Endomorphismes semi-simples

Table des matières

1. Introduction

J'ai eu envie de mettre au propre le texte qui suit car la notion de semi-simplicité est une des choses nouvelles que j'ai apprises durant mon année de préparation à l'agrégation. En prépa on découvre qu'il y a des matrices diagonalisables dans $\mathbf{C}$ qui ne sont pas diagonalisables dans $\mathbf{R}$. Un des objectifs de ce texte est d'avoir un peu plus de choses à dire à ce sujet si les questions du jury s'orientent vers les histoires de diagonalisabilité dans une clôture algébrique. En effet, lorsque le corps de base $\mathbf{K}$ est parfait, nous allons voir que la diagonalisabilité dans $\overline{\mathbf{K}}$ est équivalente à la semi-simplicité (qui est une notion que l'on introduira en termes de sous-espaces stables). Cette semi-simplicité est elle-même équivalente à une condition sur le polynôme minimal (celle d'être sans facteur carré dans $\mathbf{K}[X]$), et donc la notion d'endomorphisme semi-simple se trouve à l'intersection de nombreuses leçons d'agrégation telles que : *Sous-espaces stables, polynômes d'endomorphismes, endomorphismes diagonalisables, extensions de corps...*
J'espère que ces notes permettront à d'autres de prendre du recul sur les questions de diagonalisabilité sur différents corps. On peut extraire des pages suivantes plusieurs développements, pour ma part je présentais la décomposition de Dunford-Jordan-Chevalley et le résultat sur les corps dans lesquels on a un « théorème spectral ». Je pense qu'il est également possible de présenter les théorèmes 3.1 et 4.1 en développement, mais je n'ai pas essayé de les ajuster pour qu'ils prennent 15 minutes, donc il y a peut-être des choses à ajouter ou à enlever. Les démonstrations de certains résultats ne sont pas extraites de lectures personnelles mais du complément de cours de Matthieu Romagny sur les algèbres de dimension finie. C'est aussi dans ce cours que j'ai appris que la décomposition dite de Dunford était mal nommée et se généralisait considérablement.

N'hésitez surtout pas à me signaler par mail toute erreur / imprécision, à me demander d'éclaircir un point pas clair, ou à me dire si vous avez trouvé ces notes utiles !

2. Tentative de motivation de la définition

Ce n'est qu'une tentative, c'est ainsi que je l'aurais motivée si on m'avait posé la question, mais ce n'est qu'une motivation issue du peu de recul d'un élève en fin de préparation à l'agrégation. Il y a sûrement des motivations plus profondes qui m'ont échappées.

On rappelle l'exercice classique suivant :

Proposition 2.1 :
Soit E un $\mathbf{R}$-espace vectoriel de dimension finie, soit $f \in \mathcal{L}(E)$. On a : f est diagonalisable si et seulement si tout sous-espace vectoriel de E admet un supplémentaire stable par f.

Démo : Supposons f diagonalisable. Soit F un sous-espace vectoriel quelconque de E. Soit $(e_1, \dots, e_m)$ une base de F. Puisqu'on a supposé f diagonalisable, il existe une base $(v_1, \dots, v_n)$ de E formée de vecteurs propres pour f. D'après le théorème de la base incomplète, on peut compléter la base $(e_1, \dots, e_m)$ de F en une base $(e_1, \dots, e_m, e_{m+1}, \dots, e_n)$ de E, où on a rajouté uniquement des vecteurs de notre base de vecteurs propres (c'est-à-dire $e_{m+1}, \dots, e_n$ ont été pris parmi les v_i). En effet, la famille $\{e_1, \dots, e_m\}$ est libre, et elle est contenue dans la famille génératrice $\{e_1, \dots, e_m, v_1, \dots, v_n\}$, donc il existe une famille $\mathcal{F}$ de vecteurs de E, telle que

$$\{e_1, \dots, e_m\} \subseteq \mathcal{F} \subseteq \{e_1, \dots, e_m, v_1, \dots, v_n\}$$

et $\mathcal{F}$ à la fois libre et génératrice. Si on veut se rappeler l'argument :

- Si $\{e_1, \dots, e_m\}$ est génératrice, $F = E$ et on conclut.
- Sinon $F \neq E$, et alors l'un des v_i n'appartient pas à F. En effet, si tous les v_i étaient dans F, l'espace vectoriel qu'ils engendrent serait contenu dans F, ce qui contredit le fait que $\{v_1, \dots, v_n\}$ est génératrice. Quitte à renommer, on peut supposer que $v_1 \notin F$. Alors la famille $\{e_1, \dots, e_m, v_1\}$ est libre car le vecteur ajouté n'est pas dans l'espace vectoriel engendré par les précédents. Si elle est génératrice, on a fini, sinon on recommence en partant de la famille $\{e_1, \dots, e_m, v_1\}$. On finit bien par obtenir une base car à chaque étape on s'arrange pour que la famille créée soit libre, et elle finit par être génératrice car on peut ajouter tous les v_i (si on part de $F = \{0\}$ par exemple).

On prend alors $G := \text{vect}(e_{m+1}, \dots, e_n)$. C'est un supplémentaire de F dans E, et il est stable par f car $e_{m+1}, \dots, e_n$ sont des vecteurs propres de f.

Réciproquement, supposons que tout sous-espace vectoriel de E admet un supplémentaire stable par f. Considérons

$$F := \bigoplus_{\lambda \in \text{Sp}(f)} \ker(f - \lambda \text{id})$$

le sous-espace vectoriel de E formé de la somme directe des sous-espaces propres de f. Si f n'était pas diagonalisable, F serait strictement inclus dans E. Soit H un hyperplan de E contenant F. Alors par hypothèse H admet un supplémentaire stable par f. Ce supplémentaire est une droite, engendrée par un vecteur propre de f. Mais c'est une contradiction car tous les vecteurs propres de f sont dans H. Ainsi, f est diagonalisable. □

Nous allons maintenant définir la notion d'endomorphisme semi-simple en relâchant un peu la condition de l'exercice ci-dessus : on va seulement demander aux sous-espaces stables de posséder un supplémentaire stable.

Définition 2.2 :
Soit $\mathbf{K}$ un corps, E un $\mathbf{K}$-espace vectoriel de dimension finie. On dit que $u \in \mathcal{L}(E)$ est semi-simple si tout sous-espace stable par u admet un supplémentaire stable par u.

Remarque :
On dira qu'une matrice $M \in \mathcal{M}_n(\mathbf{K})$ est semi-simple si l'endomorphisme de $\mathbf{K}^n$ qui lui est canoniquement associé est semi-simple.

3. Semi-simplicité et polynôme minimal

Le résultat suivant fait le lien entre la définition en termes de sous-espaces stables, et une condition sur le polynômes minimal de l'endomorphisme (quand je disais que ça allait bien dans *sous-espaces stables* et *polynômes d'endomorphismes...*)

Théorème 3.1 :
u est semi-simple si et seulement son polynôme minimal est sans facteur carré dans $\mathbf{K}[X]$.

Démo : Références possibles : RMS 129-1 p.50, c'est également un exercice du livre *Algèbre, le grand combat* de Grégory Berhuy.

- Notons π_u le polynôme minimal de u, que l'on suppose sans facteur carré.

  - Supposons dans un premier temps que π_u est un polynôme irréductible de $\mathbf{K}[X]$. Dans ce cas $\mathbf{L} := \mathbf{K}[X]/(\pi_u)$ est un corps (c'est une extension de $\mathbf{K}$), et la loi externe

$$\begin{array}{ccc} \mathbf{L} \times E & \to & E \\ \left(\bar{P}, x\right) & \mapsto & \bar{P} \,.\, x := P(u)(x) \end{array}$$

    est bien définie et munit E d'une structure de $\mathbf{L}$-espace vectoriel qui prolonge sa structure de $\mathbf{K}$-espace vectoriel. En effet, on peut vérifier que

$$\begin{array}{ccc} \mathbf{K}[X] \times E & \to & E \\ (P, x) & \mapsto & P \,.\, x := P(u)(x) \end{array}$$

    munit E d'une structure de $\mathbf{K}[X]$-module, et que cette application « passe au quotient par π_u » sans souci par définition du polynôme minimal.

