# Algèbres de dimension finie
# Décomposition de Jordan-Chevalley, exponentielle

## Table des matières



# 1 Algèbres de dimension finie : définitions élémentaires

## 1.1 Algèbres, éléments algébriques, polynôme minimal

**1.1.1 Définitions.** (1) Une algèbre (associative, unitaire) sur un corps $k$ est un $k$-espace vectoriel $A$ muni d'une structure d'anneau (associatif, unitaire) dont la multiplication est bilinéaire.

(2) Un élément $a \in A$ est *transcendant* si le morphisme d'évaluation $\mathrm{ev}_a : k[X] \to A$, $P \mapsto P(a)$ est injectif. Il est *algébrique* sinon. On appelle alors *polynôme minimal de $a$* noté $\mu_a$ le générateur unitaire de $\ker(\mathrm{ev}_a)$. On appelle *degré de $a$* le degré de son polynôme minimal.

L'image de $\mathrm{ev}_a$ est la sous-algèbre $k[a] \subset A$ des polynômes en $a$, c'est-à-dire la sous-algèbre de $A$ engendrée par $a$. C'est une algèbre commutative et $\mathrm{ev}_a$ induit un isomorphisme $k[X]/(\mu_a) \xrightarrow{\sim} k[a]$.

**1.1.2 Exercice.** À toute $k$-algèbre associative, unitaire $A$ on associe l'application $f_A : k \to A$ définie par $f_A(x) = x \cdot 1$. Montrez que $f_A$ est un morphisme d'anneaux dont l'image est incluse dans le centre de $A$. Maintenant soit $A$ un $k$-espace vectoriel. Montrez que la donnée d'une structure de $k$-algèbre (associative, unitaire) sur $A$ est équivalente à la donnée d'une structure d'anneau (associatif, unitaire) et d'un morphisme d'anneaux $k \to A$ dont l'image est incluse dans le centre de $A$.

Dans la suite, nous serons intéressés principalement par les $k$-algèbres qui sont de dimension finie (en tant qu'espaces vectoriels). Dans une telle algèbre, pour une raison de dimension, tout élément est algébrique. Voici quelques exemples.

**1.1.3 Exemples.** (1) Le corps des complexes $\mathbb{C}$ est une $\mathbb{R}$-algèbre de dimension 2. N'importe quelle extension finie de corps $K/k$ est une $k$-algèbre de dimension finie.

(2) L'algèbre des quaternions $\mathbb{H}$ (voir section 4). C'est une $\mathbb{R}$-algèbre de dimension 4, de base $\{1, i, j, k\}$ avec les relations $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$. Tout quaternion $q = a + bi + cj + dk$ possède un *conjugué* $\overline{q} = a - bi - cj - dk$, une *norme* $N(q) = q\overline{q} \in \mathbb{R}$ et une *trace* $T(q) = q + \overline{q} \in \mathbb{R}$. Si l'on pose $n = N(q)$ et $t = T(q)$, on voit immédiatement que $q$ est racine du polynôme réel $X^2 - tX + n$ car celui-ci n'est rien d'autre que $(X - q)(X - \overline{q})$. On voit donc que si $q \notin \mathbb{R}$, il est algébrique de degré 2 sur $\mathbb{R}$. On en déduit facilement que la sous-algèbre $\mathbb{R}[q] \subset \mathbb{H}$ est isomorphe à $\mathbb{C}$. Ainsi $\mathbb{H}$ peut également être vue comme une $\mathbb{C} \simeq \mathbb{R}[q]$-algèbre de dimension 2.

(3) L'algèbre $\mathrm{M}_n(k)$ des matrices carrées de taille $n$. C'est un cas particulier de l'algèbre $\mathscr{L}(E)$ des endomorphismes d'un espace vectoriel $E$ de dimension finie.

(4) La sous-algèbre $\mathrm{T}_n(k) \subset \mathrm{M}_n(k)$ des matrices triangulaires supérieures, ou plus généralement la sous-algèbre $\mathrm{T}_{\underline{a}}(k)$ des matrices triangulaires supérieures par blocs, à blocs diagonaux de tailles fixées $\underline{a} = (a_1, \ldots, a_r)$ avec $a_1 + \cdots + a_r = n$. C'est un cas particulier de l'algèbre $\mathscr{L}_{\mathscr{F}}(E)$ des endomorphismes qui laissent stables les sous-espaces vectoriels d'une chaîne $\mathscr{F} = \{0 = F_0 \subset F_1 \subset \cdots \subset F_r = E\}$, avec $a_i = \dim(F_i/F_{i-1})$. Une telle chaîne est appelée *drapeau*.

(5) L'algèbre $\mathrm{D}_n(k)$ des matrices diagonales, ou plus généralement l'algèbre $\mathrm{D}_{\underline{a}}(k)$ des matrices diagonales par blocs, à blocs diagonaux de format $\underline{a}$ fixé. C'est un cas particulier de l'algèbre $\mathscr{L}_{\mathscr{G}}(E)$ des endomorphismes qui laissent stables les sous-espaces vectoriels d'une décomposition en somme directe $\mathscr{G} = \{G_1 \oplus \cdots \oplus G_r = E\}$, avec $a_i = \dim(G_i)$.

(6) L'algèbre $k[X]/(F)$, pour tout polynôme non nul $F \in k[X]$.

(7) La sous-algèbre $k[u, v] \subset \mathscr{L}(E)$ engendrée par deux endomorphismes $u, v$. Elle est commutative si et seulement si $uv = vu$.

**1.1.4 Lien avec le polynôme caractéristique.** Dans le cas où $A = \mathscr{L}(E)$, le polynôme minimal $\mu_a$ est très lié au polynôme caractéristique $\chi_a$. Voici quelques propriétés :

(1) *divisibilité* : on a $\mu_a \mid \chi_a$. C'est le théorème de Cayley-Hamilton.

(2) *facteurs irréductibles* : $\mu_a$ et $\chi_a$ ont les mêmes facteurs irréductibles. La lectrice pourra le démontrer à titre d'exercice très intéressant. Notez qu'aucune hypothèse sur le corps $k$ n'est nécessaire.

(3) *continuité* : $\chi_a$ est « continu » en $a$ alors que $\mu_a$ ne l'est pas (on se place sur $k = \mathbb{R}$ ou $\mathbb{C}$ pour pouvoir parler de continuité). En effet, si l'on fixe une base de $E$ on voit que les coefficients de $\chi_a$ sont des polynômes en les coefficients de l'endomorphisme $a$. Par exemple, en dimension 2, pour une matrice $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ on a $\chi_M(X) = X^2 - (a+d)X + (ad - bc)$ dont les coefficients $a + d$ et $ad - bc$ sont polynomiaux en $a, b, c, d$. En revanche, le polynôme minimal $\mu_a$ peut avoir des discontinuités : ainsi,

pour $M_t = \left(\begin{smallmatrix} t & 0 \\ 0 & 0 \end{smallmatrix}\right)$ on a $\mu_{M_t}(X) = X(X-t)$ pour $t \neq 0$, et $\mu_{M_0}(X) = X$ n'est pas égal à la limite de $\mu_{M_t}$ lorsque $t \to 0$.

