Université de Rennes 1 — Année universitaire 2018-2019
Licence de mathématiques
Module Anneaux et Arithmétique

Exemple de rédaction des solutions
des exercices 3.15 et 4.3

Tout particulièrement dans la solution du premier exercice ci-dessous, je me suis attaché à faire référence précisément aux résultats et définitions du cours utilisés sous forme numérotée. Par exemple la définition 2.76 désigne la définition 76 du chapitre 2. Lors d'un examen écrit où les documents de cours ne sont pas autorisés, il n'est bien sûr pas question d'exiger ce genre de références numérotées dans la rédaction. Je tenais cependant à souligner ainsi à quel point une bonne connaissance des résultats et des définitions du cours est importante pour aborder sereinement les exercices de TD et d'examen.

Exercice 15

(feuille 3) Remarque initiale : pour les deux dernières questions, par ailleurs assez délicates, cet exercice supposait implicitement connue la notion de sous-algèbre d'une algèbre et ses propriétés élémentaires. Comme elles sont très similaires à la notion de sous-anneau d'un anneau et les propriétés correspondantes, elles ne figurent pas dans le cours pour ne pas alourdir démesurément le chapitre 2. Rappelons ici quelques énoncés. Les démonstrations ne sont *a priori* pas très difficiles (« Il suffit d'écrire »)

- Soit A un anneau et $\iota\colon A \to B$ une A-algèbre ; une *sous-A-algèbre de B* est un sous-anneau C de B tel que $\iota(A) \subset C$. Exemple : B est une sous-A-algèbre de B ; $\iota(A)$ est une sous-A-algèbre de B.
- Soit A un anneau et $\iota\colon A \to B$ une A-algèbre ; soit $A \times B \to B$, $(a, b) \mapsto a \cdot b$ la loi de composition externe induite ; soit C un sous-anneau de B ; alors C est une sous-A-algèbre de B si et seulement si pour tout $a \in A$ et tout $c \in C$ on a $a \cdot c \in C$ si et seulement si pour tout $a \in A$ on a $a \cdot 1_B \in C$.
- Soit A un anneau et $\iota\colon A \to B$ une A-algèbre. Une intersection quelconque de sous-A-algèbres de B est une sous-A-algèbre de B.
- Soit A un anneau, $A \to B$ une A-algèbre et $S \subset B$ une partie de B. Il existe une unique sous-A-algèbre de B contenant S et minimale (au sens de l'inclusion) pour cette condition. On l'appelle la *sous-A-algèbre de B engendrée par S*.
- Soit A un anneau, $A \to B$ et $A \to C$ des A-algèbres et $\varphi\colon B \to C$ un morphisme de A-algèbres. Soit D une sous-A-algèbre de B. Alors $\varphi(D)$ est une sous-A-algèbre de C. En particulier $\varphi(B)$ est une sous A-algèbre de C.
- Soit A un anneau, $A \to B$ une A-algèbre et $b \in B$. Soit $\mathrm{ev}_b\colon A[X] \to B$ l'unique morphisme de A-algèbres qui envoie X sur b (*cf.* définition 2.76). Alors la sous-A-algèbre de B engendrée par b est $\mathrm{ev}_b(A[X])$ (*cf.* l'exercice 1 du TD 2) et est notée $A[b]$. On a la description :
$$A[b] = \{\sum_{i \in \mathbf{N}} a_i \cdot b^i\}_{(a_i) \in A^{(\mathbf{N})}}.$$

1. Par définition de l'algébricité et la proposition 2.14, a est algébrique sur $\mathbf{K}$ si et seulement si $\mathrm{Ker}(\mathrm{ev}_a) \neq \{0\}$. Ceci équivaut à l'existence d'un élément $P \in \mathbf{K}[X] \setminus \{0\}$ dans $\mathrm{Ker}(\mathrm{ev}_a)$, en d'autres termes à l'existence d'un élément $P \in \mathbf{K}[X] \setminus \{0\}$ tel que $P(a) = 0$.
2. Première remarque préliminaire : il faut corriger deux choses dans l'énoncé ; tout d'abord, il faut lire $\{a^i\}_{0 \leqslant i \leqslant n}$ et non $\{a^i\}_{1 \leqslant i \leqslant n}$; ensuite il faut supposer, pour que la dernière équivalence soit valide, que A n'est pas l'anneau nul ; ceci entraîne en particulier que le morphisme $\mathbf{K} \to A$ qui définit la structure de $\mathbf{K}$-algèbre est nécessairement injectif (car les

idéaux du corps $\mathbf{K}$ sont $\{0\}$ et $\mathbf{K}$) d'où on déduit ensuite que si $a \in A$ et $P \in \mathbf{K}[X] \setminus \{0\}$ vérifie $P(a) = 0$, alors P n'est pas constant

