est un idéal premier associé à M, il s'agit donc également de la réunion des idéaux premiers associés à M.

(iv) Si un élément a de A définit une homothétie nilpotente sur M, il existe un entier n tel que a^n appartienne à chacun des idéaux $\mathrm{Ann}(x)$, $x \in \mathrm{M}-\{0\}$, donc à chaque idéal premier associé à M, et a appartient ainsi à l'intersection de ces derniers.

Pour établir que, réciproquement, l'homothétie $\mathrm{M} \xrightarrow{a\cdot} \mathrm{M}$ induite par un élément a de A appartenant à l'intersection des idéaux premiers associés de M est nilpotente, on peut utiliser la suite de sous-modules $(0) = \mathrm{M}_0 \subset \mathrm{M}_1 \subset \ldots \subset \mathrm{M}_n = \mathrm{M}$ construite ci-dessous à la question 4 : a annule par hypothèse chacun des quotients $\mathrm{M}_i/\mathrm{M}_{i-1}$ et sa puissance n-ème annule par conséquent M.

3) Supposons A non nul et soit $\mathfrak{p}$ un idéal premier minimal de A. L'anneau $\mathrm{A}_{\mathfrak{p}}$ étant non nul, il possède un idéal premier associé et ce ne peut être que $\mathfrak{p}\mathrm{A}_{\mathfrak{p}}$ puisque le spectre de $\mathrm{A}_{\mathfrak{p}}$ est réduit à cet idéal premier ; vu la question 2 (ii), nous en déduisons que $\mathfrak{p}$ est un idéal premier associé à A.

4) (i) Si M est non nul, il possède un idéal premier associé $\mathfrak{p}_1$ et, si $x \in \mathrm{M}-\{0\}$ est tel que $\mathrm{Ann}(x) = \mathfrak{p}_1$, le sous-module $\mathrm{M}_1 = \mathrm{A}x$ de M est isomorphe à $\mathrm{A}/\mathfrak{p}_1$. Si $\mathrm{M}_1 = \mathrm{M}$, il n'y a plus rien à faire ; sinon, le même argument appliqué au A-module non nul M/M_1 conduit à un sous-module M_2 de M contenant M_1 et tel que $\mathrm{M}_2/\mathrm{M}_1$ soit isomorphe à $A/\mathfrak{p}_2$, où $\mathfrak{p}_2$ est un idéal premier associé à M/M_1. En itérant cette construction, nous obtenons une suite croissante $(\mathrm{M}_i)_{i\geq 1}$ de sous-modules de M dont les quotients successifs sont isomorphes à $\mathrm{A}/\mathfrak{p}_1$, $\mathfrak{p}_1 \in \mathrm{Spec}(\mathrm{A})$. Cette suite est stationnaire car M est un A-module noethérien (il est de type fini sur un anneau noethérien) et, si $\mathrm{M}_{n+1} = \mathrm{M}_n$, alors $\mathrm{Ass}(\mathrm{M}/\mathrm{M}_n) = \emptyset$ et donc $\mathrm{M} = \mathrm{M}_n$ en vertu de la question 1.

(ii) Soit $\mathfrak{p}$ un idéal premier associé à M et soit $x \in \mathrm{M} - \{0\}$ tel que $\mathfrak{p} = \mathrm{Ann}(x)$. Notant r le plus petit entier naturel tel que $x \in \mathrm{M}_r$ et désignant par $\bar{x}$ l'image de x dans $\mathrm{M}_r/\mathrm{M}_{r-1}$, $\mathfrak{p}$ est contenu dans l'annulateur de $\bar{x}$. On vérifie immédiatement que $\mathfrak{p}_r$ est l'annulateur de tout élément non nul de $\mathrm{A}/\mathfrak{p}_r$ et $\mathfrak{p}$ est donc contenu dans $\mathfrak{p}_r$.
Remarque : en particulier, tout A*-module noethérien ne possède qu'un nombre* fini *d'idéaux premiers associés.*

Exercice 2 — 1) Étant donné un élément x de B, on désigne par $\mathrm{A}[x]$ la sous-A-algèbre de B engendrée par x ; c'est l'image de l'unique A-homomorphisme $\mathrm{A}[\mathrm{T}] \to \mathrm{B}$ envoyant T sur x.