On vient d'apprendre une mauvaise nouvelle : le polynôme minimal présente de mauvaises propriétés de continuité par rapport à $a$. Voici maintenant une bonne nouvelle : il est indépendant du corps de base $k$. Nous allons démontrer ceci dans le lemme suivant, où nous profitons de l'occasion pour démontrer la même propriété pour le pgcd (ce qui nous sera utile plus loin).

**1.1.5 Lemme.** *Soit $k$ un corps et $K/k$ une extension.*

(1) *Le pgcd de deux polynômes est indépendant du corps de base : pour tous $P, Q \in k[X]$ on a l'égalité* $\mathrm{pgcd}_K(P,Q) = \mathrm{pgcd}_k(P,Q)$ *entre les pgcd calculés dans $K[X]$ et dans $k[X]$.*

(2) *Le polynôme minimal est indépendant du corps de base : pour toute matrice $M \in \mathrm{M}_n(k)$, on a l'égalité $\mu_{M,K} = \mu_{M,k}$ entre les polynômes minimaux de $M$ comme élément de $\mathrm{M}_n(K)$ ou de $\mathrm{M}_n(k)$.*

**Preuve :** (1) Le pgcd se calcule par l'algorithme d'Euclide, qui est le même dans $k[X]$ et dans $K[X]$ (il ne fait d'ailleurs intervenir que des polynômes qui appartiennent à $k[X]$).
(2) Soit $d = \deg \mu_{M,K}$. Par définition c'est le plus grand entier $e$ tel que $\mathrm{Id}, M, M^2, \ldots, M^{e-1}$ est une famille libre dans l'espace vectoriel $\mathrm{M}_n(K)$. Écrivons ces matrices comme des vecteurs colonnes sur la base canonique $E_{i,j}$ et formons la matrice rectangulaire $X_e := (\mathrm{Id}, M, M^2, \ldots, M^{e-1}) \in \mathrm{M}_{e,n^2}(k)$. Ce qui précède s'exprime ainsi : $X_d$ possède un mineur de taille $d$ non nul, et $X_{d+1}$ a tous ses mineurs de taille $d+1$ nuls. On voit que ces conditions s'expriment dans $k$ (le point crucial est que $X_e$ est à coefficients dans $k$) et ne dépendent donc pas de $K$. Il en découle que $d = \deg \mu_{M,K} = \deg \mu_{M,k}$. Enfin $\mu_{M,K} \mid \mu_{M,k}$ puisque $\mu_{M,k}$ est un polynôme de $K[X]$ annulateur de $M$. Étant tous deux unitaires de même degré, ces polynômes sont égaux. □

## 1.2 Propriétés des éléments algébriques

On travaille avec un corps $k$ et une $k$-algèbre (associative, unitaire) de dimension finie $A$.

**1.2.1 Définitions.** Soit $a \in A$ de polynôme minimal $\mu_a$. On dit que $a$ est *nilpotent* si $\mu_a = X^r$ pour un certain $r \geqslant 1$, *unipotent* si $a - 1$ est nilpotent, et *semi-simple* si $\mu_a$ est sans facteur carré.

La notion de nilpotence, et la notion d'unipotence qui en est une variante multiplicative, sont classiques. La semi-simplicité l'est moins, et nous allons expliquer ce qu'elle signifie dans le cas des algèbres de matrices $\mathrm{M}_n(k)$ lorsque le corps $k$ est parfait. Rappelons que :

**1.2.2 Définition.** Un corps $k$ est dit *parfait* s'il est de caractéristique 0, ou s'il est de caractéristique $p > 0$ et son endomorphisme de Frobenius $\mathrm{Fr} : k \to k$, $x \mapsto x^p$ est surjectif (donc bijectif).

Les corps finis ou algébriquement clos sont parfaits. Si $k_0$ est de caractéristique $p$, le corps de fractions rationnelles $k = k_0(X)$ n'est pas parfait, car $X$ n'est pas une puissance $p$-ième (c'est un élément de degré 1 alors que les puissances $p$-ièmes sont de degré multiple de $p$).

**1.2.3 Lemme.** *Soit $k$ un corps parfait et $\overline{k}$ une clôture algébrique de $k$. Une matrice $A \in \mathrm{M}_n(k)$ est semi-simple si et seulement si $A$ est diagonalisable dans $\mathrm{M}_n(\overline{k})$.*

**Preuve :** On notera $p \geqslant 0$ la caractéristique de $k$. Les subtilités de la démonstration sont présentes surtout lorsque $p > 0$. Le point crucial est que dans un corps parfait, tout polynôme de dérivée nulle est une puissance $p$-ème. En effet, si $P' = 0$, en écrivant $P = \sum a_i X^i$, on voit que les $a_i$ avec $i$ premier à $p$ sont nuls. Il reste les $a_i$ avec $i = jp$. Si on écrit $a_{jp} = b_j^p$, on obtient $P = (\sum b_j X^j)^p$.

Supposons que $A$ est semi-simple et soit $\mu$ son polynôme minimal, qui s'écrit donc $\mu = P_1 \dots P_r$ où les $P_i$ sont irréductibles distincts. Soit $P$ l'un des $P_i$ et montrons que chacune de ses racines $\alpha$ dans $\overline{k}$ est simple. Comme $P$ est irréductible, il est égal au polynôme minimal de $\alpha$ sur $k$. En caractéristique $p = 0$ on a certainement $P' \neq 0$. Dans le cas de caractéristique $p > 0$, comme $P$ est irréductible ce n'est pas une puissance $p$-ème, donc d'après ce qu'on a dit au-dessus, le fait que $k$ soit parfait implique que $P' \neq 0$. Il s'ensuit que $P'(\alpha) \neq 0$, donc $P \mid P'$ ce qui est impossible pour des raisons de degré. Donc les racines de $P$ dans $\overline{k}$ sont simples. Maintenant montrons que $P_i, P_j$ n'ont pas de racine commune dans $\overline{k}$ si $i \neq j$. En effet, si $P_i(\alpha) = P_j(\alpha) = 0$, utilisant 1.1.5(1) on voit que $\operatorname{pgcd}_k(P_i, P_j) = \operatorname{pgcd}_{\overline{k}}(P_i, P_j) \neq 1$ ce qui est une contradiction. On conclut que les racines de $\mu$ dans $\overline{k}$ sont toutes distinctes. Comme $A$ est annulé par $\mu$, il est diagonalisable dans $\mathrm{M}_n(\overline{k})$.

