Autour d'un théorème de Jacobson

Marc SAGE

6 février 2018

Table des matières

On utilisera pour tous objets a et b le ***symbole de Kronecker***[1] $\delta_a^b := \begin{cases} 1 \text{ si } a = b \\ 0 \text{ si } a \neq b \end{cases}$.

Les anneaux sont supposés unitaires (l'unité est notée 1) mais pas nécessairement commutatifs. Une ***unité*** désigne un élément inversible.

On dire qu'un élément a ***divise*** un élément b si on peut écrire $b = \lambda a$ pour un certain élément λ. On écrira alors $a \mid b$.

Cette courte feuille est consacrée à un théorème de Jacobson démontré indépendamment dans la feuille sur les anneaux. On commence par deux cas particuliers qui seront englobés par la troisième partie.

1 Les anneaux de Boole sont commutatifs

Un anneau ***booléen*** est un anneau dont tout élément est idempotent.
Montrer qu'un anneau booléen est commutatif.

Solution proposée.
Remarquons déjà que l'idempotence de 2 entraîne sa nullité (écrire $2 = 2^2 - 2$). Ensuite, étant donnés deux éléments a et b, on peut faire apparaître le défaut de commutativité $[a, b] := ab - ba \overset{2=0}{=} ab + ba$ dans le carré $(a + b)^2$, ce qui donne

$$[a, b] = (a + b)^2 - a^2 - b^2 = (a + b) - a - b = 0, \ CQFD.$$

Remarque. On renvoit au DM sur les anneaux de Boole pour plus de détails sur leur classification et leur liens avec les algèbres de Boole.

2 Les anneaux où $a^3 = a$ pour tout a sont commutatifs

Soit A un anneau où $a^3 = a$ pour tout $a \in A$. On veut montrer que A est commutatif.

Première démonstration.

1. *Montrer que l'homothétie de rapport* 6 *est nulle puis expliciter un isomophisme d'anneaux* $A \simeq 2A \times 3A$.
2. *Montrer que l'on supposer* A *de caractéristique* 2 *ou* 3.
3. *Conclure.* (On pourra utliser les nullités éventuelles des quantités $s^2 + s$ et $ab^2 + bab + b^2a$.)

Deuxième démonstration.

1. *Montrer que les idempotents de* A *sont centraux et en déduire que les carrés de* A *sont centraux.* (On pourra regarder les produits iaj pour i et j idempotents duaux et a élément quelconque.)
2. *Montrer que* $2a$ *et* $3a$ *sont centraux et conclure.*

Première solution proposée.

1. L'hypothèse appliquée à 2 donne $8 = 2^3 = 2$, d'où $6 = 0$, *CQFD.*

   En écrivant $a = 3a - 2a$, on voit que $A = 3A + 2A$. La décomposition est de plus unique vu l'implication $2a = 3b \overset{\times 3}{\Longrightarrow} 0 = 9b = 3b$. On peut donc écrire $A = 3A \oplus 2A$, ce qui induit une bijection $\begin{cases} A & \xrightarrow{\sim} & 3A \times 2A \\ a & \longmapsto & (3a, -2a) \\ 3x - 2y & \longleftarrow & (3x, 2y) \end{cases}$ qui a le bon goût d'être un isomorphisme d'anneaux (pour les lois induites, les neutres de $3A$ et $2A$ étant respectivement 3 et -2).

   Remarque. On aurait pu utiliser un exercice précédent : les éléments 2 et 3 étant des idempotents non triviaux, l'anneau A est décomposable selon $2A \times 3A$.

[1] Certains notent le $\delta_{a,b}$. Il me semble plus lisible de comparer deux expressions – nécessairement écrites dans une dimension selon le sens de l'écriture – en utilisant l'autre dimension du papier. De même, il est plus facile de comparer des couples $\binom{a}{b}$ et $\binom{\alpha}{\beta}$ plutôt que des couples (a, b) et (α, β), surtout si les coordonnées sont longues.

2. Les anneaux $2A$ et $3A$ vérifiant la même propriété que A. Si l'on montre qu'ils sont commutatifs, l'anneau produit $2A \times 3A \simeq A$ le sera. Il suffit donc de se restreindre à $3A$ (où $2 = 0$) et à $2A$ (où $3 = 0$).

3. Les deux identités vont s'obtenir en faisant apparaître des cubes (afin d'utiliser l'hypothèse) ainsi que des doubles/triples selon la caractéristique.