(i) $\Rightarrow$ (ii). Si x est entier sur A, il existe $a_{n-1}, \ldots, a_0 \in \mathrm{A}$ tels que

$$x^n + \varphi(a_{n-1})x^{n-1} + \ldots + \varphi(a_0) = 0$$

et il est clair que $\mathrm{A}[x]$ est engendré par $1, x, \ldots, x^{n-1}$ en tant que A-module.

(ii) $\Rightarrow$ (iii). Cette implication est triviale.

(iii) $\Rightarrow$ (i). Soient $t_1, \ldots, t_n$ des générateurs de C en tant que A-module. Il existe par hypothèse des éléments a_{ij} de A tels que $xt_j = \sum_i \varphi(a_{ij})t_i$ $(1 \leq i \leq n)$; les formules de Cramer fournissent dans ces conditions une matrice $\mathrm{Q} \in \mathrm{M}_n(\mathrm{A})$ telle que

$$\mathrm{Q}(x\mathrm{I}_n - (\varphi(a_{ij}))) = \det(x\mathrm{I}_n - (\varphi(a_{ij})))\mathrm{I}_n$$

et l'élément $\det(x\mathrm{I}_n - (\varphi(a_{ij})))$ de B annule donc le A-module C. On en déduit $\det(x\mathrm{I}_n - (\varphi(a_{ij}))) = 0$ car $1 \in \mathrm{C}$ et il suffit de développer ce déterminant pour obtenir une relation de dépendance intégrale de x sur A.

2) Soient x, y deux éléments de B entiers sur A. La sous-A-algèbre $\mathrm{A}[x,y]$ de B engendrée par x et y est un A-module de type fini (si x et y sont annulés par des polynômes unitaires de $\mathrm{A}[\mathrm{T}]$ de degrés respectifs n et m, $\mathrm{A}[x,y]$ est engendré en tant que A-module par les $x^i y^j$, $0 \leq i \leq n-1$, $0 \leq j \leq m-1$). Comme les éléments $x+y$ et xy de B appartiennent à $\mathrm{A}[x,y]$, ils sont entiers sur A en vertu du critère (iii) de la question précédente.

L'ensemble A' des éléments de B entiers sur A est une sous-A-algèbre de B d'après ce qui précède. Étant donnée une B-algèbre C, un élément de C entier sur A est *a fortiori* entier sur A' ; réciproquement, si $x \in \mathrm{C}$ est entier sur A', il existe par hyptohèse des éléments $a'_{n-1}, \ldots, a'_0$ de A' tels que $x^n + a'_{n-1}x^{n-1} + \ldots + a'_0 = 0$; la sous-A-algèbre de C engendrée par $x, a'_{n-1}, \ldots, a'_0$ est alors un A-module de type fini et x est donc entier sur A.

3) Commençons par deux rappels.

– Un élément r de $\mathbb{Q}$ est entier sur $\mathbb{Z}$ si et seulement si $r \in \mathbb{Z}$ (vérification : si $r^n + a_{n-1}r^{n-1} + \ldots + a_0 = 0$, écrire r sous la forme a/b avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z} - \{0\}$ premiers entre eux et observer que multiplier la relation précédente par b^n permet d'obtenir que b divise a^n, ce qui n'est possible que si $b = \pm 1$ puisque a et b sont premiers entre eux).
– Soit D un entier naturel non nul sans facteur carré. Si l'on désigne par $\sqrt{\mathrm{D}}$ l'image de T dans l'anneau quotient $\mathrm{K} = \mathbb{Q}[\mathrm{T}]/(\mathrm{T}^2 - \mathrm{D})$, il découle directement de la division euclidienne que ce dernier est isomorphe à l'espace vectoriel $\mathbb{Q} \oplus \mathbb{Q}\sqrt{\mathrm{D}}$ muni de la structure d'anneau définie par

$$(a + b\sqrt{\mathrm{D}})(a' + b'\sqrt{\mathrm{D}}) = (aa' + bb'\mathrm{D}) + (ab' + a'b)\sqrt{\mathrm{D}} \ ;$$

il s'agit d'un corps puisque D n'est pas un carré dans $\mathbb{Q}$.