    Maintenant, montrons qu'un sous-$\mathbf{K}$-espace vectoriel de E est stable par u si et seulement si c'est un sous-$\mathbf{L}$-espace vectoriel de E. Si F est un sous-$\mathbf{K}$-espace vectoriel de E stable par u, alors il est stable par $P(u)$ pour tout $P \in \mathbf{K}[X]$, et donc c'est un sous-$\mathbf{L}$-espace vectoriel de E (en effet, la stabilité par addition était déjà acquise par la structure de $\mathbf{K}$-espace vectoriel, il ne restait donc plus qu'à vérifier la stabilité par la multiplication externe par les éléments de $\mathbf{L}$). Réciproquement, si F est un sous-$\mathbf{L}$-espace vectoriel de E, il est stable par tous les polynômes en u, donc en particulier stable par u.

    Ainsi, si l'on prend F un sous-espace vectoriel de E stable par u, c'est un sous-$\mathbf{L}$-espace vectoriel, et donc il admet un supplémentaire G en tant que $\mathbf{L}$-espace vectoriel (c'est ici que l'hypothèse π_u irréductible intervient de manière cruciale. En effet, si $\mathbf{L}$ n'était pas un corps, on ne pourrait pas conclure, car dans la théorie des modules, il n'est pas vrai que tout sous-module admet un sous-module supplémentaire). Les sous-espaces G et F sont aussi en somme directe dans E vu comme $\mathbf{K}$-espace vectoriel

(car le fait d'être en somme directe ne dépend pas du corps sur lequel on regarde notre espace-vectoriel), et G est stable par u (car c'est un sous-$\mathbf{L}$-espace vectoriel). On a donc bien montré que dans le cas où π_u est irréductible dans $\mathbf{K}[X]$, l'endomorphisme u est semi-simple.

- Si maintenant π_u est composé :

$$\pi_u = P_1 \dots P_r$$

où les P_i sont des irréductibles unitaires deux à deux distincts[1] de $\mathbf{K}[X]$.

Pour tout $1 \leqslant i \leqslant r$, on note $F_i := \ker(P_i(u))$. Chaque F_i est stable par u, et on note u_i l'endomorphisme induit par u sur F_i. On a alors $\pi_{u_i} = P_i$. En effet, par définition de F_i, $P_i(u)$ est nul sur F_i, donc P_i est un polynôme annulateur de u_i, et comme il est irréductible unitaire, c'est bien le polynôme minimal de u_i.

Considérons maintenant un sous-espace vectoriel F stable par u. D'après le lemme des noyaux appliqué à l'endomorphisme induit par u sur F, on a :

$$F = \bigoplus_{i=1}^{r} (F_i \cap F)$$

Fixons un $i \in [\![1, r]\!]$. Comme F est stable par u, $F_i \cap F$ est un sous-espace vectoriel de F_i stable par u_i. Or u_i a pour polynôme minimal P_i, qui est irréductible dans $\mathbf{K}[X]$, donc d'après le premier cas ci-dessus, u_i est semi-simple. Il existe donc G_i un supplémentaire de $F_i \cap F$ dans F_i, stable par u_i. La somme (directe) des G_i fournit alors un supplémentaire de F stable par u ! En effet, par le lemme des noyaux,

$$E = \ker(\pi_u(u)) = \bigoplus_{i=1}^{r} F_i = \bigoplus_{i=1}^{r} (F_i \cap F) \oplus G_i = F \oplus \underbrace{\left(\bigoplus_{i=1}^{r} G_i \right)}_{=:G}$$

et G est bien stable par u. Ainsi, tout sous-espace vectoriel stable par u admet un supplémentaire stable par u, donc u est semi-simple.

- Si maintenant π_u a un facteur carré, montrons que u n'est pas semi-simple. Pour cela, on cherche à exhiber un sous-espace F, stable par u, mais n'admettant pas de supplémentaire stable par u.

Écrivons $\pi_u = P^2 Q$, avec $P \in \mathbf{K}[X]$ unitaire non constant. On considère le sous-espace vectoriel $F := \ker(P(u))$. Il est bien stable par u.
Maintenant, si G est un supplémentaire de F dans E, alors pour tout $x \in G$, $(PQ)(u)(x) \in F$. En effet,

$$P(u)\left[(PQ)(u)(x)\right] = (P^2Q)(u)(x) = \pi_u(u)(x) = 0.$$

D'autre part, si G était stable par u, il serait stable par tout polynôme en u, et donc on aurait également :

$$\forall x \in G,\ (PQ)(u)(x) \in G$$

[1] car π_u est toujours supposé sans facteur carré

Ainsi, si G était stable par u, on aurait :

$$\forall x \in G,\ (PQ)(u)(x) \in F \cap G = \{0\}$$

Donc $(PQ)(u)$ serait nul sur G, et comme cet endomorphisme est également nul sur F, il serait nul sur tout E, et donc π_u diviserait PQ, ce qui est absurde (car $\pi_u = P^2Q$ avec P unitaire non constant).
Finalement, F n'admet pas de supplémentaire stable par u, donc u n'est pas semi-simple, ce qui conclut la démonstration.

□

Remarque :
On peut définir la notion d'élément semi-simple d'une **K**-algèbre de dimension finie par cette condition portant sur le polynôme minimal. En effet, si notre **K**-algèbre n'est pas une algèbre de matrices ou d'endomorphismes, la condition sur les sous-espaces stables perd son sens, alors que celle sur le polynôme minimal en a toujours un.

Corollaire 3.2 :
u est diagonalisable si et seulement si il est semi-simple et son polynôme caractéristique est scindé dans **K**.

Démo :

- Si u est diagonalisable, χ_u est bien sûr scindé dans **K**, et π_u est scindé à racines simples dans **K**, donc sans facteur carré dans $\mathbf{K}[X]$.
- Réciproquement, si χ_u est scindé sur **K**, alors comme π_u divise χ_u dans $\mathbf{K}[X]$ (Cayley-Hamilton), π_u est un produit de facteurs de degré 1 dans $\mathbf{K}[X]$. Si on suppose de plus u semi-simple, alors π_u est sans facteur carré dans $\mathbf{K}[X]$ d'après le théorème précédent, et donc π_u est scindé à racines simples dans **K**, d'où la diagonalisabilité de u.

□

4. Lien avec la diagonalisabilité lorsque le corps de base est parfait

Sur un corps parfait, la semi-simplicité est équivalente à la diagonalisabilité dans une clotûre algébrique !

Théorème 4.1 :
Soit **K** un corps parfait, et $\overline{\mathbf{K}}/\mathbf{K}$ une clôture algébrique. Soit $M \in \mathcal{M}_n(\mathbf{K})$. La matrice M est semi-simple si et seulement si elle est diagonalisable dans $\mathcal{M}_n\left(\overline{\mathbf{K}}\right)$

Avant de passer à la démonstration de ce théorème, voici quelques rappels sur les corps parfaits.

Soit **K** un corps. Soit $\overline{\mathbf{K}}$ une clotûre algébrique de **K** et **L** une extension algébrique de **K** telle que $\mathbf{K} \subseteq \mathbf{L} \subseteq \overline{\mathbf{K}}$.

- Un polynôme $P \in \mathbf{K}[X]$ est dit séparable s'il n'a pas de racines multiples dans $\overline{\mathbf{K}}$.
- Un élément $a \in \mathbf{L}$ est dit séparable sur **K** si son polynôme minimal sur **K** est séparable.
- L'extension algébrique $\mathbf{L}/\mathbf{K}$ est dite séparable si tous les éléments de **L** sont séparables sur **K**.

Définition 4.2 :
Un corps $\mathbf{K}$ est dit parfait si chacune de ses extensions algébriques est séparable.

On a une caractérisation très pratique des corps parfaits.

Théorème 4.3 :
Les corps parfaits sont exactement :

- Les corps de caractéristique nulle.
- Les corps de caractéristique $p > 0$ dont le morphisme de Frobenius ($x \mapsto x^p$) est surjectif.

En particulier, tous les corps finis sont parfaits, car leur morphisme de Frobenius est injectif, donc surjectif car c'est une application entre deux ensembles finis de même cardinal. Pour trouver un exemple de corps non-parfait, il faut donc chercher parmi les corps de caractéristique positive qui ne sont pas des corps finis (typiquement, les $\mathbf{F}_p(T)$, comme on l'explique ci-dessous).