Réciproquement supposons $A$ diagonalisable dans $\mathrm{M}_n(\overline{k})$. Alors $\mu_{A,\overline{k}}$ est à racines simples dans $\overline{k}$. D'après 1.1.5(2), on a $\mu_{A,k} = \mu_{A,\overline{k}}$ qui est certainement sans facteur carré. □

## 1.3 Représentations linéaires et semi-simplicité

**1.3.1 L'idée des représentations.** Les ensembles de bijections d'ensembles ou de transformations bijectives de certaines structures comme les espaces vectoriels sont des *groupes*. Ceci a pour conséquence qu'on peut « représenter » un groupe donné $G$ comme groupe de bijections au moyen de morphismes $\rho : G \to \mathfrak{S}_X$ ou $\rho : G \to \mathrm{GL}(E)$. Ceci permet de mieux l'étudier, utilisant par exemple toute notre connaissance de l'algèbre linéaire. On parle de *représentations ensemblistes* ou *linéaires* de $G$. Dans le cas linéaire, l'espace vectoriel $E$ est appelé l'*espace de la représentation*.

De la même manière, les ensembles d'endomorphismes de $k$-espaces vectoriels sont des *$k$-algèbres* (associatives unitaires) et on peut « représenter » une $k$-algèbre donnée $A$ comme ensemble d'endomorphismes linéaires au moyen de morphismes $\rho : A \to \mathrm{End}(E)$. On parle de *représentations linéaires* de $A$. Pour que la théorie soit souple et complète, on autorise tous les morphismes $\rho$, mais les représentations d'un groupe ou d'une algèbre qui la reflètent le mieux sont celles pour lesquelles $\rho$ est injectif, qu'on appelle représentations *fidèles*.

**1.3.2 Exemples.** Voici les deux familles les plus importantes de représentations fidèles.

(1) Représentations naturelles. Si $G \subset \mathfrak{S}_n$, il a une représentation dite *naturelle* dans l'ensemble $\{1, \dots, n\}$ correspondant au morphisme d'inclusion donné $\rho : G \hookrightarrow \mathfrak{S}_n$. Si $G \subset \mathrm{GL}(E)$, il a une représentation naturelle dans l'espace vectoriel $E$. Si $A \subset \mathrm{End}(E)$, elle a une représentation naturelle dans l'espace vectoriel $E$.

(2) Représentations régulières. Il s'agit des représentations obtenues en faisant agir un groupe ou une algèbre sur lui-même, resp. sur elle-même, par multiplication à gauche ou à droite.
(a) La *représentation (ensembliste) régulière gauche* du groupe $G$ est la représentation $L : G \to \mathfrak{S}_G$ comme groupe de bijections de $G$ par les multiplications à gauche $L_g : G \to G$, $x \mapsto gx$. C'est celle qui apparaît dans le théorème de Cayley en théorie des groupes finis. La *représentation régulière droite* $R : G \to \mathfrak{S}_G$ est définie par $R_g : G \to G$, $x \mapsto xg^{-1}$. Notez que sans la présence de l'inverse dans cette formule, l'application $R$ serait un anti-morphisme : on aurait $R(gh) = R(h)R(g)$.

(b) La *représentation (linéaire) régulière gauche* du groupe $G$ est la représentation $L : G \to \mathrm{GL}(k^G)$ comme groupe d'automorphismes linéaires de l'espace vectoriel $E = k^G = \oplus_{g\in G} k e_g$ via les morphismes $L_g : E \to E$, $e_h \mapsto e_{gh}$. Ce n'est rien d'autre que la représentation obtenue lorsqu'on étend par linéarité la représentation ensembliste par permutation des vecteurs de base, comme dans (a). Elle est fondamentale en théorie des représentations linéaires de groupes finis. La *représentation régulière droite* est définie par $R : G \to \mathrm{GL}(k^G)$, $R_g(e_h) = e_{hg^{-1}}$.
(c) La *représentation (linéaire) régulière gauche* d'une $k$-algèbre $A$ est le morphisme de $k$-algèbres $L : A \hookrightarrow \mathrm{End}(A)$ défini par les endomorphismes $L_a : A \to A$, $x \mapsto ax$. La *représentation (linéaire) régulière droite* est le morphisme $R : A \hookrightarrow \mathrm{End}(A)$ défini par les endomorphismes $R_a : A \to A$, $x \mapsto xa$. Il est important de noter que les éléments d'une algèbre n'étant pas tous inversibles, on ne peut pas définir $R_a(x) = xa^{-1}$ et on doit donc se contenter d'un anti-morphisme. La fidélité de la représentation régulière gauche montre que toute algèbre de dimension finie est une sous-algèbre d'une algèbre de matrices, puisque $\mathrm{End}(A) \simeq \mathrm{M}_n(k)$ si $\dim(A) = n$.

(3) Commentaire sur les notations. Les lettres $L$ et $R$ pour les représentations sont les initiales de *left* et *right*. Dans la littérature en langue française, l'usage des initiales $G$ et $D$ serait possible mais il est assez rare (et pour un groupe $G$, la lettre $G$ est déjà prise...). La lettre $R$ est aussi utilisée pour l'initiale de *regular* ou *régulière*.

(4) La représentation régulière droite $R : G \to \mathrm{GL}(k^G)$ d'un groupe est isomorphe à la représentation régulière gauche $L : G \to \mathrm{GL}(k^G)$ via l'isomorphisme $\varphi : k^G \to k^G$, $e_h \mapsto e_{h^{-1}}$. Ceci ne signifie par qu'elle soit inutile, puisque $R$ et $L$ commutent et peuvent donc coexister pour donner une représentation du groupe $G \times G$. L'histoire est semblable pour les représentations d'algèbres, mais un peu moins simple (on obtient une représentation de $A \times A^\circ$ où $A^\circ$ est l'*algèbre opposée* de $A$).

**1.3.3 Remarque.** La représentation régulière est utile par exemple pour construire l'algèbre des quaternions (voir section 4). En effet, si on se souvient des relations $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$, on connaît l'action de $i$ et $j$ par multiplication à gauche sur l'algèbre $\mathbb{H}$. En d'autres termes, les images de $i$ et $j$ par $\mathbb{H} \to \mathrm{End}(\mathbb{H}) \simeq \mathrm{M}_4(\mathbb{R})$ sont des matrices explicites. On peut donc définir $\mathbb{H}$ comme la sous-algèbre de $\mathrm{M}_4(\mathbb{R})$ engendrée par ces matrices.