Soit $\mathscr{O}_\mathrm{K}$ le sous-anneau de K constitué des éléments entiers sur $\mathbb{Z}$ (c'est la *fermeture intégrale* de $\mathbb{Z}$ dans K). Il est manifeste que $\mathscr{O}_\mathrm{K}$ contient $\sqrt{\mathrm{D}}$ et donc l'anneau $\mathbb{Z}[\sqrt{\mathrm{D}}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{\mathrm{D}}$; en outre, si $\mathrm{D} \equiv 1 \bmod 4$, $\frac{\sqrt{\mathrm{D}}+1}{2}$ est également entier sur $\mathbb{Z}$ puisqu'il est annulé par le polynôme unitaire

$$\mathrm{T}^2 - \mathrm{T} + \frac{1 - \mathrm{D}}{4}$$

de $\mathbb{Z}[\mathrm{T}]$ et $\mathscr{O}_\mathrm{K}$ contient donc $\mathbb{Z}[\frac{\sqrt{\mathrm{D}}+1}{2}]$.

Soit réciproquement $x = a + b\sqrt{\mathrm{D}}$ un élément de K entier sur $\mathbb{Z}$.

Si $b = 0$, $x = a$ est un élément de $\mathbb{Q}$ entier sur $\mathbb{Z}$ et donc $x \in \mathbb{Z}$.

Si $b \neq 0$, le polynôme

$$(\mathrm{T} - (a + b\sqrt{\mathrm{D}}))(\mathrm{T} - (a - b\sqrt{\mathrm{D}})) = \mathrm{T}^2 - 2a\mathrm{T} + (a^2 - b^2\mathrm{D})$$

est irréductible sur $\mathbb{Q}$ et divise donc tout polynôme de $\mathbb{Q}[\mathrm{T}]$ annulant $a + b\sqrt{\mathrm{D}}$. Il en découle qu'un polynôme unitaire dans $\mathbb{Z}[\mathrm{T}]$ annulant $a + b\sqrt{\mathrm{D}}$ annule également $a - b\sqrt{\mathrm{D}}$ et donc $a - b\sqrt{\mathrm{D}} \in \mathscr{O}_\mathrm{K}$. Nous en déduisons que les nombres rationnels

$$2a = (a + b\sqrt{\mathrm{D}}) + (a - b\sqrt{\mathrm{D}}) \text{ et } a^2 - b^2\mathrm{D} = (a + b\sqrt{\mathrm{D}})(a - b\sqrt{\mathrm{D}})$$

sont entiers sur $\mathbb{Z}$ et donc sont des entiers.

Les conditions $2a \in \mathbb{Z}$ et $a^2 - b^2\mathrm{D} \in \mathbb{Z}$ impliquent immédiatement $(2b)^2\mathrm{D} \in \mathbb{Z}$; comme il est sans facteur carré, D ne peut compenser les facteurs premiers du dénominateurs de $2b$ et donc $2b \in \mathbb{Z}$. Si l'entier $2b$ est pair, $b \in \mathbb{Z}$; cela entraîne $a^2 \in \mathbb{Z}$ et donc $a \in \mathbb{Z}$, de sorte que $x \in \mathbb{Z}[\sqrt{\mathrm{D}}]$.