Enfin, terminons cette partie de prérequis sur les corps parfaits par une propriété qui nous servira dans les démonstrations qui suivent (cette propriété caractérise en fait les corps parfaits, voir RMS 129-1 p.52).

Proposition 4.4 :
Soit $\mathbf{K}$ un corps parfait, et $P \in \mathbf{K}[X]$ un polynôme irréductible. Alors $P \wedge P' = 1$.

Démo : Par contraposée, supposons que $P \wedge P' \neq 1$ et montrons que P ne peut pas être irréductible.
Soit Q un facteur irréductible commun à P et P' dans $\mathbf{K}[X]$. Alors $Q|P$. Mais comme P est irréductible et Q n'est pas constant, Q et P sont associés. On en déduit que $P|P'$ (car $Q|P'$ et Q et P sont associés). Puisque $\deg P > \deg P'$, P' doit être nul.

- Si $\mathbf{K}$ est de caractéristique nulle, $P' = 0$ implique P constant, et donc P n'est pas irréductible.
- Si $\mathbf{K}$ est de caractéristique $p > 0$, la nullité de P' veut dire qu'en dérivant, on a fait tomber des puissances divisibles par p, et donc il existe $R \in \mathbf{K}[X]$ tel que $P = R(X^p)$. On peut donc écrire
$$P = R(X^p) = \sum_{i=1}^{n} a_i (X^p)^i$$
puis utiliser la surjectivité du morphisme de Frobenius (théorème 4.3) pour remplacer les a_i par des b_i^p. Puisque le Frobenius est un morphisme d'anneaux, on en déduit que
$$P = \left(\sum_{i=1}^{n} b_i X^i \right)^p$$
donc n'est pas irréductible.

□

Remarque :
Cette propriété n'est pas vraie sur n'importe quel corps.
En effet, considérons le corps $\mathbf{K} := \mathbf{F}_2(T)$, et le polynôme $P := X^2 - T \in \mathbf{K}[X]$. Ce polynôme n'a pas de racine dans $\mathbf{K}$. En effet, si $F(T) \in \mathbf{K}$ était racine de P, on aurait $F(T)^2 = T$. Mais le terme de gauche a une valuation paire en T (en tant que fraction rationnelle en T), tandis que

le terme de droite a une valuation impaire en T. Donc P est de degré 2, sans racine dans $\mathbf{K}$, donc il est irrédutible dans $\mathbf{K}[X]$. Cependant, il n'est pas premier avec P', car $P' = 0$ (on est en caractéristique 2, donc le terme en X^2 a une dérivée nulle, et n'oublions pas que T est une constante du corps de base $\mathbf{K}$!). Ainsi $\mathbf{F}_2(T)$ n'est pas parfait.

Démo du théorème 4.1. Soit $\mathbf{K}$ un corps parfait et $M \in \mathcal{M}_n(\mathbf{K})$. Nous allons montrer que M est semi-simple si et seulement si elle est diagonalisable dans $\overline{\mathbf{K}}$.

- Si M est diagonalisable dans $\overline{\mathbf{K}}$, alors le polynôme minimal de M vue comme un élément de $\mathcal{M}_n\left(\overline{\mathbf{K}}\right)$ $\left(\text{noté } \pi_{M,\overline{\mathbf{K}}}\right)$ est scindé à racines simples dans $\overline{\mathbf{K}}$.

  Or $\pi_{M,\overline{\mathbf{K}}} = \pi_{M,\mathbf{K}}$: que l'on voit M comme une matrice à coefficients dans $\mathbf{K}$ ou comme une matrice à coefficients dans $\overline{\mathbf{K}}$, son polynôme minimal reste le même (voir annexe 7.1). Donc $\pi_{M,\mathbf{K}}$ est scindé à racines simples dans $\overline{\mathbf{K}}$, donc sans facteur carré dans $\mathbf{K}$. D'après le théorème 3.1, M est semi-simple. Remarquons que l'hypothèse « $\mathbf{K}$ parfait » ne sert pas pour cette implication.

- Si maintenant M n'est pas diagonalisable dans $\overline{\mathbf{K}}$, alors $\pi_{M,\overline{\mathbf{K}}}$ n'est pas scindé à racines simples dans $\overline{\mathbf{K}}$, il a donc au moins une racine multiple (comme $\overline{\mathbf{K}}$ est algébriquement clos, ce n'est pas le côté « scindé » qui fait défaut). On réutilise le fait que $\pi_{M,\overline{\mathbf{K}}} = \pi_{M,\mathbf{K}}$ et on en déduit que $\pi_{M,\mathbf{K}}$ a une racine double dans $\overline{\mathbf{K}}$.

  Pour alléger, notons P le polynôme $\pi_{M,\mathbf{K}} \in \mathbf{K}[X]$.

  Nous venons d'expliquer qu'il existe $\alpha \in \overline{\mathbf{K}}$ tel que $(X-\alpha)^2$ divise P dans $\overline{\mathbf{K}}[X]$. On en déduit facilement que $(X-\alpha)$ divise à la fois P et P' dans $\overline{\mathbf{K}}[X]$: P et P' ne sont donc pas premiers entre eux dans $\overline{\mathbf{K}}[X]$. Mais le calcul du pgcd de P et P' peut s'effectuer à l'aide de l'algorithme d'Euclide, qui renvoie le même résultat que l'on considère les coefficients des polynômes comme des éléments de $\mathbf{K}$ ou comme des éléments de $\overline{\mathbf{K}}$ (ceci résulte de l'unicité du quotient et du reste dans la division euclidienne). Donc P et P' ne sont pas premiers entre eux dans $\mathbf{K}[X]$.

  Montrons que cela implique l'existence d'un facteur carré pour P. Soit U un facteur irréductible commun à P et P' dans $\mathbf{K}[X]$. Écrivons $P = UV$. Alors $P' = U'V + UV'$. Or U divise P' par hypothèse, et U divise UV' à vue, donc U divise $U'V$. Mais comme U est irréductible, il est premier avec U' d'après la proposition 4.4 (c'est là qu'on utilise que $\mathbf{K}$ est parfait !). On en déduit (lemme de Gauss) que U divise V , et donc U^2 divise P. Ainsi, $\pi_{M,\mathbf{K}}$ a un facteur carré dans $\mathbf{K}[X]$, donc M n'est pas semi-simple (théorème 3.1).

□

Remarque :
Lorsque le corps de base n'est plus supposé parfait, cette caractérisation s'effondre. En effet, il suffit de considérer M : la matrice compagnon du polynôme $P = X^2 - T$ de la remarque précédente. Cette matrice à coefficients dans $\mathbf{K} = \mathbf{F}_2(T)$ a pour polynôme minimal le polynôme P (une matrice compagnon a son polynôme minimal égal à son polynôme caractéristique). Comme P est irréductible, il est sans facteur carré dans $\mathbf{K}[X]$, donc M est semi-simple.

Maintenant, considérons $\alpha \in \overline{\mathbf{K}}$ une racine carrée de $-T$: $\alpha^2 = -T$. Alors

$$P = X^2 - T = X^2 + \alpha^2 = (X-\alpha)^2.$$

Ainsi, si M était diagonalisable dans $\overline{\mathbf{K}}$, ce serait l'homothétie de rapport α ! Ce n'est pas le cas, donc M ne peut pas être diagonalisable dans $\overline{\mathbf{K}}$. Finalement, M est semi-simple sans être diagonalisable dans $\overline{\mathbf{K}}$, il faut donc faire attention lorsque le corps n'est pas parfait, des choses étranges surviennent.

5. Décomposition de Dunford-Jordan-Chevalley sur un corps parfait

Commençons par rappeler le théorème plus classique que nous allons tenter de généraliser.

Soit E un $\mathbf{C}$-espace vectoriel de dimension finie, et soit $u \in \mathcal{L}(E)$. Il existe un unique couple (d, n) d'endomorphismes de E tel que d et n commutent, d est diagonalisable, n est nilpotent, et $u = d + n$. De plus, d et n sont des polynômes en u.

Ce résultat reste vrai si u est un endomorphisme d'un $\mathbf{R}$-espace vectoriel de dimension finie dont le polynôme caractéristique est scindé sur $\mathbf{R}$. On peut trouver une démonstration de ces théorèmes dans le livre *Réduction des endomorphismes* de Roger Mansuy.