Seconde remarque préliminaire : par définition de $\mathbf{K}[a]$ (définition 2.76), le théorème 2.49 (théorème d'isomorphisme) et la remarque suivant le théorème 2.77, $\mathbf{K}[a]$ est isomorphe comme $\mathbf{K}$-algèbre à $\mathbf{K}[X]/\operatorname{Ker}(\mathrm{ev}_a)$; par ailleurs, en notant x la classe de X dans $\mathbf{K}[X]/\operatorname{Ker}(\mathrm{ev}_a)$, il existe un isomorphisme de $\mathbf{K}[a]$ sur $\mathbf{K}[X]/\operatorname{Ker}(\mathrm{ev}_a)$ qui envoie a sur x.

Supposons a algébrique sur $\mathbf{K}$ et montrons qu'il existe $n \in \mathbf{N}$ tel que $\{a^i\}_{0\leqslant i\leqslant n}$ est une base du $\mathbf{K}$-espace vectoriel $\mathbf{K}[a]$. Comme a est algébrique sur $\mathbf{K}$, l'idéal $\operatorname{Ker}(\mathrm{ev}_a)$ est non nul, donc engendré par un polynôme $P \in \mathbf{K}[X]$ non nul (proposition 2.29). Comme P est non nul et annule a, d'après la première remarque préliminaire, P n'est pas constant. Soit $n \in \mathbf{N}$ tel que P est de degré $n+1$. D'après le théorème 3.10, $\mathbf{K}[X]/\operatorname{Ker}(\mathrm{ev}_a)$ est un $\mathbf{K}$-espace vectoriel de dimension $\deg(P) = n+1$, dont une $\mathbf{K}$-base est $\{x^i\}_{0\leqslant i\leqslant n}$. D'après la seconde remarque préliminaire, et compte tenu du fait qu'un isomorphisme de $\mathbf{K}$-algèbres est en particulier un isomorphisme de $\mathbf{K}$-espaces vectoriels, $\{a^i\}_{0\leqslant i\leqslant n}$ est une $\mathbf{K}$-base de $\mathbf{K}[a]$.

Supposons qu'il existe $n \in \mathbf{N}$ tel que $\{a^i\}_{0\leqslant i\leqslant n}$ est une base du $\mathbf{K}$-espace vectoriel $\mathbf{K}[a]$. et montrons que $\mathbf{K}[a]$ est un $\mathbf{K}$-espace vectoriel de dimension finie. C'est immédiat par le cours d'algèbre linéaire et le fait que par hypothèse $\mathbf{K}[a]$ admet une base finie.

Supposons que $\mathbf{K}[a]$ est un $\mathbf{K}$-espace vectoriel de dimension finie, de dimension notée n, et montrons que a est algébrique sur $\mathbf{K}$. On sait (cours d'algèbre linéaire) que l'ensemble $\{a^i\}_{0\leqslant i\leqslant n}$, étant de cardinal $n+1$, est lié sur $\mathbf{K}$. Ceci signifie qu'il existe $(\alpha_i)_{0\leqslant i\leqslant d} \in \mathbf{K}^{d+1} \setminus \{0\}$ tel que $\sum_{i=0}^{d} \alpha_i a^i = 0$. Posant $P = \sum_{i=0}^{d} \alpha_i X^i \in \mathbf{K}[X]$, on a donc $P(a) = \mathrm{ev}_a(P) = 0$. Comme $(\alpha_i)_{0\leqslant i\leqslant d}$ est non nul, P est non nul. D'après la question précédente a est algébrique sur $\mathbf{K}$.

Au final, on a bien démontré les équivalences demandées.