Si l'entier $2b$ est impair, $(2b)^2$ est congru à 1 modulo 4 et $\mathrm{D} \equiv (2a)^2$ est donc un carré modulo 4, ce qui implique $\mathrm{D} \equiv 0 \bmod 4$ ou $\mathrm{D} \equiv 1 \bmod 4$. Comme 4 ne divise pas D, $\mathrm{D} \equiv 1 \bmod 4$ et

$$a + b\sqrt{\mathrm{D}} = (a - b) + (2b)\frac{1+\sqrt{\mathrm{D}}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$$

car la condition $(2a)^2 \equiv 1 \bmod 4$ implique $2a \equiv 1,\ 3 \bmod 4$ et donc $2a - 2b \equiv 0 \bmod 2$.

Exercice 3 — Soient A un anneau et B une A-algèbre entière ; on note $\varphi : \mathrm{A} \to \mathrm{B}$ l'homomorphisme structural.

1) On suppose A et B intègres, φ injectif et on identifie A avec $\varphi(\mathrm{A})$.

Si A est un corps, B est un corps : tout élément x de B vérifie par hypothèse une relation de la forme

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

avec $a_i \in \mathrm{A}$; si x est non nul, l'intégrité de B implique l'existence de $p \in \{0, \ldots, n-1\}$ tel que $a_p \neq 0$ et $x(x^{n-p-1} + a_{n-1}x^{n-p-2} + \ldots + a_{p+1}) = -a_p$; A étant un corps, a_p est inversible et il en est de même de x.

Si B est un corps, A est un corps : tout élément non nul a de A est inversible dans B et il existe une relation

$$(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \ldots + a_0 = 0$$

avec $a_i \in \mathrm{A}$; en multipliant cette dernière par a^{n-1}, on obtient $a^{-1} \in \mathrm{A}$.

2) Soient $\mathfrak{p}$ et $\mathfrak{q}$ deux idéaux premiers de A tels que $\mathfrak{p} \subset \mathfrak{q}$; on suppose qu'il existe un idéal premier $\mathfrak{p}'$ de B tel que ${}^a\varphi(\mathfrak{p}') = \mathfrak{p}$ et il s'agit de prouver qu'il existe un idéal premier $\mathfrak{q}'$ de B tel que ${}^a\varphi(\mathfrak{q}') = \mathfrak{q}$.

On vérifie immédiatement que l'anneau $\mathrm{B}_\mathfrak{q}$ est entier sur l'anneau $\mathrm{A}_\mathfrak{q}$ et, le spectre de l'anneau $\mathrm{B}_\mathfrak{q}$ s'identifiant à l'ensemble des idéaux premiers $\mathfrak{q}'$ de B tels que ${}^a\varphi(\mathfrak{q}') \subset \mathfrak{q}$, il est loisible de supposer que l'anneau A est local, d'idéal maximal $\mathfrak{q}$; c'est ce que nous faisons.

L'homomorphisme structural $\varphi : \mathrm{A} \to \mathrm{B}$ induit un homomorphisme injectif $\mathrm{A}/\mathfrak{p} \to \mathrm{B}/\mathfrak{p}'$ faisant de $\mathrm{B}/\mathfrak{p}'$ une algèbre entière sur $\mathrm{A}/\mathfrak{p}$ (la vérification est immédiate). L'anneau local $\mathrm{A}/\mathfrak{p}$ n'est par hypothèse pas un corps ; en vertu de la question précédente, $\mathrm{B}/\mathfrak{p}'$ n'en est pas un non plus et il existe donc un idéal premier $\mathfrak{q}'$ de B contenant $\mathfrak{p}'$ et tel que ${}^a\varphi(\mathfrak{q}') \subset \mathfrak{q}$.

La conclusion découle maintenant d'une application du lemme de Zorn. L'ensemble des idéaux premiers $\mathfrak{b}$ de B tels que $\mathfrak{p} \subset^a \varphi(\mathfrak{b}) \subset \mathfrak{q}$ est non vide et inductif : la réunion d'une famille strictement ordonnée de tels idéaux satisfait encore à cette condition ; cet ensemble admet donc un élément maximal $\mathfrak{b}$ et on déduit de la discussion qui précède que nécessairement ${}^a\varphi(\mathfrak{b}) = \mathfrak{q}$.