**1.3.4 Endomorphismes semi-simples.** Nous nous contentons ici de rappeler l'énoncé du théorème central sur les endomorphismes semi-simples pour les replacer dans le contexte de l'algèbre linéaire. Ce théorème n'aura pas d'importance pour la suite puisque nous utiliserons exclusivement la caractérisation de la définition 1.1.1. Nous ne donnons pas de preuve, et nous renvoyons à [Tau] § 10.14, [BMP] th. 4.29, [Gou], problèmes du chapitre 4.

**1.3.5 Théorème.** *Soient $k$ un corps parfait, $A$ une $k$-algèbre de dimension finie, $\rho : A \to \mathrm{End}(E)$ une représentation linéaire fidèle de dimension finie, et $a \in A$. Les conditions suivantes sont équivalentes :*

(1) *Tout sous-espace $\rho(a)$-stable de $E$ possède un supplémentaire stable.*

(2) *L'endomorphisme $\rho(a)$ est diagonalisable après passage à une clôture algébrique de $k$.*

(3) *Le polynôme minimal de $a$ est produit de polynômes irréductibles distincts i.e. sans facteur carré.*

D'un certain point de vue, le rôle de $A$ est secondaire. En effet, comme $\rho$ est injectif, on peut identifier $a$ et $\rho(a)$ qui ont d'ailleurs mêmes polynômes minimaux. Alors le théorème donne un résultat sur un élément d'une algèbre de matrices $\mathrm{End}(E)$. D'un autre point de vue, le point (3) montre que la propriété de semi-simplicité de $a$ ne dépend pas de la représentation linéaire fidèle $E$ choisie.

# 2 La décomposition de Jordan-Chevalley

## 2.1 Énoncé et commentaires

Le théorème qui affirme que toute matrice $M \in \mathrm{M}_n(\mathbb{C})$ est somme d'une matrice diagonalisable et d'une matrice nilpotente qui commutent est souvent appelé *décomposition de Dunford* dans l'enseignement français. Les raisons de cette dénomination sont étranges ; si Nelson Dunford a démontré un théorème de ce genre, c'était certainement postérieur aux travaux pionniers de Jordan (vers 1870) et à ceux de Chevalley (vers 1950) qui ont donné sa forme moderne au théorème. La dénomination anglo-saxonne de *décomposition de Jordan-Chevalley* est bien plus fidèle à l'histoire, et le très intéressant article [CEZ] l'explique clairement. Nous utiliserons donc cette dernière terminologie.

Nous allons présenter une version très générale du théorème, valable dans une algèbre de dimension finie quelconque sur un corps parfait. La preuve, due à Chevalley, est basée sur la méthode de Newton d'approximation des solutions d'une équation. Elle présente l'avantage de ne pas nécessiter le calcul des valeurs propres de la matrice ; elle est entièrement effective.

**2.1.1 Théorème.** *Soit $k$ un corps parfait et $A$ une $k$-algèbre de dimension finie. Alors pour tout $a \in A$ il existe un unique couple $(s, n)$ dans $A$ tel que $a = s + n$, $s$ est semi-simple, $n$ est nilpotent, et $sn = ns$. De plus $s$ et $n$ sont des polynômes en $a$, et $\mu_s$ divise $\mu_a$.*

**2.1.2 Remarques.** (1) On a vu au lemme 1.2.3 que si $k$ est algébriquement clos, par exemple si $k = \mathbb{C}$, alors « semi-simple » signifie simplement « diagonalisable ». Le théorème ci-dessus redonne la décomposition $D + N$ habituelle.

(2) Supposons que $k = \mathbb{R}$. Soit $M \in \mathrm{M}_n(\mathbb{R})$. Si on croit à la décomposition $D + N$ sur $\mathbb{C}$, on peut écrire $M = S + N$ avec $S, N \in \mathrm{M}_n(\mathbb{C})$. En prenant les conjuguées complexes, on a alors $\overline{S} + \overline{N} = \overline{M} = M = S + N$. Par unicité des parties diagonalisable et nilpotente, on voit que $\overline{S} = S$ et $\overline{N} = N$, i.e. $S, N \in \mathrm{M}_n(\mathbb{R})$. La matrice $S$ est diagonalisable sur $\mathbb{C}$ donc semi-simple sur $\mathbb{R}$. Ce cas particulier facile se trouve dans [BMP], application 4.32 et il est utile par exemple pour décrire l'image de l'exponentielle matricielle réelle, cf [BMP], exercice 4.17.

On a une version multiplicative de la décomposition de Jordan-Chevalley.

**2.1.3 Théorème.** *Soit $k$ un corps parfait et $A$ une $k$-algèbre de dimension finie. Pour tout $a \in A$ inversible, il existe un unique couple $(s, u)$ dans $A$ tel que $a = su$, $s$ est semi-simple inversible, $u$ est unipotent, et $su = us$. De plus $s$ et $n$ sont des polynômes en $a$, et $\mu_s$ divise $\mu_a$.*

Ce résultat se déduit directement de la décomposition $a = s+n$. On voit que $s = a-n$ est somme d'un inversible et d'un nilpotent qui commutent, il est donc inversible. Posons $u = 1 + s^{-1}n$. Alors $a = su$ et cette décomposition possède les propriétés annoncées.

## 2.2 Démonstration : la méthode de Newton

Ce qui suit est traité dans [RB], problème 3.1 (corrigé en fin d'ouvrage) ou dans [RW], module II.5, § 3.3, prop. 45 (page 268). Ces auteurs se placent dans $\mathrm{M}_n(K)$ avec pour $K$ le corps des complexes ou un corps de caractéristique 0, ce qui n'enlève rien à l'intérêt du développement. Nous adoptons autant que possible des notations proches de [RB].

**2.2.1 Unicité.** Supposons que $a = s + n = s' + n'$. On peut plonger $A$ dans $\mathrm{End}(A)$ par la représentation régulière. En choisissant une base de $A$, on peut identifier $\mathrm{End}(A)$ avec une algèbre de matrices $\mathrm{M}_n(k)$ puis la plonger dans $\mathrm{M}_n(\overline{k})$. Alors $s, s'$ sont diagonalisables. La preuve classique de l'unicité s'applique : on montre que $s$ et $s'$ commutent donc $s - s'$ est diagonalisable, puis que $n$ et $n'$ commutent donc $n' - n$ est nilpotente, et finalement $s - s' = n' - n$ est nulle.

**2.2.2 Idée de la preuve.** Par condition nécessaire, si $s$ est semi-simple son polynôme minimal $\mu_s$ est sans facteur carré. Si de plus $\mu_s$ divise $\mu_a$, l'élément $s$ est annulé par le polynôme $P$ produit des facteurs irréductibles distincts de $\mu_a$, qu'on appelle le *radical* de $\mu_a$. L'idée de la preuve est de construire $s$ comme une racine de l'équation $P(s) = 0$ à l'aide de la méthode d'approximation de Newton, en partant de $a_0 = a$. La situation est particulièrement favorable pour deux raisons :

— le point de départ de l'algorithme $a = s + n$ est très proche de la racine cherchée $s$, puisque les nilpotents sont les infinitésimaux de l'algèbre ;

— comme $k$ est parfait, on a $P' \neq 0$ premier avec $P$ donc $P'(a) \neq 0$.