En remplaçant « d diagonalisable » par « d semi-simple », nous allons nous débarrasser de l'hypothèse sur le polynôme caractéristique et donner un énoncé plus général. Lorsque le corps de base est algébriquement clos, on retombe bien sur le théorème connu, en utilisant le théorème 4.1.

Théorème 5.1 :
Soit $\mathbf{K}$ un corps parfait, E un $\mathbf{K}$-espace vectoriel de dimension finie. Pour tout $u \in \mathcal{L}(E)$, il existe un unique couple $(s, n) \in \mathcal{L}(E)^2$ tel que :

$$\begin{cases} s \text{ est semi-simple, } n \text{ est nilpotent} \\ s \circ n = n \circ s \\ u = s + n \end{cases}$$

De plus, s et n sont des polynômes en u.

Démo : Références possibles : *Nouvelles histoires hédonistes de groupes et de géométries*, de Philippe Caldero et Jérôme Germoni, aux alentours de la page 162 du tome 1, ou RMS 129-1, ou les développements de Benjamin Havret (disponibles sur sa page http://www.normalesup.org/~havret/Travauxscolaires.html) où il indique encore une autre référence : J. Risler, P. Boyer, *Algèbre pour la licence 3 : groupes, anneaux, corps.*

Toute l'idée de la preuve est de construire s comme un zéro d'un polynôme sans facteur carré, de sorte que s sera automatiquement semi-simple. L'aspect un peu magique de la démonstration est qu'on va trouver un zéro du polynôme en utilisant la même formule de récurrence que dans la méthode de Newton, alors qu'on ne cherche pas une racine réelle, mais un endomorphisme annulé par notre polynôme !

Étape 1 : Il existe $P \in \mathbf{K}[X]$ tel que P est sans facteur carré et $P(u)$ est nilpotent.

Écrivons la décomposition du polynôme minimal de u en produit d'irréductibles de $\mathbf{K}[X]$:

$$\pi_u = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_r^{\alpha_r}$$

Il suffit alors de prendre $P := P_1 P_2 \dots P_r$. En effet, si on pose $\alpha := \max\{\alpha_i \ , \ 1 \leqslant i \leqslant r\}$, π_u divise P^α, et donc $P(u)^\alpha = 0$. Ainsi, P est bien sans facteur carré, et $P(u)$ est nilpotent.

Cependant, ce polynôme P n'est pas le plus accessible en pratique, car trouver le polynôme minimal n'est pas facile. On aimerait bien trouver un moyen plus effectif d'obtenir un polynôme P vérifiant les conditions requises. C'est ce qu'on se propose de faire dans l'étape bonus ! (*Étape 5*)

Étape 2 : Si P satisfait les conditions de l'étape 1, alors $P'(u) \in \mathbf{K}[u]^\times$.

En effet, P est sans facteur carré dans $\mathbf{K}[X]$, donc premier avec P' (voir la fin de la preuve du théorème 4.1, où l'on a montré que l'existence d'un facteur commun à P et P' impliquait l'existence d'un facteur carré pour P).
Or π_u et P ont les mêmes facteurs irréductibles dans $\mathbf{K}[X]$, donc P' et π_u sont également premiers entre eux. On peut donc écrire une relation de Bézout entre π_u et P' : il existe $U, V \in \mathbf{K}[X]$ tels que $U\pi_u + VP' = 1$. En évaluant en u et en utilisant le fait que $\pi_u(u) = 0$, on obtient :

$$V(u)P'(u) = \mathrm{id}_E$$

ce qui montre bien que $P'(u) \in \mathbf{K}[u]^\times$.

Étape 3 : Guidés par la méthode de Newton, on aimerait définir une suite de la manière suivante :

$$\begin{cases} a_0 = u \\ \forall n \in \mathbf{N},\ a_{n+1} = a_n - \frac{P(a_n)}{P'(a_n)} \end{cases}$$

dans l'espoir qu'en partant de notre endomorphisme connu u, on finisse par atteindre un endomorphisme qui annule P, et qui sera donc semi-simple.

Pour que le rêve devienne réalité, nous devons montrer qu'on peut bien « diviser par $P'(a_n)$ » à chaque étape. Rappelons que $P'(a_n)$ est un élément de $\mathcal{L}(E)$, donc la notation sous forme de fraction est un peu abusive, mais elle est là pour sous-entendre qu'on peut multiplier de n'importe quel côté par $P'(a_n)^{-1}$. En effet, nous allons montrer par récurrence que pour tout $n \in \mathbf{N}$,

(i) a_n est bien défini et est un polynôme en u.

(ii) $P(a_n) \in \left(P(u)^{2^n}\right) := P(u)^{2^n}\mathbf{K}[u]$ (idéal engendré par $P(u)^{2^n}$ dans l'anneau $\mathbf{K}[u]$).

(iii) $a_n - u \in (P(u)) := P(u)\mathbf{K}[u]$.

- Les trois points sont clairement satisfaits au rang 0. Remarquons que l'étape précédente, dont la conclusion était que $P'(u) \in \mathbf{K}[u]^\times$, permet de bien définir le terme a_1 sans se poser de question sur le côté de la multiplication par $P'(u)^{-1}$.
- Soit $n \in \mathbf{N}$. Si les trois points sont satisfaits au rang n, alors :
  - pour montrer que (i) est satisfaite au rang $n+1$, il suffit de montrer que $P'(a_n)$ appartient à $\mathbf{K}[u]^\times$. D'après (iii) au rang n, il existe $R_n \in \mathbf{K}[X]$ tel que

    $$a_n = u + P(u)R_n(u).$$

    On utilise alors le mini lemme suivant[2] :

[2] On me dit dans l'oreillette qu'on peut le voir comme un corollaire du lemme 5.3.

Lemme 5.2 :
Il existe $Q \in \mathbf{K}[X,Y]$ tel que $P'(X+Y) = P'(X)+YQ(X,Y)$.

D'où :

$$P'(a_n) = \underbrace{P'(u)}_{\in \mathbf{K}[u]^\times} + \underbrace{P(u)R_n(u)Q(u,P(u)R_n(u))}_{\text{nilpotent de } \mathbf{K}[u]}$$

Ainsi, $P'(a_n)$ est la somme d'un inversible et d'un nilpotent qui commutent, donc inversible dans $\mathbf{K}[u]$ (voir annexe 7.3). Par conséquent, le point (i) est satisfait au rang $n+1$.

- Pour montrer (ii), nous avons à nouveau besoin d'un petit lemme polynomial :

Lemme 5.3 :
Il existe $S \in \mathbf{K}[X,Y]$ tel que

$$P(X+Y) = P(X) + YP'(X) + Y^2S(X,Y).$$

On a donc

$$\begin{aligned} P(a_{n+1}) &= P\left(a_n - \frac{P(a_n)}{P'(a_n)}\right) \\ &= \underbrace{P(a_n) - \frac{P(a_n)}{P'(a_n)}P'(a_n)}_{=0} + \left(-\frac{P(a_n)}{P'(a_n)}\right)^2 S\left(a_n, -\frac{P(a_n)}{P'(a_n)}\right) \end{aligned}$$

Or $P(a_n) \in \left(P(u)^{2^n}\right)$, donc $(P(a_n))^2 \in \left(P(u)^{2^{n+1}}\right)$. Le point (ii) est donc satisfait au rang $n+1$.

- Enfin,

$$a_{n+1} - u = a_n - u - \frac{P(a_n)}{P'(a_n)}.$$

Or $a_n - u \in (P(u))$ et $\frac{P(a_n)}{P'(a_n)} \in \left(P(u)^{2^n}\right)$, donc $a_{n+1} - u$ est bien divisible par $P(u)$ dans $\mathbf{K}[u]$, ce qui montre (iii) au rang $n+1$ et conclut la récurrence.

Remarque (très importante !) **:**
On peut bien évaluer les égalités des lemmes 5.2 et 5.3 en nos endomorphismes car comme tout se passe dans $\mathbf{K}[u]$, tout commute. C'est essentiel car pour établir les égalités dans $\mathbf{K}[X,Y]$ on identifie XY et YX, donc on ne peut les évaluer qu'en des endomorphismes qui commutent deux à deux. Merci à Clarence qui m'a fait remarquer ça !