3) Prouvons enfin que l'image de l'application ${}^a\varphi : \mathrm{Spec(B)} \to \mathrm{Spec(A)}$ est une partie fermée de $\mathrm{Spec(A)}$ et qu'il s'agit de tout $\mathrm{Spec(A)}$ lorsque φ est injectif.

Traitons pour commencer le cas d'un morphisme structural φ injectif. Il n'y a rien à démontrer lorsque $\mathrm{A} = 0$ car alors $0 = 1$ dans B, donc $\mathrm{B} = 0$ et les deux ensembles $\mathrm{Spec(A)}$, $\mathrm{Spec(B)}$ sont vides ; nous supposons $\mathrm{A} \neq 0$ dans ce qui suit. Quel que soit l'idéal premier $\mathfrak{p}$ de A, l'anneau est non nul $\mathrm{A}_\mathfrak{p}$ et se plonge dans l'anneau $\mathrm{B}_\mathfrak{p}$; ce dernier est donc également non nul et possède ainsi un idéal premier, ce qui fournit un idéal premier $\mathfrak{p}'$ de B tel que ${}^a\varphi(\mathfrak{p}') \subset \mathfrak{p}$. En particulier, nous obtenons ainsi que la fibre de l'application ${}^a\varphi$ est non vide au-dessus de tout idéal premier *minimal* de A, et il découle alors de la question précédente qu'elle est non vide au-dessus de *tout* point de $\mathrm{Spec(A)}$ puisque tout idéal premier de A contient un idéal premier minimal.

Passons maintenant au cas général. Désignant par $\mathfrak{a}$ le noyau de φ, il est immédiat de vérifier que B est une algèbre entière sur $\mathrm{A}/\mathfrak{a}$ et, la projection canonique $p : \mathrm{A} \to \mathrm{A}/\mathfrak{a}$ induisant un homéomorphisme de $\mathrm{Spec}(\mathrm{A}/\mathfrak{a})$

sur le fermé $\mathrm{V}(\mathfrak{a})$ de $\mathrm{Spec}(\mathrm{A})$, on tire du diagramme commutatif

$$\begin{tikzcd} & \mathrm{Spec}(\mathrm{B}) \arrow[dl] \arrow[d, "{}^a\varphi"] \\ \mathrm{Spec}(\mathrm{A}/\mathfrak{a}) \arrow[r, "{}^a p"] & \mathrm{Spec}(\mathrm{A}) \end{tikzcd}$$

que l'application ${}^a\varphi$ envoie $\mathrm{Spec}(\mathrm{B})$ sur $\mathrm{V}(\mathfrak{a})$.

Exercice 4 — L'assertion (i) revient à dire que l'anneau B^{G} est une A-algèbre de type fini et, si tel est le cas, l'assertion (ii) découle directement du théorème de stabilité de Hibert : toute algèbre de type fini sur un anneau noethérien est un anneau noethérien.

L'anneau B est entier sur la A-algèbre B^{G} des éléments de B invariants sous G : quel que soit en effet $b \in \mathrm{B}$, le polynôme $\prod_{g\in\mathrm{G}}(\mathrm{T} - g(b))$ est unitaire, annule B et est à coefficients dans B^{G} puisqu'il est manifestement invariant sous l'action de G ; comme ce polynôme annule b, b est entier sur B^{G}. Soient $x_1, \ldots, x_n$ des générateurs de B comme A-algèbre ; notant B_0 la sous-A-algèbre de B^{G} engendrée par les coefficients de polynômes unitaires annulant $x_1, \ldots, x_n$, il est immédiat que B est un module de type fini sur B_0. L'anneau A étant noethérien, il en est de même de la A-algèbre de type fini B_0 en vertu du théorème de Hilbert et tout sous-B_0-module de B est donc de type fini ; comme $\mathrm{B}_0 \subset \mathrm{B}^{\mathrm{G}}$, cela s'applique en particulier à B^{G} et cet anneau est donc finalement une algèbre de type fini sur A, engendrée par des générateurs de la A-algèbre B_0 et un nombre fini de générateurs de B^{G} en tant que B_0-module.