**2.2.3 La preuve.**

*1. Cadre.* Tous les calculs vont se passer dans $A_0 = k[a] \simeq k[X]/(\mu_a)$, la sous-algèbre engendrée par $a$. Quitte à remplacer $A$ par $A_0$, on suppose donc que $A = A_0$. En particulier $A$ est commutative et engendrée par $a$. On note $\mu = \mu_a$ et $p = \mathrm{car}(k) \geqslant 0$.

*2. Fonction à laquelle on applique l'algorithme.* Soit $P$ le produit des facteurs irréductibles distincts de $\mu$, aussi appelé *radical* de $\mu$. D'un point de vue théorique, on peut écrire $P = P_1 \dots P_s$ si $\mu = P_1^{r_1} \dots P_s^{r_s}$ est la décomposition en produit d'irréductibles de $\mu$. Le calcul est cependant effectif :

— si $p = 0$, ou plus généralement si les multiplicités $r_i$ sont premières à $p$, on a l'expression explicite $P = \mu/(\mu, \mu')$ où le pgcd se calcule par l'algorithme d'Euclide.

— en général, le calcul est effectif grâce à l'algorithme décrit dans 2.3 ci-dessous.

*3. Valeur intiale de l'algorithme : estimation de $P(a)$ et $P'(a)$.* Par construction, il existe un entier $r$ tel que $\mu$ divise $P^r$. On peut prendre $r = \max(r_1, \dots, r_s)$ si on a des informations sur les multiplicités, et en tout cas $r = \deg(\mu)$ convient. En particulier $P(a)^r = 0$ i.e. $\epsilon := P(a)$ est nilpotent d'indice $\leqslant r$. Dans la suite, nous noterons $x = \mathrm{O}(\epsilon^n)$ pour dire qu'un élément $x$ appartient à l'idéal engendré par $\epsilon^n$. Comme $k$ est parfait, les polynômes $P_i$ sont tous à racines simples dans $\overline{k}$. En particulier $\mu$ et $P'$ sont premiers entre eux. En prenant une relation de Bézout, on voit que $P'(a)$ est inversible dans $A$.

*4. La méthode de Newton.* On considère ensuite la suite définie par récurrence :

$$\begin{cases} a_0 = a \\ a_{n+1} = a_n - \frac{P(a_n)}{P'(a_n)}. \end{cases}$$

Montrons par récurrence les trois assertions suivantes :

(i) $a_n$ est bien défini,

(ii) $P(a_n) = \mathrm{O}(\epsilon^{2^n})$,

(iii) $a_n - a = \mathrm{O}(\epsilon)$.

Pour $n = 0$, ces trois propriétés sont évidentes. Pour $n \geqslant 1$, du fait que $a_n = a + \mathrm{O}(\epsilon)$ on déduit que $P'(a_n) = P'(a) + \mathrm{O}(\epsilon)$. Cet élément est somme d'un inversible et d'un nilpotent, il est donc

inversible. Il s'ensuit que $a_{n+1}$ est bien défini ce qui établit (i). Maintenant notons $P(X+Y) = P(X) + YP'(X) + Y^2Q(X,Y)$ où $Q$ est un certain polynôme. On calcule alors

$$P(a_{n+1}) = P\left(a_n - \frac{P(a_n)}{P'(a_n)}\right) = P(a_n) - \frac{P(a_n)}{P'(a_n)}P'(a_n) + \left(\frac{-P(a_n)}{P'(a_n)}\right)^2 Q\left(a_n, \frac{-P(a_n)}{P'(a_n)}\right) = \mathrm{O}(\epsilon^{2^{n+1}})$$

ce qui établit (ii). Enfin $a_{n+1} - a = a_n - \frac{P(a_n)}{P'(a_n)} - a = \mathrm{O}(\epsilon)$ ce qui établit (iii). Ceci conclut la preuve des trois propriétés.

*5. Stationnarité.* Lorsque $n = \lceil \log_2(r) \rceil$, on a $\epsilon^{2^n} = 0$ donc $P(a_n) = 0$ et la suite stationne à $s = a_\infty = a_n$. Cet élément est une racine de $P$ donc semi-simple. De plus, $a - s = a - a_n = \mathrm{O}(\epsilon)$ est nilpotent. On a obtenu la décomposition $a = s + n$ recherchée.

## 2.3 Calcul du radical d'un polynôme sur un corps parfait.

Dans la mise en place de la méthode de Newton, nous avons affirmé que le calcul du radical d'un polynôme à coefficients dans un corps parfait est effectif. Nous présentons un algorithme (tiré de [BCGLLSS], chap. 32, § 3) qui réalise ce calcul dans un corps parfait $k$ où le calcul de la racine $p$-ième dans $k$ est effectif. Par exemple, si $k$ est un corps fini de cardinal $q = p^d$, on a $\mathrm{Fr}^d = \mathrm{Id}_k$ donc la racine $p$-ième est l'itéré $(d-1)$-uple du morphisme de Frobenius. Pour un polynôme à coefficients dans $k$ de dérivée nulle, le calcul de la racine $p$-ième est alors effectif également puisqu'il se fait coefficient par coefficient.

**2.3.1 Lemme.** *L'algorithme* rad *suivant calcule le radical d'un polynôme non nul $P \in k[X]$ :*

*Si* $\deg(P) = 0$ *faire* $R := 1$ *et sortir*
*Si* $P' = 0$ *faire* $R := \mathrm{rad}(P^{1/p})$
*Si* $P' \neq 0$ *faire* $U := P \wedge P'$
$V := P/U$
$n := \deg(P)$
$W := U \wedge V^{n-1}$
$R := V * \mathrm{rad}(U/W)$
*Afficher* $R$.