Pour finir, prenons $m \geqslant 1$ tel que $P(u)^{2^m} = 0$ (ce qui est possible car $P(u)$ est nilpotent). D'après le point (ii), $P(a_n) \in \left(P(u)^{2^n}\right)$. Ainsi, pour tout $n \geqslant m$, $P(a_n) = 0$, et donc la suite a_n stationne en a_m. En posant $s := a_m$, on a bien s qui est semi-simple car il est annulé par le polynôme P qui est sans facteur carré. De plus $n := u - s = u - a_m \in (P(u))$ d'après (iii), donc est bien nilpotent. On a donc bien montré l'existence des endomorphismes s et n, et on les a trouvés comme des éléments de $\mathbf{K}[u]$. Mais en plus on a donné un moyen effectif de les obtenir !

Étape 4 : Montrons l'unicité de la décomposition $u = s + n$.

Si s' et n' conviennent également : comme s' et n' commutent, s' commute avec $u = s' + n'$, donc avec tout polynôme en u (de même pour n'). Comme s et n (obtenus à l'étape précédente) sont des polynômes en u, s' et n' commutent avec s et n.
Or $s + n = s' + n'$, donc

$$s - s' = n' - n.$$

Dans le terme de droite, on a une somme de deux nilpotents qui commutent, donc $n' - n$ est nilpotent. Dans le terme de gauche, on a deux matrices diagonalisables dans $\overline{\mathbf{K}}$ (théorème 4.1) qui commutent, donc leur somme est diagonalisable. Finalement, $s - s'$ est à la fois nilpotent et diagonalisable dans $\overline{\mathbf{K}}$, donc nul. On en déduit que $s = s'$, puis $n = n'$.

Étape 5 : Un moyen plus utilisable en pratique pour trouver un polynôme P sans facteur carré tel que $P(u)$ soit nilpotent.

Lorsque $\mathbf{K}$ est de caractéristique nulle, le polynôme

$$P := \frac{\chi_u}{\operatorname{pgcd}(\chi_u, \chi_u')}$$

convient pour l'étape 1. En effet, décomposons χ_u en facteurs irréductibles dans $\mathbf{K}[X]$:

$$\chi_u = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_r^{\alpha_r}$$

(où les P_i sont deux à deux non-associés). Alors :

$$\chi_u' = \sum_{i=1}^{r} \alpha_i P_i' P_i^{\alpha_i - 1} \prod_{j \neq i} P_j^{\alpha_j}$$

et donc $P_1^{\alpha_1 - 1} P_2^{\alpha_2 - 1} \dots P_r^{\alpha_r - 1}$ divise χ_u'. On a donc :

$$\operatorname{pgcd}(\chi_u, \chi_u') = P_1^{\alpha_1 - 1} \dots P_r^{\alpha_r - 1} \operatorname{pgcd}\left(P_1 \dots P_r, \sum_{i=1}^{r} \alpha_i P_i' \prod_{j \neq i} P_j \right).$$

Montrons que

$$\operatorname{pgcd}\left(P_1 \dots P_r, \sum_{i=1}^{r} \alpha_i P_i' \prod_{j \neq i} P_j \right) = 1.$$

On aura ainsi $\operatorname{pgcd}(\chi_u, \chi_u') = P_1^{\alpha_1 - 1} \dots P_r^{\alpha_r - 1}$, et donc $P = \frac{\chi_u}{\operatorname{pgcd}(\chi_u, \chi_u')} = P_1 \dots P_r$ sera bien sans facteur carré, et $P(u)$ sera bien nilpotent.

Comme les P_k sont deux à deux premiers entre eux, il suffit de montrer que chaque P_k est premier avec la somme de droite pour en déduire que leur produit est aussi premier avec cette somme. On fixe donc un $k \in [\![1, r]\!]$, et on veut montrer que P_k est premier avec $\sum_i \alpha_i P_i' \prod_{j \neq i} P_j$.

Si, par l'absurde, P_k divisait $\sum_i \alpha_i P_i' \prod_{j \neq i} P_j$. Alors comme il divise tous les termes où $i \neq k$ (en effet, P_k apparaît dans le $\prod_{j \neq i} P_j$), il diviserait aussi $\alpha_k P_k' \prod_{j \neq k} P_j$.

Or P_k est premier avec $\alpha_k P_k' \prod_{j \neq k} P_j$. En effet, il ne divise pas $\prod_{j \neq k} P_j$, et il est également premier avec $\alpha_k P_k'$ car $\alpha_k \neq 0$ (on utilise ici l'hypothèse sur la caractéristique de $\mathbf{K}$ pour affirmer que la chute de l'exposant α_k ne tue pas ce terme) et P_k est premier avec P_k' car P est irréductible et $\mathbf{K}$ est un corps parfait (proposition 4.4).

Donc P_k ne divise pas $\sum_i \alpha_i P_i' \prod_{j \neq i} P_j$, et comme il est irréductible, il est premier avec cette somme. Finalement, le lemme de Gauss nous permet d'en déduire que le produit $P_1 \dots P_r$ est premier avec la somme, et de conclure comme nous l'avons expliqué auparavant.

□

6. Corps K tels que toute matrice symétrique à coefficients dans K est semi-simple.

Référence : RMS 126-2 p.176.

Prérequis : Nous allons utiliser la décomposition de Jordan-Chevalley sur un corps parfait vue dans la partie précédente, il faut donc savoir répondre à d'éventuelles questions là-dessus.

Notation : Comme nous allons beaucoup parler de matrices symétriques, on notera $\mathcal{S}_n(\mathbf{K})$ l'ensemble des matrices $n \times n$ à coefficients dans $\mathbf{K}$ qui sont symétriques.

Allons-y ! On sait d'après le théorème spectral que toute matrice symétrique réelle est diagonalisable (donc semi-simple). Notre but est de donner une caractérisation des corps $\mathbf{K}$ pour lesquels on a l'implication suivante :

$$M \in \mathcal{S}_n(\mathbf{K}) \implies M \text{ est semi-simple.} \tag{1}$$

Ces corps seront dit n-réels. Nous allons voir que cette question qui semble plongée dans le monde de l'algèbre linéaire admet une solution de nature très arithmétique. Plus précisément nous allons montrer les résultats suivants :

Théorème 6.1 (*Cas* $n = 2$) **:**
Soit $\mathbf{K}$ un corps. $\mathbf{K}$ est 2-réel si et seulement si -1 n'est pas un carré dans $\mathbf{K}$.

Théorème 6.2 (*Cas* $n \geqslant 3$) **:**
Soit $\mathbf{K}$ un corps et $n \geqslant 3$.

(*i*) Si $\mathrm{char}(\mathbf{K}) \neq 0$, alors $\mathbf{K}$ n'est pas n-réel.

(*ii*) Si $\mathrm{char}(\mathbf{K}) = 0$, $\mathbf{K}$ est n-réel si et seulement si -1 n'est pas la somme de $n-1$ carrés dans $\mathbf{K}$.

Cette dernière condition peut se réécrire comme « l'équation $x_1^2 + x_2^2 + \cdots + x_{n-1}^2 = -1$ n'a pas de solution $(x_1, x_2, \ldots, x_{n-1}) \in \mathbf{K}^{n-1}$ » ce qui est finalement une condition de nature assez arithmétique.

▷ Commençons par prouver le théorème 6.1. Soit $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in \mathcal{S}_2(\mathbf{K})$. Son polynôme caractéristique est donné par :

$$\chi_A = X^2 - \mathrm{tr}(A)X + \det(A) = X^2 - (a+c)X + ac - b^2$$

Il y a trois cas possibles :

- *le polynôme caractéristique de A n'a pas de racine dans $\mathbf{K}$.*
  Dans ce cas, $\chi_A \in \mathbf{K}[X]$ est de degré 2 sans racine dans $\mathbf{K}$, donc il est irréductible dans $\mathbf{K}[X]$. Comme $\pi_A \mid \chi_A$, et $\deg(\pi_A) \geqslant 1$, $\pi_A = \chi_A$. Donc π_A est sans facteur carré dans $\mathbf{K}[X]$ et A est semi-simple (sans contrainte sur le corps $\mathbf{K}$).

- *le polynôme caractéristique de A a deux racines distinctes dans $\mathbf{K}$.*
  Dans ce deuxième cas, A annule un polynôme scindé à racines simples dans $\mathbf{K}[X]$, donc A est diagonalisable sur $\mathbf{K}$, donc semi-simple (là encore peu importe le corps $\mathbf{K}$).