3. L'énoncé oubliait de préciser que P était supposé unitaire.

   Soit $a \in A$. Par définition de $\mathbf{K}[a]$ et les résultats ci-dessus sur les sous-$\mathbf{K}$-algèbres, $\mathbf{K}[a]$ est un sous-$\mathbf{K}$-espace vectoriel de A (on peut aussi le démontrer « à la main » sans faire appel à la notion de sous-algèbre). Par ailleurs d'après le théorème 3.10 et comme $P \in \mathbf{K}[X] \setminus \{0\}$, A est un $\mathbf{K}$-espace vectoriel de dimension finie. Donc, par le cours d'algèbre linéaire, $\mathbf{K}[a]$ est un $\mathbf{K}$-espace vectoriel de dimension finie. D'après la question précédente, a est algébrique sur $\mathbf{K}$.

   Par définition de x, le morphisme quotient $\pi\colon \mathbf{K}[X] \to \mathbf{K}[X]/\langle P\rangle = A$ envoie X sur x. Par définition du morphisme d'évaluation, on a $\pi = \mathrm{ev}_x$. Comme le noyau de π est $\langle P\rangle$, par définition du polynôme minimal, le polynôme minimal de x sur $\mathbf{K}$ est P.

4. Notons P le polynôme minimal de a sur $\mathbf{K}$. D'après la première remarque préliminaire de la solution de la question 2, P est non constant, en particulier n'est pas un élément de $\mathbf{K}[X]^\times = \mathbf{K}^\times$. Soit Q, R des éléments de $\mathbf{K}[X]$ tels que $P = QR$. Montrons que Q ou R est un élement de $\mathbf{K}^\times$. Comme P est non nul et A est intègre, Q et R ne sont pas nuls. Comme P est le polynôme miminal de a, on a $P(a) = 0 = Q(a)R(a)$. Comme A est intègre, on a $Q(a) = 0$ ou $R(a) = 0$. Quitte à échanger Q et R, on peut supposer que $Q(a) = 0$ c'est à dire $Q \in \operatorname{Ker}(\mathrm{ev}_a)$. Par définition du polynôme minimal, P divise Q. Comme Q est non nul, on en déduit $\deg(Q) \geqslant \deg(P)$. Par ailleurs ($A$ est intègre) $\deg(P) = \deg(Q) + \deg(R)$ et (R est non nul) $\deg(R) \in \mathbf{N}$ donc $\deg(P) \leqslant \deg(Q)$. Finalement $\deg(P) = \deg(Q)$ et $\deg(R) = 0$ donc R est constant et non nul, donc $R \in \mathbf{K}^\times$. D'après la définition d'un élément irréductible et le fait que $\mathbf{K}[X]^\times = \mathbf{K}^\times$, on a bien démontré que P était un élément irréductible de $\mathbf{K}[X]$.

Par définition de $\mathbf{K}[a]$ et la proposition 2.12, $\mathbf{K}[a]$ est un sous-anneau de A. Par la seconde remarque préliminaire de la question 2, $\mathbf{K}[a]$ est isomorphe à $\mathbf{K}[X]/\langle P\rangle$. Comme P est irréductible, $\langle P\rangle$ est maximal (proposition 2.29) donc $\mathbf{K}[X]/\langle P\rangle$ est un corps (théorème 2.58), donc $\mathbf{K}[a]$ également. Donc $\mathbf{K}[a]$ est bien un sous-corps de A.

5. Dans l'énoncé, il fallait lire $\{a^i b^j\}_{0\leqslant i,j\leqslant n}$ et non $\{a^i b^j\}_{1\leqslant i,j\leqslant n}$ et préciser que n était non nul.

   Supposons que A n'est pas l'anneau nul [1]. Soit n_a le degré du polynôme minimal de a et n_b le degré du polynôme minimal de b. Comme A n'est pas l'anneau nul, n_a et n_b sont strictement positifs.