**Preuve :** Écrivons la décomposition de $P$ en facteurs irréductibles $P = \prod_{i\in I} Q_i^{\alpha_i} = EF$, où $E$ regroupe les facteurs de multiplicités $\alpha_i$ premières à $p$, et $F$ les facteurs de multiplicités $\alpha_i$ multiples de $p$. Appliquons l'algorithme à $P$. Les éventualités $\deg(P) = 0$ ou $P' = 0$ sont faciles. Supposons donc que $P' \neq 0$. Lorsqu'on dérive l'expression $P = EF$, le facteur $F$ a une dérivée nulle et se comporte donc comme une constante. On obtient $P' = E'F$ et $P \wedge P' = (E \wedge E')F$. Le calcul de $E \wedge E'$ est facile : si $Q^\alpha$ est l'un des facteurs qui apparaissent dans $E$, on a $E = Q^\alpha G$ d'où $E' = Q^{\alpha-1}(\alpha Q'G + QG')$. On voit que $Q^{\alpha-1} \mid E'$ mais $Q^\alpha \nmid E'$ car $\alpha \not\equiv 0 \mod p$. Finalement :

$$U = P \wedge P' = \prod_{p\nmid\alpha_i} Q_i^{\alpha_i - 1} \cdot \prod_{p\mid\alpha_i} Q_i^{\alpha_i}.$$

Ensuite $V = P/U = \prod_{p\nmid\alpha_i} Q_i$ donc $V^{n-1} = \prod_{p\nmid\alpha_i} Q_i^{n-1}$. Comme $\alpha_i \leqslant n$ pour tout $i$, on obtient $W = U \wedge V^{n-1} = \prod_{p\nmid\alpha_i} Q_i^{\alpha_i - 1}$ et $U/W = \prod_{p\mid\alpha_i} Q_i^{\alpha_i}$. Ici n'apparaissent plus que les multiplicités multiples de $p$, et $\mathrm{rad}(P) = \mathrm{rad}(V)\,\mathrm{rad}(U/W)$. Comme les degrés de $V$ et $U/W$ sont strictement inférieurs au degré de $P$, l'algorithme se termine. □

## 2.4 Que se passe-t-il sur les corps non parfaits ?

Pour nous, les propriétés importantes des corps parfaits seront les suivantes.

**2.4.1 Lemme.** *Soit $k$ un corps de caractéristique $p > 0$.*

(1) *Si $t \in k$ n'est pas une puissance $p$-ième, le polynôme $X^p - t \in k[X]$ est irréductible.*

(2) *Les conditions suivantes sont équivalentes :*

(a) *$k$ est parfait.*

(b) *tout polynôme $P \in k[X]$ de dérivée nulle est une puissance $p$-ième.*

(c) *tout polynôme $P \in k[X]$ irréductible a une dérivée non nulle.*

(d) *tout polynôme $P \in k[X]$ irréductible a ses racines* simples *dans une clôture algébrique $\overline{k}/k$.*

**Preuve :** (1) Soit $P = X^p - t$ et notons $\alpha$ une racine de $P$ dans une clôture algébrique $\overline{k}$. Soit $Q \in k[X]$ un facteur de $P$, unitaire de degré $i > 0$. Puisque $P = X^p - t = X^p - \alpha^p = (X - \alpha)^p$, on peut écrire $Q = (X - \alpha)^i = X^p - i\alpha X^{i-1} + \dots$. Comme $Q$ est à coefficients dans $k$ et $\alpha \notin k$, on doit avoir $i = 0$ dans $k$, c'est-à-dire $i = p$.

(2) (a) $\Rightarrow$ (b). Soit $P$ tel que $P' = 0$. En écrivant $P = \sum a_i X^i$, on voit que les $a_i$ avec $i$ premier à $p$ sont nuls. Il reste les $a_i$ avec $i = jp$. Si on écrit $a_{jp} = b_j^p$, on obtient $P = (\sum b_j X^j)^p$.

(b) $\Rightarrow$ (c). Un polynôme de dérivée nulle est une puissance $p$-ième donc n'est pas irréductible.

(c) $\Rightarrow$ (d). Soit $P$ irréductible. D'après (c) le polynôme $P'$ est non nul, donc premier avec $P$. Une racine multiple de $P$ dans $\overline{k}$ serait aussi racine de $P'$, donc ne peut exister.

(d) $\Rightarrow$ (a). Si $t \in k$ n'est pas une puissance $p$-ième, d'après (1) le polynôme $P = X^p - t$ est irréductible et possède une racine $p$-uple dans $\overline{k}$. □

**2.4.2 Un contre-exemple.** Sur un corps $k$ non parfait, les problèmes apparaissent pour les endomorphismes dont le polynôme minimal contient des facteurs irréductibles à dérivée nulle. L'exemple typique d'un tel polynôme est $P = X^p - t$ avec un terme constant $t$ qui n'est pas une puissance $p$-ième dans $k$. Si $a$ est un élément d'une algèbre $A$ avec polynôme minimal $\mu_a = P$, il est semi-simple (voir 1.3.5) donc admet une décomposition $s + n$ avec $s = a$ et $n = 0$. Pour obtenir un exemple où la décomposition de Jordan-Chevalley n'existe pas, nous devons supposer que $P^2 \mid \mu_a$, par exemple $\mu_a = P^2$. On peut construire un tel $a$ à l'aide d'une matrice compagnon, ce qui revient à prendre $A = k[X]/(P^2)$ et $a$ égal à la classe de $X$ agissant par multiplication sur $A$. Plaçons-nous dans cette situation. Supposons que l'on puisse écrire $a = s + n$ avec $s$ semi-simple, $n$ nilpotent, et $sn = ns$. On note que les éléments nilpotents de l'algèbre $A$ sont les multiples de $P(a)$, et ils sont tous de carré nul puisque $P(a)^2 = 0$. Comme $n^2 = 0$, on a :

$$0 = \mu_a(a) = \mu_a(s + n) = \mu_a(s) + n\mu_a'(s).$$

Il en découle que $\mu_a(s) = -n\mu_a'(s)$ est nilpotent, donc $\mu_a^2(s) = P^4(s) = 0$. On en déduit que $\mu_s | P^4$. Comme $s$ est semi-simple, on trouve $\mu_s = P$ donc $P(s) = s^p - t = 0$. Alors $a^p = s^p + n^p = s^p = t$ donc $P$ annule $a$, ce qui est impossible.

# 3 L'exponentielle dans une algèbre de dimension finie

## 3.1 Définition et premières propriétés

Soit $k$ l'un des corps $\mathbb{R}$ ou $\mathbb{C}$ (l'hypothèse utile est d'avoir un corps normé complet, par exemple le corps des nombres $p$-adiques $\mathbb{Q}_p$ conviendrait). Soit $A$ une $k$-algèbre (associative et unitaire) de dimension finie. Pour tout choix d'une norme de $k$-espace vectoriel $\|\cdot\|$ sur $A$, la formule

$$N(a) = \sup_{\|x\|=1} \|ax\|$$

définit une norme d'algèbre, i.e. une norme d'espace vectoriel sous-multiplicative. Il s'ensuit que pour tout $x \in A$ et tout entier $N$, on a l'inégalité :

$$\sum_{n=0}^{N} \left\| \frac{1}{n!} x^n \right\| \leqslant \sum_{n=0}^{N} \frac{1}{n!} \|x\|^n \leqslant e^{\|x\|},$$

donc la série $\sum_{n\geqslant 0} \frac{1}{n!} x^n$ est normalement convergente.