- *le polynôme caractéristique de A a une racine double dans* $\mathbf{K}$.
  Ce cas correspond à $\mathrm{disc}(\chi_A) = (a-c)^2 + 4b^2 = 0$. Il existe $\lambda \in \mathbf{K}$ tel que $\chi_A = (X-\lambda)^2$. On a donc $\pi_A = X - \lambda$ ou $\pi_A = (X-\lambda)^2$, et seule la première alternative nous donne la semi-simplicité de A. Or $\pi_A = X - \lambda$ implique que A est l'homothétie de rapport λ.

Ainsi, le corps $\mathbf{K}$ est 2-réel si et seulement si pour toute matrice $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in \mathcal{S}_2(\mathbf{K})$ telle que $\mathrm{disc}(\chi_A) = 0$, on a $a = c$ et $b = 0$.

Autrement dit, $\mathbf{K}$ est 2-réel si et seulement si :

$$\forall (a,b,c) \in \mathbf{K}^3, \left[(a-c)^2 + 4b^2 = 0 \implies b = 0 \text{ et } a = c\right].$$

si et seulement si :

$$\forall (a,b,c) \in \mathbf{K}^3, \left[(a-c)^2 + 4b^2 = 0 \implies b = 0\right].$$

Maintenant, si $\mathrm{char}(\mathbf{K}) \neq 2$, il est facile de montrer à l'aide de cette dernière équivalence que $\mathbf{K}$ est 2-réel si et seulement si -1 n'est pas un carré dans $\mathbf{K}$ (raisonner par contraposée dans les deux sens).

Si $\mathrm{char}(\mathbf{K}) = 2$, il suffit de considérer la matrice $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ pour obtenir une matrice symétrique qui n'est pas semi-simple. Donc $\mathbf{K}$ n'est pas 2-réel (et $-1 = 1$ est un carré dans un corps de caractéristique 2). On a donc bien montré le théorème 6.1.

▷ Passons à la démonstration du théorème 6.2. Soit $n \geqslant 3$. On montre d'abord le sens « $\Rightarrow$ » de l'équivalence du point (ii). Par contraposée, supposons que -1 est la somme de $n-1$ carrés dans $\mathbf{K}$, et montrons que $\mathbf{K}$ n'est pas n-réel.

Soit $a_1, \ldots, a_{n-1} \in \mathbf{K}$ tels que $-1 = a_1^2 + \cdots + a_{n-1}^2$. On introduit :

$$X := \begin{pmatrix} a_1 \\ \vdots \\ a_{n-1} \\ 1 \end{pmatrix} \in \mathbf{K}^n \text{ et } A := X\,{}^tX = \begin{pmatrix} a_1\,{}^tX \\ \vdots \\ a_{n-1}\,{}^tX \\ {}^tX \end{pmatrix} \in \mathcal{M}_n(\mathbf{K})$$

Montrons que $A \in \mathcal{S}_n(\mathbf{K})$ et que A n'est pas semi-simple.

- A est symétrique par construction (${}^tA = {}^t(X\,{}^tX) = X\,{}^tX = A$).
- $\ker(A)$ est un sous-espace stable par A qui n'admet aucun supplémentaire stable. Tout repose sur le fait que $A^2 = 0$ (on a tout fait pour). En effet : $A^2 = \left(X\,{}^tX\right)^2 = X\left({}^tXX\right)\,{}^tX$. Or ${}^tXX = 1 + a_1^2 + \cdots + a_{n-1}^2 = 0$ (par choix des a_i), donc on a bien $A^2 = 0$.

  Considérons F un supplémentaire de $\ker(A)$ dans $\mathbf{K}^n$. F n'est pas réduit à $\{0\}$ car A n'est pas nulle (sa dernière ligne est ${}^tX \neq 0$). Si $Y \in F \setminus \ker(A)$, alors $AY \in \ker(A)$ car $A^2 = 0$ et $AY \neq 0$ car $Y \notin \ker(A)$. Puisque F et $\ker(A)$ sont en somme directe, on en déduit que $AY \notin F$. Ainsi, F n'est pas stable par A. On a donc montré que A admettait un sous espace stable ($\ker(A)$) n'admettant aucun supplémentaire stable, donc A n'est pas semi-simple.

Ainsi, il existe une matrice de $\mathcal{S}_n(\mathbf{K})$ qui n'est pas semi-simple, donc $\mathbf{K}$ n'est pas n-réel. Remarquons que nous n'utilisons pas l'hypothèse $\mathrm{char}(\mathbf{K}) = 0$ du point (ii), de sorte que cette

implication s'applique également pour des corps de caractéristique non nulle. Pour montrer le point (i) du théorème 6.2 il suffit donc de montrer que lorsque $\mathrm{char}(\mathbf{K}) \neq 0$, -1 s'écrit comme somme de $n-1$ carrés dans $\mathbf{K}$.

Soit p un nombre premier. L'équation $x^2 = -1 - y^2$, d'inconnues $x, y \in \mathbf{F}_p$ admet une solution. En effet, pour $p = 2$, $(x, y) = (1, 0)$ est solution, et pour $p \neq 2$, il suffit de dénombrer les ensembles parcourus par x^2 et $-1 - y^2$ lorsque x et y parcourent $\mathbf{F}_p$. Comme p est premier impair, on sait que $\left|\left(\mathbf{F}_p^\times\right)^2\right| = \frac{p-1}{2}$, et donc qu'il y a $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ carrés dans $\mathbf{F}_p$. Ainsi, si on note $A := \{x^2 \mid x \in \mathbf{F}_p\}$ et $B := \{-1 - y^2 \mid y \in \mathbf{F}_p\}$, on a $|A| = \frac{p+1}{2}$ et $|B| = \frac{p+1}{2}$. Donc :

$$|A \cap B| = |A| + |B| - |A \cup B| = p + 1 - |A \cup B|$$

Or $A \cup B \subseteq \mathbf{F}_p$, donc $|A \cup B| \leqslant p$. On en déduit que $|A \cap B| \geqslant 1$, d'où l'existence d'un couple $(x, y) \in \mathbf{F}_p$ tel que $x^2 + y^2 = -1$. Maintenant, si $\mathbf{K}$ est un corps de caractéristique p, alors $\mathbf{K}$ contient une copie de $\mathbf{F}_p$, donc comme -1 est la somme de deux carrés dans $\mathbf{F}_p$, il est somme de deux carrés dans $\mathbf{K}$.

D'après ce qu'on a prouvé au-dessus, ceci implique que $\mathbf{K}$ n'est pas 3-réel, donc n'est pas n-réel pour $n \geqslant 3$. On a montré le point (i) du théorème 6.2. Il reste à montrer le sens « $\Leftarrow$ »du point (ii). On considère donc un corps $\mathbf{K}$ de caractéristique nulle, tel que -1 n'est pas la somme de $n-1$ carrés dans $\mathbf{K}$. On veut montrer que nécessairement $\mathbf{K}$ est n-réel. C'est le sens qui demande le plus de travail, on le découpe en plusieurs lemmes.

Lemme 6.3 :
Si $A \in \mathcal{S}_n(\mathbf{K})$, alors les deux matrices de sa décomposition de Jordan-Chevalley sont également symétriques.

Démo : Soit $A \in \mathcal{S}_n(\mathbf{K})$. Soit $(D, N) \in \mathcal{M}_n(\mathbf{K})^2$ avec :

$$\begin{cases} A = D + N \\ D \text{ semi-simple} \\ N \text{ nilpotente} \\ DN = ND \end{cases}$$

sa décomposition de Jordan-Chevalley[3]. Puisque A est symétrique, on a :

$${}^tA = {}^t(D+N) = \underbrace{{}^tD + {}^tN = A}_{(*)}$$

Or :

- N nilpotente $\implies$ ${}^tN$ nilpotente
- D semi-simple $\implies$ ${}^tD$ semi-simple (par exemple parce que D et ${}^tD$ ont le même polynôme minimal)
- D et N commutent $\implies$ ${}^tD$ et ${}^tN$ commutent.