   Par la seconde remarque préliminaire de la solution de la question 2 et le théorème 3.10, $\{a^i\}_{0\leqslant i\leqslant n_a-1}$ est une $\mathbf{K}$-base de $\mathbf{K}[a]$. De même, $\{b^i\}_{0\leqslant i\leqslant n_b-1}$ est une $\mathbf{K}$-base de $\mathbf{K}[b]$ Soit $n = \mathrm{Max}(n_a-1, n_b-1, 1)$. Montrons que

   $$\mathrm{Vect}(\{a^i b^j\}_{0\leqslant i,j\leqslant n}) = \mathrm{Vect}(\{a^i b^j\}_{i,j\in\mathbf{N}})$$

   Comme $\{a^i b^j\}_{0\leqslant i,j\leqslant n} \subset \{a^i b^j\}_{i,j\in\mathbf{N}}$ on a l'inclusion $\mathrm{Vect}(\{a^i b^j\}_{0\leqslant i,j\leqslant n}) \subset \mathrm{Vect}(\{a^i b^j\}_{i,j\in\mathbf{N}})$. Pour montrer l'inclusion réciproque, il suffit de montrer que pour tout $(k,\ell)\in\mathbf{N}^2$ on a

   $$a^k b^\ell \in \mathrm{Vect}(\{a^i b^j\}_{0\leqslant i,j\leqslant n})$$

   Soit $(k,\ell)\in\mathbf{N}^2$. Comme $a^k\in\mathbf{K}[a]$ et d'après ce qui précède, il existe $P\in\mathbf{K}[X]$ tel que $\deg(P)\leqslant n_a-1$ et $a^k = P(a)$. De même, il existe $Q\in\mathbf{K}[X]$ tel que $\deg(P)\leqslant n_b-1$ et $b^\ell = Q(b)$. Alors $a^k b^\ell = P(a)Q(b)$ et les conditions sur les degrés de P et de Q permettent de constater que $P(a)Q(b)\in\mathrm{Vect}(\{a^i b^j\}_{0\leqslant i,j\leqslant n})$.

   Pour conclure sur la première question, il reste à montrer $\mathrm{Vect}(\{a^i b^j\}_{i,j\in\mathbf{N}})$ est une sous-$\mathbf{K}$-algèbre de A. Cela peut se faire « à la main », en appliquant la définition. On peut aussi constater, en utilisant la propriété universelle des algèbres de polynômes, qu'il existe un unique morphisme de $\mathbf{K}$-algèbre de $\mathbf{K}[X,Y]\to A$ qui envoie X sur a et Y sur b, et que son image

   $$\{\sum_{(i,j)\in\mathbf{N}^2}\alpha_{i,j}a^i b^j\}_{(\alpha_{i,j})\in A^{(\mathbf{N}^2)}}$$

   coïncide avec $\mathrm{Vect}(\{a^i b^j\}_{i,j\in\mathbf{N}})$. On note désormais $\mathbf{K}[a,b]$ ce dernier ensemble.

   Passons à la deuxième question. Comme $1_A = 1_{\mathbf{K}}$ annule $X - 1_{\mathbf{K}}\in\mathbf{K}[X]$, 1_A est algébrique sur A. Soit alors $a,b\in A$ des éléments algébriques sur $\mathbf{K}$ et $\alpha\in\mathbf{K}$. Montrons que $a+b$, $a-b$, ab et $\alpha\cdot a$ sont algébriques sur $\mathbf{K}$. Ceci achèvera de montrer que l'ensemble des éléments de A algébriques sur $\mathbf{K}$ est une sous-$\mathbf{K}$-algèbre de A. Comme $a+b\in\mathbf{K}[a,b]$, que $\mathbf{K}[a,b]$ est une sous-$\mathbf{K}$-algèbre de A et que $\mathbf{K}[a+b]$ est la sous-$\mathbf{K}$-algèbre de A engendrée par $a+b$, on a $\mathbf{K}[a+b]\subset\mathbf{K}[a,b]$. D'après la première question $\mathbf{K}[a,b]$ est un $\mathbf{K}$-espace vectoriel de dimension finie. Donc $\mathbf{K}[a+b]$ est également un $\mathbf{K}$-espace vectoriel de dimension finie. D'après la question 2, $a+b$ est algébrique sur $\mathbf{K}$. Comme $a-b$, ab et $\alpha\cdot a$ sont également dans $\mathbf{K}[a,b]$, le même raisonnement montre que ce sont égalemement des éléments algébriques sur $\mathbf{K}$, ce qui conclut.

6. Si $B = \{0_B\}$ est l'anneau nul, pour tout corps $\mathbf{K}$ et tout morphisme d'anneaux $\mathbf{K}\to B$, le morphisme d'évaluation ev_{0_B} a pour noyau $\mathbf{K}[X]$, et 0_B est algébrique sur $\mathbf{K}$. Donc l'équivalence demandée est claire dans ce cas.