   Lorsque $2 = 0$, on écrit $0 = (s+1)^3 - (s+1) = 3s^2 + 3s = s^2 + s$, d'où en substituant une somme $a + b$ à s

   $$0 = (a+b) + (a+b)^2 = 0 + ab + ba + 0, \text{ ce qui conclut } ab = -ba \overset{2=0}{=} ba.$$

4. Lorsque $3 = 0$, on écrit

   $$2a = (a+b)^3 + (a-b)^3 = 2a + 2ab^2 + 2bab + 2b^2a,$$

   d'où la nullité de $ab^2 + bab + b^2a$ en simplifiant par 2 (qui est involutif donc inversible). En multipliant cette dernière par b d'une part à droite d'autre part à gauche, on obtient

   $$ab + \underline{bab^2 + b^2ab} = 0 = \underline{bab^2 + b^2ab} + ba, \text{ d'où le résultat après simplification.}$$

Seconde solution proposée.

1. Soit i idempotent et $a \in A$. On a donc $i(1-i) = 0 = (1-i)i$, d'où $[ia(1-i)]^2 = 0$. Par hypothèse, on a

   $$ia(1-i) = [ia(1-i)]^3 = 0,$$

   d'où $ia = iai$. On montrerait de même que le produit $(1-i)ai$ est nul, d'où $ai = iai = ia$, *CQFD.*

   Il suffit de montrer qu'un carré est idempotent, ce qui immédiat :

   $$\left(a^2\right)^2 = a^4 = a^3a = a^2.$$

2. Décomposer $a = 3a - 2a$ permettra de conclure.

   Or, d'une part $2a = (a+1)^2 - a^2 - 1$ est central comme somme de carrés (centraux), d'autre part $a + 1 = (a+1)^3 = a^3 + 3a^2 + 3a + 1$ montre que $3a = -3a^2$ est central (comme multiple entier d'un carré).

Remarque. Contrairement à la première solution qui utilise vraiment les particularités de 2 et 3, la seconde solution se généralise (en partie) quand on remplaçe l'exposant 3 par un entier quelconque (*cf.* deux premières questions du dernier exercice – difficile).

3 Un théorème de Jacobson

Soit A un anneau tel que $\forall a \in A,\ \exists n \geq 2,\ a^n = a$. On souhaite montrer que A est commutatif (théorème attribué à **Jacobson**).

La résolution de cet exercice nécessite la connaissance des corps finis, du corps de décomposition d'un polynômes ainsi que des rudiments de réduction. On rappelle quelques définitions ci-après.

Un élément a d'une algèbre sur un corps K est dit ***algébrique*** s'il est racine d'un polynôme à coefficients dans K. L'idéal des polynômes annulateurs de a admet alors un unitaire générateur unitaire non constant de degré minimal, appelé ***polynôme minimal*** de a, qui est irréductible sur K.

Une K-algèbre est dite ***finie*** si sa dimension en tant que K-espace vectoriel est finie, ***algébrique*** si tous ses éléments sont algébriques (sur K).

1. *Montrer qu'un produit ab est nul ssi le produit ba l'est.*
2. *Montrer que A est réduit (pas d'autre nilpotent que 0).*
3. *Montrer qu'on peut supposer l'existence d'un premier p tel que A est une algèbre sur $\mathbb{F}_p$.*
   Fixons un $a \in A$: il y a un $n \geq 2$ tel que $a^n = a$. Décomposons $X^n - X = \prod P^{\omega_P}$ sur $\mathbb{F}_p$.

4. *Montrer qu'il suffit de montrer que a commute aux $A_P := \operatorname{Ker} P(a\cdot)$.*
5. On fixe un facteur irréductible P de $X^n - X$ sur $\mathbf{F}_p$ dont on admettra en lemme que tout corps de rupture en est un corps de décposition. *En munissant A_P d'une structure d'espace vectoriel, montrer qu'il suffit de montrer que a commute aux vecteurs propres de l'"homothétie" $\cdot a$.*
6. *Ramener le problème au cas où A est une $\mathbb{F}_p$-algèbre finie.*

   On suppose désormais que A est une telle algèbre.
7. *Montrer qu'il y a un élément $a \in A$ non nul et non inversible ainsi qu'un entier $n \geq 1$ tels que*

$$A = \underbrace{\operatorname{Ker}(a\cdot)}_{=:B} \oplus \underbrace{\operatorname{Ker}((a^n\cdot) - \mathrm{Id})}_{=:C}.$$