**3.1.1 Définition.** Pour $x \in A$, on appelle *exponentielle de $x$ dans $A$* et on note $\exp_A(x)$ la somme de la série $\sum_{n\geqslant 0} \frac{1}{n!} x^n$.

**3.1.2 Remarque.** Comme nous sommes en dimension finie, le sous-espace vectoriel $k[x]$ des polynômes en $x$ est fermé. Il s'ensuit que $\exp_A(x)$, qui est la limite de la suite $\sum_{n=0}^{N} \frac{1}{n!} x^n$ d'éléments de $k[x]$, est un élement de $k[x]$. Autrement dit $\exp_A(x)$ est un polynôme en $x$.

**3.1.3 Proposition.** *Soit $f : A \to B$ un morphisme de $k$-algèbres. Alors, pour tout $x \in A$, on a $f(\exp_A(x)) = \exp_B(f(x))$.*

**Preuve :** Comme $f$ est un morphisme, on a $f(\sum_{n=0}^{N} \frac{1}{n!} x^n) = \sum_{n=0}^{N} \frac{1}{n!} f(x)^n$. Or $f$ est une application linéaire entre deux espaces vectoriels de dimension finie, elle est donc continue. En passant à la limite sur $N$, on obtient l'égalité désirée. □

**3.1.4 Remarque.** En utilisant la représentation régulière (gauche) $A \hookrightarrow \mathrm{End}_k(A) \simeq \mathrm{M}_n(k)$ où $n = \dim(A)$, d'après la proposition on aura :

$$\exp_A = \exp_{\mathrm{End}_k(A)|A}.$$

Ceci montre que si on le souhaite, on peut toujours se placer dans une algèbre de matrices pour calculer une exponentielle. En fait, souvent c'est la démarche contraire qui sera payante : on sera dans une algèbre de matrices et on calculera l'exponentielle dans une algèbre plus petite. C'est exactement la même chose que ce qui se passe avec les groupes finis, qui peuvent tous être plongés dans un groupe symétrique via le théorème de Cauchy, ce que l'on fait rarement en pratique.

**3.1.5 Exemple.** (1) Soit $A$ une $\mathbb{R}$-algèbre de dimension finie et $I \in A$ tel que $I^2 = -1$. (Ici $1 = 1_A$ est le neutre multiplicatif de l'algèbre). Alors le polynôme minimal de $I$ sur $\mathbb{R}$ est $X^2 + 1$, et le morphisme de $k$-algèbres $f_0 : \mathbb{R}[X] \to A$ défini par $f_0(X) = I$ se factorise en un morphisme

$f : \mathbb{R}[X]/(X^2+1) \simeq \mathbb{C} \to A$. Dit d'une autre manière, la sous-$\mathbb{R}$-algèbre de $A$ engendrée par $I$ est $\mathbb{R} \oplus \mathbb{R}I$, isomorphe à $\mathbb{C}$. En on déduit que pour tout $t \in \mathbb{R}$ :

$$\exp_A(tI) = \exp_A(f(ti)) = f(\exp_{\mathbb{C}}(ti)) = f(\cos(t) + i\sin(t)) = \cos(t) + I\sin(t)$$

où l'on a noté $\cos(t)$ au lieu de $\cos(t)1$.

(2) On peut prendre $A = \mathrm{M}_2(\mathbb{R})$ et $I = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ (ou son opposée). Le résultat s'écrit :

$$\exp\begin{pmatrix} 0 & -t \\ t & 0 \end{pmatrix} = \begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix}.$$

C'est la fameuse matrice de rotation $R_t$, qui est donc une exponentielle. Ce calcul est parfois fait « à la main » dans les livres, en calculant les puissances de $tI$, en regroupant les puissances paires et en reconnaissant la série du cosinus, etc. Bien sûr c'est plus lourd, mais surtout cela revient à refaire le calcul de $\exp(it)$ dans $\mathbb{C}$ !

(3) On peut prendre $A = \mathbb{H}$ et $I = r \in \mathbb{H}$ un quaternion imaginaire pur de norme 1. En effet, si $r$ est imaginaire pur, on a $\overline{r} = -r$ et s'il est de norme 1, on a $r\overline{r} = 1$. On en déduit que $r^2 = -1$. Pour un quaternion quelconque $q \in \mathbb{H}$, notons $a \in \mathbb{R}$ sa partie réelle et $t$ la norme de $q - a$. On obtient $q = a + tr$ avec $r$ imaginaire pur de norme 1, donc $\exp(q) = \exp(a + rt) = e^a(\cos(t) + r\sin(t))$.

(4) On tire de ce calcul un exemple de deux matrices qui ne commutent pas et telles que $\exp(A+B) \neq \exp(A)\exp(B)$. Prenons $A = \left(\begin{smallmatrix} 0 & -t \\ 0 & 0 \end{smallmatrix}\right)$ et $B = \left(\begin{smallmatrix} 0 & 0 \\ t & 0 \end{smallmatrix}\right)$ qui sont deux matrices de carré nul. On a :

$$\exp(A+B) = \exp(tI) = \cos(t) + I\sin(t) \;\neq\; \exp(A)\exp(B) = (1+A)(1+B) = 1 + A + B + AB.$$

Ceci étant dit, dès que $A$ et $B$ sont deux matrices de carré nul qui ne commutent pas, on voit que $\exp(A)\exp(B) \neq \exp(B)\exp(A)$ qui ne peut donc être égal à $\exp(A+B)$.

**3.1.6 Théorème.** *Soit $k = \mathbb{R}$ ou $\mathbb{C}$ et $A$ une $k$-algèbre de dimension finie. Soit $a = s + n$ la décomposition de Jordan-Chevalley additive de $a$. Alors $\exp(a) = \exp(s)\exp(n)$ est la décomposition de Jordan-Chevalley multiplicative de $\exp(a)$.*

**Preuve :** Utilisons la représentation régulière pour plonger $A$ dans l'algèbre d'endomorphismes $\mathrm{End}_k(A)$, et utilisons une une $k$-base $e_1, \ldots, e_n$ de $A$ pour identifier celle-ci à une algèbre de matrices. On a donc $A \hookrightarrow \mathrm{M}_n(k) \subset \mathrm{M}_n(\mathbb{C})$. Comme $s$ est semi-simple, vu dans $\mathrm{M}_n(\mathbb{C})$ il est diagonalisable. Notons $s = PDP^{-1}$ avec $P \in \mathrm{GL}_n(\mathbb{C})$ et $D \in \mathrm{M}_n(\mathbb{C})$ diagonale. On a alors $\exp(s) = P\exp(D)P^{-1}$, où $\exp(D)$ est diagonale. Ainsi $\exp(s)$ est diagonalisable dans $\mathrm{M}_n(\mathbb{C})$ donc semi-simple dans $A$. De plus $\exp(n) = 1 + n + \ldots$ est unipotent. Enfin $s$ et $n$ sont des polynômes en $a$, donc aussi $\exp(s)$ et $\exp(n)$ (voir remarque 3.1.2), ce qui montre qu'ils commutent. Le résultat en découle par unicité de la décomposition de Jordan-Chevalley. □