   On considère désormais une A-algèbre $A\to B$ tel que B n'est pas l'anneau nul. En particulier le morphisme $A\to B$ est nécessairement injectif. On peut alors supposer dans la suite que A est un sous-anneau de B et que $\mathbf{K}$ est un sous-anneau de A.

1. Le cas où A est l'anneau nul se traite très rapidement ; voyez vous pourquoi ?

Soit $b \in B$ un élément algébrique sur $\mathbf{K}$. Il existe donc $P \in \mathbf{K}[X] \setminus \{0\}$ tel que $P(b) = 0$. Comme $\mathbf{K}$ est un sous-anneau de A, on a $P \in A[X] \setminus \{0\}$. Ceci montre que b est algébrique sur A.

Pour démontrer la réciproque, il est utile de démontrer le résultat intermédiaire suivant (qui s'appuie notamment sur l'implication qu'on vient de démontrer).

Soit $\mathbf{K}$ un corps, A une $\mathbf{K}$-algèbre intègre. Supposons tout d'abord que A est un corps et un $\mathbf{K}$-espace vectoriel de dimension finie, et considérons une A-algèbre B telle que B est un A-espace vectoriel de dimension finie. Alors B est un $\mathbf{K}$-espace vectoriel de dimension finie. En effet, soit $\{b_i\}_{i\in I}$ une famille génératriece finie de B comme A-espace vectoriel, et $\{a_j\}_{j\in J}$ une famille génératrice finie de A comme $\mathbf{K}$-espace vectoriel. On vérifie alors que $\{b_i a_j\}_{j\in J, i\in I}$ est une famille génératrice finie de B comme $\mathbf{K}$-espace vectoriel.

Pour n un entier strictement positif et $a_1, \dots, a_n$ des éléments de A, on note $\mathbf{K}[a_1, \dots, a_n]$ la sous-$\mathbf{K}$-algèbre de A engendrée par $\{a_1, \dots, a_n\}$. On va alors généraliser le résultat de la question 4. On considère l'hypothèse de récurrence $\mathcal{P}_n$ suivante, pour n entier strictement positif : « Soit $\mathbf{K}$ un corps, A une $\mathbf{K}$-algèbre intègre, $a_1, \dots, a_n \in A$ des éléments algébriques sur $\mathbf{K}$; alors $\mathbf{K}[a_1, \dots, a_n]$ est un corps et un $\mathbf{K}$-espace vectoriel de dimension finie. » D'après les questions 2 et 4, $\mathcal{P}_1$ est vraie. Soit n un entier strictement positif. Supposons $\mathcal{P}_n$ vraie et montrons que $\mathcal{P}_{n+1}$ est encore vraie. Soit $\mathbf{K}$ un corps, A une $\mathbf{K}$-algèbre intègre, et $a_1, \dots, a_n \in A$ des éléments algébriques sur $\mathbf{K}$. Posons $A_n := \mathbf{K}[a_1, \dots, a_n]$. D'après $\mathcal{P}_n$ et le fait que $a_1, \dots, a_n$ sont algébriques sur $\mathbf{K}$, A_n est un corps et un $\mathbf{K}$-espace vectoriel de dimension finie. Notons que A est naturellement munie d'une structure de A_n-algèbre ; en outre on vérifie qu'on $A_n[a_{n+1}] = \mathbf{K}[a_1, \dots, a_{n+1}]$. Comme a_{n+1} est algébrique sur $\mathbf{K}$, il est algébrique sur A_n. D'après $\mathcal{P}_1$, $A_n[a_{n+1}]$ est un corps et un A_n-espace vectoriel de dimension finie. En particulier, $\mathbf{K}[a_1, \dots, a_{n+1}]$ est un corps. Par ailleurs, comme $\mathbf{K}[a_1, \dots, a_{n+1}]$ est un A_n-espace vectoriel de dimension finie et que A_n est un $\mathbf{K}$-espace vectoriel de dimension finie, $\mathbf{K}[a_1, \dots, a_{n+1}]$ est un $\mathbf{K}$-espace vectoriel de dimension finie (*cf.* ci-dessus). Ainsi $\mathcal{P}_{n+1}$ est vérifiée. Finalement, on conclut que pour tout n entier strictement positif, $\mathcal{P}_n$ est vraie.