8. *Montrer que l'algèbre A est décomposable et conclure.*
9. *Démontrer le lemme admis à la question 5.*

Solution proposée

1. Si $ab = 0$, alors $ba = (ba)^n = b(ab)^{n-1 \geq 1} a = 0$.
2. Si $a^n = a$, on multiplie par a^{n-1} jusqu'à dépasser l'ordre de nilpotence de a, d'où $a = 0$.
3. invoquer un ? tq $2^? = 2$ mq car $A =: c > 0$. On fait alors récu sur nombre diviseurs premiers *avec répét* de c. Soit $p \mid c$ premier, soit $n \geq 2$ tq $p^n = p$, alors p^{n-1} idempotent, donc $A \cong p^{n-1}A \times \left(1 - p^{n-1}\right) A$. Le 2e facteur est tué après p itérations, donc est une $\mathbf{F}_p$-algèbre ; le premier facteur est tué après $\frac{c}{p}$ itérations (car $n \geq 2$!), donc sa carac est $\leq \frac{c}{p} < c$.
4. L'élément $\prod P(a)$ est nilpotent donc (rq 2) nul, donc les "homothéties" de rapport a sont annulés par $\prod P$:

$$\left[\prod P\right](a) = \prod P(a) = 0.$$

   Le lemme des noyaux permet alors de décomposer $A := \bigoplus A_P$.
5. L'homothétie $\cdot a$ stabilise A_P (clair) et y est annulé par P : si $x \in A_P$, on a $P(a)\, x = 0$, d'où $[P(\cdot a)](x) = [\cdot P(a)](x) = xP(a) \overset{\text{rq } 1}{=} 0$. Ainsi, en notant K un corps de rupture de P, le sev A_P est un K-ev pour la loi $px := p(a)\, x$ et l'homothétie $\cdot a$ est un endo de cet ev (vérier $[\cdot a](px) = [\cdot a](p(a)\, x) = p(a)\, xa = p(xa) = p([\cdot a](x))$) annulé par un poly scindé simple sur K (corps rupture => corps décomposition car P irréd), donc diagonalisable.
6. Soit x un tel vecteur propre, mettons $xa = p(a)\, x$. De cette égalité et de ce que x et a admet un poly annulateur vient que l'algèbre $\mathbb{F}_p[a, x]$ est de dim finie. Étant par ailleurs un sous-anneau de A, elle vérifie la même hypothèse, donc (si on admet le cas où $\dim_{\mathbf{F}_p} A$ est finie) est abélienne, en particulier a et x commutent, CQFD.
7. Fixons un élément $a \in A$ non nul et non inversible (s'il n'en existait pas, tout élément non nul serait inversible et A serait une algèbre à division finie, commutative par le théorème de Wedderburn) : il est annulé par le polynôme $X^{n+1} - X$ pour un certain entier $n \geq 1$, donc le polynôme $X(X^n - 1)$ annule l'homothétie $a\cdot$, d'où la décomposition souhaitée vu que X et $X^n - 1$ sont étrangers.
8. La somme directe ci-dessus nous donne déjà un isomorphisme d'espaces vectoriels $A \simeq B \times C$. Si l'on montre que B et C sont des algèbres, cet isomorphisme deviendra d'algèbres si en outre les algèbres B et C sont orthogonales (au sens où le produit d'un élément de B par un élément de C est toujours nul). Montrons tout cela.

   Déjà, les espaces B et C sont stables par combinaison linéaire (ce sont des sous-espaces vectoriels). Étant chacun le noyau d'une homothétie $\lambda\cdot$, ils sont clairement stables par produit. Le problème est maintenant d'en exhiber des unités.

   Par définition de C, tout élément $c \in C$ vérifie $(a^n - 1)\, c = 0$, donc également $c(a^n - 1) = 0$ d'après une remarque préliminaire, ce qui s'écrit aussi $a^n c = c = ca^n$: voici une unité a^n.

   Le cas de B est moins immédiat. Cependant, intuiter son unité est aisé quand on se souvient que l'unité d'un produit de deux anneaux B et C est la somme directe $(1_B, 1_C)$ des unités de ces anneaux. Ainsi, dans notre cas, l'unité de B doit être le complément à 1 de celle de C, à savoir $1 - a^n$. Vérifions : tout élément $b \in B$ vérifie $ab = 0$, d'où $(1 - a^n)\, b \overset{n \geq 1}{=} b - a^{n-1}ab = b$ comme souhaité (et pareil de l'autre côtre vu que les nullités des produits ab et ba vont de pair).