Ainsi, l'égalité $(*)$ est une décomposition de Jordan-Chevalley de A, donc par unicité de cette décomposition, on a $N = {}^tN$ et $D = {}^tD$. □

Notons $\mathcal{N}_n(\mathbf{K}) := \{\text{matrices nilpotentes de } \mathcal{M}_n(\mathbf{K})\}$ et $\mathcal{R}_n(\mathbf{K}) := \{A \in \mathcal{M}_n(\mathbf{K}) \mid A^2 = 0\}$

[3]NB : On utilise ici l'hypothèse $\mathrm{char}(\mathbf{K}) = 0$, car la décomposition de Jordan-Chevalley nécessite que le corps soit parfait.

Lemme 6.4 :
$\mathbf{K}$ est n-réel $\iff \mathcal{S}_n(\mathbf{K}) \cap \mathcal{N}_n(\mathbf{K}) = \{0\}$

Démo : « $\Rightarrow$ » Soit $N \in \mathcal{S}_n(\mathbf{K}) \cap \mathcal{N}_n(\mathbf{K})$. Alors comme N est nilpotente $\chi_N = X^n$. Donc il existe $k \in [\![1, n]\!]$ tel que $\pi_N = X^k$. Or N est symétrique et $\mathbf{K}$ est supposé n-réel, donc N est semi-simple, donc son polynôme minimal est sans facteur carré, donc $\pi_N = X$, d'où $N = 0$.

« $\Leftarrow$ » Soit $A \in \mathcal{S}_n(\mathbf{K})$. Soit $A = D + N$ sa décomposition de Jordan-Chevalley dans $\mathcal{M}_n(\mathbf{K})$. D'après le lemme 6.3, $N \in \mathcal{S}_n(\mathbf{K})$, et comme elle est également nilpotente, elle est nulle par hypothèse.

□

Lemme 6.5 :
$\mathbf{K}$ est n-réel $\iff \mathcal{S}_n(\mathbf{K}) \cap \mathcal{R}_n(\mathbf{K}) = \{0\}$

Démo : Le sens « $\Rightarrow$ » découle directement du lemme précédent.

« $\Leftarrow$ » On va montrer que si $\mathcal{S}_n(\mathbf{K}) \cap \mathcal{R}_n(\mathbf{K}) = \{0\}$, alors $\mathcal{S}_n(\mathbf{K}) \cap \mathcal{N}_n(\mathbf{K}) = \{0\}$, ce qui conclut grâce au lemme précédent.

Soit $A \in \mathcal{M}_n(\mathbf{K})$, à la fois symétrique est nilpotente. Soit $p \in \mathbf{N}$ tel que $2^p \geqslant n$. Alors $A^{2^p} = 0$, donc $A^{2^{p-1}} \in \mathcal{R}_n(\mathbf{K}) \cap \mathcal{S}_n(\mathbf{K})$, qui est réduit à $\{0\}$ par hypothèse, donc $A^{2^{p-1}} = 0$. Mais on peut continuer ! Le même raisonnement mené à partir de $A^{2^{p-1}} = 0$ permet de montrer que $A^{2^{p-2}} = 0$, et donc finalement : pour tout $k \in \mathbf{N}$, $A^{2^k} = 0$, d'où $A = 0$. Ainsi $\mathcal{S}_n(\mathbf{K}) \cap \mathcal{N}_n(\mathbf{K}) = \{0\}$, et donc (lemme 6.4) : $\mathbf{K}$ est n-réel. □

Fin de la preuve du théorème 6.2 :

Si -1 n'est pas la somme de $n-1$ carrés dans $\mathbf{K}$, montrons que $\mathbf{K}$ est n-réel en utilisant la caractérisation donnée par le lemme 6.5. Soit $A \in \mathcal{R}_n(\mathbf{K}) \cap \mathcal{S}_n(\mathbf{K})$. Pour tout $(i, j) \in [\![1, n]\!]^2$, le coefficient (i, j) de A^2 est nul :

$$\sum_{k=1}^{n} a_{i,k} a_{k,j} = 0.$$

En particulier, pour $i = j$, et en utilisant le fait que $A \in \mathcal{S}_n(\mathbf{K})$, on obtient :

$$\forall i \in [\![1, n]\!], \ \sum_{k=1}^{n} a_{i,k} a_{k,i} = \sum_{k=1}^{n} a_{i,k}^2 = 0$$

Et ceci implique que tous les $a_{i,k}$ sont nuls, car sinon on contradirait l'hypothèse selon laquelle -1 ne peut pas s'écrire comme somme de $n-1$ carrés. Ainsi, $A = 0$, d'où la conclusion. □

Remarques :

- La fin de la preuve permet de mieux comprendre ce vocabulaire de corps n-réel. En effet, dans $\mathbf{R}$, si une somme de carrés est nulle, alors tous ses termes sont nuls, grâce au signe. Dans un corps $\mathbf{K}$ quelconque, l'implication est fausse en général, mais les corps n-réels sont ceux dans lesquels on peut l'utiliser.
- *Pour la culture :* Ce développement soulève la question suivante : si on se donne un corps $\mathbf{K}$, quel est le nombre minimal d'éléments de $\mathbf{K}$ nécessaires à l'écriture de -1 comme une somme de carrés ? Ce nombre est appelé niveau d'un corps, et il y a des théorèmes un peu fous à ce sujet ! Merci a Matthieu Romagny de s'être renseigné sur la question. Voir par exemple le mémoire de maîtrise de Lionel Fourquaux, disponible ici : https://math.lionel.fourquaux.org/publications/. Le niveau d'un corps est soit infini, soit une puissance de 2.

Finissons par quelques exemples :

(a) -1 est un carré dans $\mathbf{C}$, donc $\mathbf{C}$ n'est pas 2-réel, et en effet : $A := \begin{pmatrix} i & 1 \\ 1 & -i \end{pmatrix} \in \mathcal{S}_2(\mathbf{C})$ et n'est pourtant pas semi-simple. En effet, $\chi_A = X^2$, donc $\pi_A = X$ ou X^2 et comme $A \neq 0$, $\pi_A = X^2$. Ainsi, π_A n'est pas sans facteurs carrés dans $\mathbf{C}[X]$, donc A n'est pas semi-simple.

(b) -1 n'est jamais un carré ou une somme de carrés dans $\mathbf{R}$, donc $\mathbf{R}$ est n-réel pour tout $n \geqslant 2$. C'est-à-dire : toute matrice symétrique réelle est diagonalisable dans $\mathbf{C}$. En fait, le théorème spectral nous dit même mieux, car toute matrice symétrique réelle est en fait diagonalisable dans $\mathbf{R}$.

(c) Dans $\mathbf{F}_5$, $-1 = 4$ est un carré, donc $\mathbf{F}_5$ n'est pas 2-réel. Par exemple, la matrice $A := \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} \in \mathcal{S}_2(\mathbf{F}_5)$ n'est pas semi-simple (même argument que pour le point (a)).

Commentaire personnel : Je trouvais la discussion sur le cas $n = 2$ un petit peu délicate à présenter au tableau. Je pense que si j'avais présenté ce développement le jour J, j'aurais opté pour un théorème unifié : on suppose $\mathbf{K}$ parfait (pour bénéficier de la décomposition de Jordan-Chevalley) et $n \geqslant 2$, puis on montre que $\mathbf{K}$ est n-réel si et seulement si -1 n'est pas la somme de $n-1$ carrés dans $\mathbf{K}$. Les arguments sont les mêmes que pour le point (ii) du théorème 6.2. Cependant il est bon d'avoir vu le reste pour savoir dire qu'en fait cette caractérisation donne toujours la même chose dans le cas des corps finis pour $n \geqslant 3$: ils ne sont jamais n-réels. En plus l'argument de cardinalité qui conduit à l'existence de solutions dans $\mathbf{F}_p$ à l'équation $x^2+y^2 = -1$ sert à d'autres moments ! Par exemple lorsqu'on étudie si une forme quadratique sur un corps fini représente un élément du corps.

7. Annexe

Cette annexe contient quelques résultats utilisés précédemment, ou des résultats en lien plus ou moins direct avec les discussions ci-dessus. En tout cas ce sont des petites propriétés utiles, qui sont parfois utilisées implicitement, et j'ai parfois mis longtemps à m'en convaincre ou à trouver une preuve qui me plaisait, donc je me suis dit que ça pourrait faire gagner du temps de les reproduire ici.