Revenons à notre problème initial, avec les notations ad hoc. Soit $b \in B$ un élément algébrique sur A. Il s'agit de montrer que b est algébrique sur $\mathbf{K}$. Par hypothèse, il existe n un entier strictement positif et $(a_i) \in A^{n+1}$ non tous nuls tel que $\sum_{i=0}^{n} a_i b^i = 0$ Soit $A_n := \mathbf{K}[a_0, \dots, a_n]$. Il existe donc $P \in A_n[X] \setminus \{0\}$ tel que $P(b) = 0$, en d'autres termes b est algébrique sur A_n. D'après ce qui précéde et l'hypothèse que tout élément de A est algébrique sur $\mathbf{K}$, A_n est un corps qui est un $\mathbf{K}$-espace vectoriel de dimension finie. Comme b est algébrique sur A_n, $A_n[b]$ est un A_n-espace vectoriel de dimension finie. D'après un argument vu ci-dessus, on en déduit que $A_n[b]$ est un $\mathbf{K}$-espace vectoriel de dimension finie. Mais par ailleurs $\mathbf{K}[b]$ est un sous-$\mathbf{K}$-espace vectoriel de $A_n[b]$. Ainsi $\mathbf{K}[b]$ est un $\mathbf{K}$-espace vectoriel de dimension finie, donc b est algébrique sur $\mathbf{K}$.

Exercice 4

(feuille 4)

1. Soit $\pi\colon A \to A[X]/\langle sX - 1\rangle$ le morphisme quotient. D'après le théorème 5.2 (et les remarques qui suivent son énoncé), pour répondre à la question, il suffit de montrer les propriétés suivantes :
   (a) $\pi(S) \subset (A[X]/\langle sX - 1\rangle)^{\times}$
   (b) pour tout anneau C et tout morphisme $\psi\colon A \to C$ tel que $\psi(S) \subset C^{\times}$, il existe un unique morphisme $\theta\colon A[X]/\langle sX - 1\rangle \to C$ tel que $\theta \circ \pi = \psi$

Notons x l'image de X dans $A[X]/\langle sX-1\rangle$. On obtient aussitôt $\pi(s)x-1=0$ donc $\pi(s)$ est inversible dans $A[X]/\langle sX-1\rangle$. Comme toute puissance d'un inversible est inversible (découle facilement des règles de calcul des puissances) et vu que $S=\{s^n\}_{n\in\mathbf{N}}$, et que pour tout $n\in\mathbf{N}$ on a $\pi(s^n)=\pi(s)^n$ d'après (image d'une puissance par un morphisme d'anneaux) on obtient bien que $\pi(S)\subset(A[X]/\langle sX-1\rangle)^\times$.

Passons à la deuxième propriété. Soit C un anneau et $\psi\colon A\to C$ un morphisme tel que $\psi(S)\subset C^\times$. On s'intéresse à l'ensemble des morphismes d'anneaux

$$\theta\colon A[X]/\langle sX-1\rangle\to C\quad\text{tels que}\quad\theta\circ\pi=\psi.$$

D'après la propriété universelle de l'anneau quotient, cet ensemble est en bijection avec l'ensemble $\mathcal{M}$ des morphismes d'anneaux $\tilde{\theta}\colon A[X]\to C$ qui induisent ψ en restriction à A et dont le noyau contient $\langle sX-1\rangle$. Comme $\langle sX-1\rangle$ est l'idéal engendré par $sX-1$, $\mathcal{M}$ est l'ensemble des morphismes $\tilde{\theta}\colon A[X]\to C$ qui induisent ψ en restriction à A et tels que $\tilde{\theta}(sX-1)=0$, ce qui équivaut à $\psi(s)\tilde{\theta}(X)=1_C$. Or, par hypothèse, $\psi(s)\in C^\times$. Notons $u\in C$ son inverse. Finalement, $\mathcal{M}$ est l'ensemble des morphismes d'anneaux $\tilde{\theta}\colon A[X]\to C$ qui induisent ψ en restriction à A et tels que $\tilde{\theta}(X)=u$. D'après la propriété universelle de l'anneau des polynômes à coefficients dans A, $\mathcal{M}$ est réduit à un élément, ce qui conclut.