Montrons enfin que B et C sont orthogonales. Cela résulte du fait[2] que tout $b \in B$ est annulé par $a = 1_C$, donc est annulé par tout $C = 1_C C = C 1_C$.

Pour conclure, il suffit de récurrer sur la dimension de A. Le cas minimal $A = \mathbb{F}_p$ est immédiat sachant le corps $\mathbb{F}_p$ commutatif. Ensuite, il s'agit pour récurrer de montrer que les sous-algèbres B et C sont *strictes* ; vu l'égalité $\dim A = \dim B + \dim C$, cela revient à montrer qu'elles sont non nulles, ou encore que leurs unités a^n et $1 - a^n$ sont non nulles. Or la nullité de a^n entraînerait celle de $a = a^n a$ (ce qui est exclu) et celle de $1 - a^n$ impliquerait l'inversibilité de a (ce qui est également exclu).

9. un tel corps est $K := {}^{\mathbb{F}_p[X]}\!/_P$ extension de $\mathbb{F}_p$ de degré $d := \deg P$, donc est un $\mathbb{F}_{p^d}$. Notons $k := \mathbb{F}_p$ pour abréger

   (a) Montrons que le nombre $\left|\mathrm{Hom}_k\left(K, \overline{k}\right)\right|$ de morphismes de K vers $\overline{k}$ fixant k est $\leq d$: un tel morphisme est déterminé par l'image de X qui doit être racine de P d'où au plus d choix.

   (b) Montrons que le nombre $\left|\mathrm{Gal}\left({}^{K}\!/_{k}\right)\right|$ d'automorphismes de $\mathbb{F}_{p^d}$ fixant $\mathbb{F}_p$ vaut d : il suffit de le montrer pour $\left|\mathrm{Gal}\left({}^{\mathbb{F}_{p^d}}\!/_{\mathbb{F}_p}\right)\right|$: on a déjà les itérés du Frobenius Fr, il suffit de montrer que l'ordre ω de ce dernier vaut d. Pour cela, on remarque que $\forall x \in \mathbb{F}_{p^d}$, $x = \mathrm{Id}(x) = \mathrm{Fr}^{\omega}(x) = x^{p^{\omega}}$, donc le polynôme $X^{p^{\omega}} - X$ s'annule sur $\mathbb{F}_{p^d}$ tout entier, donc est de degré $p^{\omega} \geq p^d$, d'où $\omega \geq d$, *CQFD.*

   (c) Montrons enfin qu'on a toujours $\left|\mathrm{Gal}\left({}^{K}\!/_{k}\right)\right| \leq \left|\mathrm{Hom}_k\left(K, \overline{k}\right)\right|$: on se donne un σ_0 dans le truc de droite. Pour $g \in \mathrm{Gal}\left({}^{K}\!/_{k}\right)$, le morphisme $\sigma_0 \circ g$ est encore un k-morphisme ; puisque σ_0 est injectif, tous les $\sigma_0 \circ g$ sont distincts quand g décrit $\mathrm{Gal}\left({}^{K}\!/_{k}\right)$. On a donc

   $$\left\{\sigma_0 \circ g\,;\, g \in \mathrm{Gal}\left({}^{K}\!/_{k}\right)\right\} \subset \underset{k}{\mathrm{Hom}}\left(K, \overline{k}\right),$$

   d'où l'inégalité en prenant les cardinaux.

   (d) Il en résulte l'égalité ensembliste, donc tous les morphismes de $\mathrm{Hom}_k\left(K, \overline{k}\right)$ ont même image $\mathrm{Im}\,\sigma_0$ (les $g \in Gal$ sont surj). COncluons.

   Soit P irréductible dans $k[X]$ et ξ une racine de P dans K. Soit $\overline{K}$ une clôture algébrique de K (qui est une clôture algébrique de k). On a $k \hookrightarrow k[\xi] \hookrightarrow K \hookrightarrow \overline{K}$. Dans $\overline{K}[X]$, P est scindé. Soit ζ une autre racine de P dans $\overline{K}$; on veut $\zeta \in K$.

   Construisons un morphisme k-morphisme $\varphi : K \longrightarrow \overline{K}$ qui envoit ξ sur ζ. Ce k-morphisme aura alors pour image K vu dans $\overline{K}$, ce qui conclura $\zeta = \varphi(\xi) \in \mathrm{Im}\,\varphi = K$.