7.1. Polynôme minimal et extensions de corps

Soit $\mathbf{L}/\mathbf{K}$ une extension de corps, et soit $A \in \mathcal{M}_n(\mathbf{K})$. On note $\pi_{A,\mathbf{K}}$ son polynôme minimal, c'est-à-dire l'unique générateur unitaire de l'idéal

$$I_{A,\mathbf{K}} := \{P \in \mathbf{K}[X] \mid P(A) = 0\}.$$

On peut également voir A comme un élément de $\mathcal{M}_n(\mathbf{L})$, et dans ce cas on note $\pi_{A,\mathbf{L}}$ son polynôme minimal : l'unique générateur unitaire de l'idéal

$$I_{A,\mathbf{L}} := \{P \in \mathbf{L}[X] \mid P(A) = 0\}.$$

Proposition 7.1 :
Avec les notations introduites ci-dessus, on a $\pi_{A,\mathbf{K}} = \pi_{A,\mathbf{L}}$.

Démo : $\pi_{A,\mathbf{K}}$ est en particulier un polynôme de $\mathbf{L}[X]$ annulant A, donc il appartient à $I_{A,\mathbf{L}}$. Ainsi, $\pi_{A,\mathbf{L}}$ divise $\pi_{A,\mathbf{K}}$ dans $\mathbf{L}[X]$. Comme ils sont tous deux unitaires, il suffit de montrer qu'ils

ont le même degré pour conclure.

Or le degré de $\pi_{A,\mathbf{K}}$ est égal au rang de la famille $\{I_n, A, \ldots, A^n\}$ (vue comme une famille de vecteurs de $\mathcal{M}_n(\mathbf{K})$), tandis que le degré de $\pi_{A,\mathbf{L}}$ est égal au rang de cette même famille vue comme une famille de vecteurs de $\mathcal{M}_n(\mathbf{L})$.

On range les matrices $E_{i,j}$ de la base canonique de $\mathcal{M}_n(\mathbf{K})$ dans l'ordre lexicographique (par exemple), et on note $\mathcal{C}$ la base $(E_1, \ldots, E_{n^2})$ de $\mathcal{M}_n(\mathbf{K})$ obtenue. On note M la matrice dont les colonnes sont les coordonnées en base $\mathcal{C}$ des vecteurs $I_n, A, \ldots, A^n$:

$$M := \mathrm{Mat}_{\mathcal{C}}\left(I_n, A, \ldots, A^n\right).$$

Il s'agit de montrer que le rang de M est le même que l'on considère M comme une matrice à coefficients dans $\mathbf{K}$ ou comme une matrice à coefficients dans $\mathbf{L}$. Mais le rang est la taille maximale des matrices inversibles extraites de M, et donc se détermine en calculant les déterminants des matrices extraites de M : une opération qui reste dans $\mathbf{K}$ même si l'on choisit de voir M comme une matrice à coefficients de $\mathbf{L}$. □

Remarques :

- Au passage, on a rappelé la caractérisation du rang comme la taille maximale des matrices inversibles extraites de M. Cette caractérisation permet de voir facilement que si $M \in \mathcal{M}_n(\mathbf{K})$ et $\mathbf{L}/\mathbf{K}$ est une extension de corps, le rang de M comme élément de $\mathcal{M}_n(\mathbf{L})$ est le même que le rang de M comme élément de $\mathcal{M}_n(\mathbf{K})$.

- On peut également montrer la proposition 7.1 en faisant appel à la réduction de Frobenius. En effet, la suite des invariants de similitude de A (vue comme une matrice à coefficients dans $\mathbf{K}$) satisfait les propriétés demandées à la suite des invariants de similitude de A (vue comme une matrice à coefficients dans $\mathbf{L}$) : par unicité, c'est la suite des invariants de similitude de A (vue comme une matrice à coefficients dans $\mathbf{L}$). En particulier, le dernier invariant de similitude (le plus grand pour le relation de divisibilité) est le même, et il s'agit du polynôme minimal.

7.2. Le polynôme minimal et le polynôme caractéristique ont les mêmes facteurs irréductibles

Cette propriété m'a occupé une bonne partie de l'année. On peut la montrer en disant qu'ils ont les mêmes racines, mais cela nous oblige à nous placer dans un corps contenant les valeurs propres, et peut embarquer dans des questions sur l'existence d'un tel corps... Ce n'est pas forcément compliqué ou dangereux de faire ça, mais je préfère la démonstration suivante, qui ne fait pas appel à des extensions des corps, ni à des théorèmes de réduction de matrices (du style Jordan ou Frobenius). On peut la trouver dans le livre de réduction des endomorphismes de Roger Mansuy (page 81).

Proposition 7.2 :
Soit $\mathbf{K}$ un corps, $A \in \mathcal{M}_n(\mathbf{K})$. Son polynôme minimal et son polynôme caractéristique ont les mêmes facteurs irréductibles dans $\mathbf{K}[X]$.

Démo : Notons π_A le polynôme minimal de A, et χ_A son polynôme caractéristique.

- D'après le théorème de Cayley-Hamilton, π_A divise χ_A, donc tout facteur irréductible de π_A est un facteur irréductible de χ_A.

- Réciproquement, pour montrer que tout facteur irréductible de χ_A est un facteur irréductible de π_A, il suffit de montrer que χ_A divise π_A^n. Notons

$$\pi_A(X) := X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0.$$

Puisque $\pi_A(A) = 0$, on a :

$$\begin{aligned}\pi_A(X)I_n &= \pi_A(X)I_n - \pi_A(A) \\ &= \left(X^m + \cdots + a_1X + a_0\right) I_n - \left(A^m + \cdots + a_1A + a_0I_n\right) \\ &= (XI_n)^m - A^m + a_{m-1}\left((XI_n)^{m-1} - A^{m-1}\right) + \cdots + a_1(XI_n - A)\end{aligned}$$

Or XI_n et A commutent dans l'anneau $\mathcal{M}_n(\mathbf{K}[X])$, donc les termes en $(XI_n)^k - A^k$ se factorisent par $XI_n - A$. Donc il existe $M \in \mathcal{M}_n(\mathbf{K}[X])$ telle que :

$$\pi_A(X)I_n = (XI_n - A)M.$$

En passant au déterminant,

$$\pi_A(X)^n = \underbrace{\det(XI_n - A)}_{=\chi_A(X)}\underbrace{\det(M)}_{\in\mathbf{K}[X]},$$

ce qui donne la relation de divisibilité voulue !

□

7.3. Somme d'un inversible et d'un nilpotent qui commutent

Un petit lemme utilisé dans la démonstration de la décomposition de Dunford-Jordan-Chevalley :

Lemme 7.3 :
Soit A un anneau. Soit $a \in A$ un élément inversible, et $n \in A$ un élément nilpotent. Si a et n commutent, alors $a + n$ est inversible.

Démo : Puisque $a+n = a\left(1_A + a^{-1}n\right)$ et que a est inversible, il suffit de montrer que $\left(1_A + a^{-1}n\right)$ est inversible. On s'inspire alors du développement en série entière :

$$\frac{1}{1+x} = \sum_{k=0}^{+\infty}(-1)^k x^k$$

pour trouver un inverse à $\left(1_A + a^{-1}n\right)$. Comme a et n commutent, a^{-1} et n commutent également, et comme n est nilpotent, $a^{-1}n$ l'est aussi. Ainsi, la somme candidate

$$\sum_{k=0}^{+\infty}(-1)^k\left(a^{-1}n\right)^k$$

(qui n'a pas de sens dans l'anneau A) peut-être remplacée par une somme finie, et on vérifie que ceci nous donne bien un inverse pour $\left(1_A + a^{-1}n\right)$. □

8. Références

- RMS 129-1.
- Grégory Berhuy : *Algèbre, le grand combat.*
- Roger Mansuy : *Réduction des endomorphismes.*
- Philippe Caldero et Jérôme Germoni : *Nouvelles histoires hédonistes de groupes et de géométries, tome 1.*

- Les développements de Benjamin Havret (disponibles sur sa page http://www.normalesup.org/~havret/).
- J. Risler et P. Boyer : *Algèbre pour la licence 3 : groupes, anneaux, corps.*
- RMS 126-2.
- Complément de cours de Matthieu Romagny sur les algèbres de dimension finie.