2. On sait que l'image réciproque d'un idéal premier par un morphisme d'anneaux est encore un idéal premier, et par ailleurs (théorie élémentaire des ensembles) si $\mathfrak{q}_1$ et $\mathfrak{q}_2$ sont deux idéaux de $S^{-1}A$ tels que $\mathfrak{q}_1\subset\mathfrak{q}_2$, alors $\iota^{-1}(\mathfrak{q}_1)\subset\iota^{-1}(\mathfrak{q}_2)$. Ainsi $\varphi:\mathfrak{q}\mapsto\iota^{-1}\mathfrak{q}$ définit bien une application croissante de l'ensemble des idéaux premiers de $S^{-1}A$ vers l'ensemble des idéaux premiers de A. On va montrer :
   (a) l'image de φ est exactement l'ensemble des idéaux premiers de A qui ne recontrent pas S.
   (b) φ est injective

   ce qui permettra de conclure.

   Soit tout d'abord $\mathfrak{q}$ un idéal premier de $S^{-1}A$. Montrons que $\mathfrak{p}:=\iota^{-1}\mathfrak{q}$ ne rencontre pas S. Il est équivalent de montrer que $\iota(S)$ ne rencontre pas $\mathfrak{q}$. Mais, par définition, on a $\iota(S)\subset(S^{-1}A)^\times$. Or, comme $\mathfrak{q}$ est un idéal premier, il est propre, et ne peut donc rencontrer $(S^{-1}A)^\times$. L'argument montre plus généralement que tout idéal propre de $S^{-1}A$ a comme image réciproque dans A un idéal qui ne rencontre pas S.

   Soit à présent $\mathfrak{p}$ un idéal premier de A qui ne rencontre pas S. On cherche un idéal premier $\mathfrak{q}$ de A tel que $\iota^{-1}\mathfrak{q}=\mathfrak{p}$. Cette dernière condition entraîne que $\iota(\mathfrak{p})\subset\mathfrak{q}$. Ainsi un candidat naturel pour $\mathfrak{q}$ est l'idéal engendré par $\iota(\mathfrak{p})$ dans $S^{-1}A$, et l'on note $\mathfrak{q}$ ce dernier idéal. Montrons alors que $\iota^{-1}\mathfrak{q}=\mathfrak{p}$, l'inclusion $\mathfrak{p}\subset\iota^{-1}(\mathfrak{q})$ étant acquise. Soit $a\in\iota^{-1}\mathfrak{q}$. Comme $\mathfrak{q}$ est l'idéal engendré par $\iota(\mathfrak{p})=\{\frac{b}{1}\}_{b\in\mathfrak{p}}$, il existe une famille finie $(a_i,b_i,s_i)_{i\in I}$ d'éléments de $A\times\mathfrak{p}\times S$ telle que

$$\frac{a}{1}=\sum_{i\in I}\frac{a_i}{s_i}\frac{b_i}{1}$$

   Multipliant par $\prod s_i$, et sachant que $\mathfrak{p}$ est un idéal de A et que S est une partie multiplicative, on obtient l'existence de $s\in S$ et $b\in\mathfrak{p}$ tel que

$$\frac{sa}{1}=\frac{b}{1}.$$

   L'égalité précédente est une égalité dans $S^{-1}A$ et se traduit par l'existence de $t\in S$ tel que $t(sa-b)=0$. En particulier $tsa\in\mathfrak{p}$. Mais $ts\in S$, $\mathfrak{p}$ est premier et ne recontre pas S, donc $a \in \mathfrak{p}$. On a bien démontré que $\iota^{-1}(\mathfrak{q}) \subset \mathfrak{p}$, d'où l'égalité $\iota^{-1}(\mathfrak{q}) = \mathfrak{p}$. Ceci permet de conclure quant à la propriété (a).

Montrons à présent l'injectivité de φ. Soit $\mathfrak{q}_1$ et $\mathfrak{q}_2$ des idéaux premiers de $S^{-1}A$ tels que $\iota^{-1}\mathfrak{q}_1 = \iota^{-1}\mathfrak{q}_2$ Montrons que $\mathfrak{q}_1 \subset \mathfrak{q}_2$. Comme $\mathfrak{q}_1$ et $\mathfrak{q}_2$ jouent des rôles symétriques, cela permettra de conclure que $\mathfrak{q}_1 = \mathfrak{q}_2$ et donc que φ est injective.