   On dispose déjà d'un morphisme $\left\{\begin{array}{ccccc} k[\xi] & \widetilde{\longrightarrow} & k[\zeta] & \subset & \overline{K} \\ p(\xi) & \longmapsto & p(\zeta) & & \end{array}\right.$ qui est bien défini car ξ et ζ sont racines de P. On peut par conséquent considérer une extension intermédiaire $k[\xi] \hookrightarrow E \hookrightarrow K$ munie d'un k-morphisme $\sigma : E \hookrightarrow \overline{K}$ envoyant ξ sur ζ et de degré sur k maximal pour ces propriétés (les degrés $[E : k[\xi]]$ sont majorés par $[K : k]$ qui est fini par hypothèse). Montrons afin de conlure que $E = K$: pour $\lambda \in K$, on peut définir un morphisme $\left\{\begin{array}{ccc} E[\lambda] & \longrightarrow & \overline{K} \\ \sum e_i \lambda^i & \longmapsto & \sum \sigma(e_i)\,\lambda^i \end{array}\right.$ qui envoit[3] $\xi \in E$ sur $\sigma(\xi) = \zeta$, d'où par maximalité l'égalité des degrés de $E[\lambda]$ et E, ce qui revient à l'égalité des extensions $E[\lambda] = E$ et permet de conclure $\lambda \in L$.

4 Exemples

On garde notre anneau A tel que $\forall a \in A,\ \exists n \geq 2,\ a^n = a$.
(*cf.* feuilles sur les idéaux pour qq détails)

1. *Mq chq élément est multiple de son carré.*
2. *Mq corps ou nul si intègre. En déduire chq premier strcit est maximal*
3. *Mq A réduit, puis qu'il est sous-anneau d'un produit de corps. Réciproque ?*
4. *Que dire si A ne possède qu'un nombre fini d'idaux maximaux ?*

DEM

[2] Ce fait est nécessaire : lorsqu'une algèbre A est décomposable en $A \simeq B \times C$, alors B s'identifie à la partie $B \times \{0\}$ qui est le noyau de la multplication par $(0, 1) = 1_C$ (et de même C est le noyau de l'homothétie de rapport 1_B).

[3] si on réfléchit un peu, il n'y a qu'une façon de procéder

1. $a = a^{n-1}a^2$
2. si intègre, $a = \lambda a^2$ donne $a = 0$ ou a inversible. Soit $\mathfrak{p}$ premei, alors $A/\mathfrak{p}$ intrège où hypothèse reste, d'où $A/\mathfrak{p}$ nul (çed $\mathfrak{p} = A$) ou corps (çed $\mathfrak{p}$ max)
3. si $a^n = 0$, alors $a^{n-1} = \lambda a^n = 0$, d'où par rec $a = 0$. produit des projec mod $\mathfrak{m}$ est injective car noyau $= \cap m = \cap p = \sqrt{0} = 0$. (! ! ! pas forcément surj car $\mathfrak{m}$ en nombre peut-être infini)

   Contre exemeple : $C^0(X, \mathbf{R}) \subset \mathbf{R}^X$ où X connexe, soit $f \neq 0$ s'annulant, alors le fermé $V(f) \neq X$ n'est pas ouvert, soit o à la frontière, alors $\frac{f}{f^2}$ n'est pas borné en o donc pas prolongealbe par continutié.

   RQ En revanche, soit A sous anenau de $\prod k$ stable par inversion ponctuell (inverse une coordonnées conserver l'appartenca à A). Un lément $a \in A$ a des composantes nulles et du'atres inversible. En multiplicant par λ_a l'inverses des composantes non nulles et n'importe quoi d'autre , on tombe sur $\lambda_a a^2 = a$
4. Le produit des projec mod $\mathfrak{m}$ est surjective, donc A est un produit de coprs. Chacun d'exu vérifie alors l'hypothèse.

   Commme ci-dessus, OPS car $A =: p$ première. Chaque corps-facteur est alors une extension algébrique de $\mathbb{F}_p$, çed sous-corps de $\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^{n!}}$. Réciproquement, chaque (sous-anneau de chq) produit (non nécesairment fini) de sous-corps de $\overline{\mathbb{F}_p}$ fonctionne. Exemple : les anneaux **de Boole** sont les sous-anneaux d'un produit de corps $\mathbb{F}_2$