Soit $a \in \mathfrak{q}_1$ que l'on écrit $\frac{b}{s}$ avec $b \in A$ et $s \in S$. En particulier $\frac{s}{1}a = \frac{b}{1} = \iota(b)$, et par ailleurs $sa \in \mathfrak{q}_1$. Donc $b \in \iota^{-1}\mathfrak{q}_1$. Par hypothèse, $b \in \iota^{-1}\mathfrak{q}_1$, donc $\iota(b) = \frac{s}{1}a \in \mathfrak{q}_2$. Mais $\frac{s}{1}$ est inversible dans $S^{-1}A$. On en déduit que $a = \frac{1}{s}(\frac{s}{1}a) \in \mathfrak{q}_2$, ce qui conclut. Ici le fait que $\mathfrak{q}_1$ et $\mathfrak{q}_2$ soient premiers ne joue aucun rôle.

Notons que la démonstration montre que la réciproque de l'applicaiton considérée est l'application qui à un idéal premier $\mathfrak{p}$ de A ne rencontrant pas S associe l'idéal de $S^{-1}A$ engendré par $\iota(\mathfrak{p})$

3. D'après l'exercice 9 du TD n°1 (plus précisément la démonstration de la question 2), il suffit de montrer que $S^{-1}A \setminus (S^{-1}A)^\times$ est l'idéal $\mathfrak{q}$ engendré par $\iota(\mathfrak{p})$ dans $S^{-1}A$. D'après la question précédent, $\mathfrak{q}$ est premier, donc propre. Il ne rencontre donc pas $(S^{-1}A)^\times$. Il reste à montrer que $S^{-1}A \setminus (S^{-1}A)^\times$ est inclus dans $\mathfrak{q}$. Soit $a \in S^{-1}A \setminus (S^{-1}A)^\times$, que l'on écrit $\frac{b}{s}$ avec $b \in A$ et $s \in S$. Si $b \in S$, la relation $\frac{b}{s}\frac{s}{b} = 1$ montre que a est inversible dans $S^{-1}A$, ce qui n'est pas le cas. Donc $b \notin S$ et par définition de S, $b \in \mathfrak{p}$. Donc $a = \frac{1}{s}\frac{b}{1} = \frac{1}{s}\iota(b)$ est bien un élément de l'idéal de $S^{-1}A$ engendré par $\iota(\mathfrak{p})$, ce qui conclut.

   Si $A = \mathbf{Z}$, p est un nombre premier et $\mathfrak{p} = p\mathbf{Z}$, on vérifie facilement, en utilisant le théorème 5.5, que $S^{-1}A$ est l'anneau $\mathbf{Z}_{(p)}$ introduit dans l'exercice 7 de la feuille de TD 1.

   Attention, il est faux en général qu'une localisation d'un anneau est un anneau local (si $A = \mathbf{Z}$ et $S = \{1, -1\}$, $S^{-1}A = \mathbf{Z}$ qui n'est pas local ; pour un exemple ne vérifiant pas $S \subset A^\times$, prendre $A = \mathbf{Z}$ et $S = \{2^n\}_{n \in \mathbf{N}}$; pour montrer dans ce dernier cas que $S^{-1}A$ n'est pas local, utiliser la question 2 de l'exercice 9 du TD n°1)

4. Dans l'énoncé, il fallait en fait lire « Déduire de la question 2 qu'il existe… »

   Soit x un élément non nilpotent de A. Soit S la partie multiplicative $\{x^n\}_{n \in \mathbf{N}}$. Comme x est non nilpotent, S ne contient pas 0_A. D'après le théorème 5.4, $S^{-1}A$ n'est pas l'anneau nul. Ainsi l'idéal nul est un idéal propre de $S^{-1}A$, et d'après le théorème 2.25, $S^{-1}A$ possède un idéal maximal. D'après la proposition 2.24, $S^{-1}A$ possède un idéal premier. Donc, d'après la question 2, il existe un idéal premier de A qui ne rencontre pas S. Comme $x \in S$, ceci permet de conclure.