## 3.2 L'exponentielle des endomorphismes nilpotents

Soit $A$ une algèbre de dimension finie sur un corps $k$ de caractéristique 0. Si $x \in A$ est nilpotent, on peut définir son exponentielle $\exp_A(x) = \sum_{n \geqslant 0} \frac{1}{n!}x^n$ sans hypothèse sur $k$ puisque cette série est un polynôme. De même, si $u \in A$ est unipotent, on peut définir son logarithme par la formule $\log_A(u) = \sum_{n \geqslant 1} \frac{(-1)^{n+1}}{n}(u-1)^n$, puisque $u-1$ est nilpotent. Ces deux applications sont en fait inverses l'une de l'autre, comme le montre le résultat suivant. Une référence est [MT], 3.3.3, p. 60, mais nous n'en suivons pas vraiment la preuve.

**3.2.1 Théorème.** *Soit $A = \mathrm{M}_n(k)$ l'algèbre des matrices sur un corps de caractéristique 0 ou $p > n$. Alors on a des bijections réciproques*

$$\{\textit{éléments nilpotents de } A\} \underset{\log_A}{\overset{\exp_A}{\rightleftarrows}} \{\textit{éléments unipotents de } A\}$$

*Si $k$ égale $\mathbb{R}$ ou $\mathbb{C}$, ces bijections sont des homéomorphismes.*

**3.2.2 Remarque.** Si $k$ égale $\mathbb{R}$ ou $\mathbb{C}$, les bijections $\exp_A$ et $\log_A$ sont données par des expressions polynomiales, donc on pourrait avoir le désir d'annoncer une régularité bien meilleure que celle d'un simple homéomorphisme. Malheureusement, ce n'est pas possible car les ensembles source et but n'ont pas de structure différentiable. Par exemple, on peut vérifier en exercice que l'ensemble des matrices nilpotentes de taille $(2,2)$ s'identifie au sous-ensemble de $k^3$ d'équation $a^2 + bc = 0$. Il s'agit d'une variété algébrique *non différentiable* qui présente une singularité en $(0,0,0)$.

**Preuve :** Si $x$ est nilpotent, $\exp(x) = 1 + x + \dots$ est unipotent. Réciproquement si $u$ est unipotent, $\log(u) = (u-1) - \frac{1}{2}(u-1)^2 + \dots$ est nilpotent. Il reste à montrer que log et exp sont inverses l'une de l'autre. Partons de l'égalité de séries formelles $\log(\exp(X)) = X$, valable dans $\mathbb{Q}[[X]]$. En regardant cela modulo $X^n$, on obtient l'égalité analogue dans l'anneau quotient $\mathbb{Q}[[X]]/(X^n) \simeq \mathbb{Q}[X]/(X^n)$. On constate alors que les seuls dénominateurs qui interviennent ont des facteurs premiers $\leqslant n-1$. Donc, cette dernière égalité est valable dans le sous-anneau $\mathbb{Z}[\frac{1}{(n-1)!}][X]/(X^n)$. Si $k$ est de caractéristique 0, on peut spécialiser $X$ en un élément nilpotent de $A$ dans l'identité $\log(\exp(X)) = X$. Si $k$ est de caractéristique $p > n$, comme $p$ ne divise pas $(n-1)!$ on peut réduire modulo $p$ pour obtenir l'identité dans $\mathbb{F}_p[X]/(X^n)$ puis la plonger dans $k[X]/(X^n)$. (On notera que $\mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}[\frac{1}{(n-1)!}]/p\mathbb{Z}[\frac{1}{(n-1)!}]$ d'après l'exercice 3.2.3 ci-dessous.) Comme précédemment, on spécialise ensuite $X$ en un élément nilpotent de $A$. On procède de la même manière pour démontrer que $\exp(\log(U)) = U$ vue comme égalité de séries formelles dans $\mathbb{Q}[[X]]$ où $X = U - 1$. □

**3.2.3 Exercice.** Soient $a, b$ deux entiers naturels premier entre eux. On note $u$ le morphisme d'anneaux obtenu en composant l'inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[\frac{1}{a}]$ et le morphisme de quotient $\mathbb{Z}[\frac{1}{a}] \to \mathbb{Z}[\frac{1}{a}]/b\mathbb{Z}[\frac{1}{a}]$. Montrez que $\ker(u) = b\mathbb{Z}$ et que $u$ induit un isomorphisme $\mathbb{Z}/b\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}[\frac{1}{a}]/b\mathbb{Z}[\frac{1}{a}]$.

## 3.3 L'exponentielle des groupes de Lie

Les groupes de Lie sont un sujet d'étude très riche, au croisement de plusieurs disciplines (algèbre, analyse, topologie, physique, théorie des groupes, théorie des nombres...). Pour l'agrégation, les références sont [MT] et [Fa]. On renvoie aussi aux compléments de cours de Géométrie Différentielle faits par Jürgen Angst début octobre.

**3.3.1 Définition.** On appelle *groupe de Lie linéaire* un sous-groupe fermé de $\mathrm{GL}_n(\mathbb{R})$.

On pourrait aussi considérer les sous-groupes fermés de $\mathrm{GL}_n(\mathbb{C})$, mais comme ce dernier est un sous-groupe fermé de $\mathrm{GL}_{2n}(\mathbb{R})$ cela n'ajouterait pas de généralité. Un point essentiel de la théorie est le théorème de Cartan-von Neumann ([MT] p. 68 et théorème 3.4.3 p. 66) qui affirme que tout sous-groupe fermé non discret de $\mathrm{GL}_n(\mathbb{R})$ est une sous-variété. Dans notre contexte, ce résultat est important également parce que sa preuve utilise l'exponentielle que nous allons définir ci-dessous.

Cependant, on n'insiste pas ici sur ces points ; à l'agrégation, l'intérêt des groupes de Lie résulte surtout dans l'étude d'exemples explicites comme $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{SL}_n(\mathbb{R})$, $\mathrm{O}_n(\mathbb{R})$, $\mathrm{SO}_n(\mathbb{R})$, $\mathrm{Sp}_n(\mathbb{R})$, $\mathrm{U}_n(\mathbb{C})$, ou éventuellement le groupe des quaternions de norme 1.

**3.3.2 Définition.** Soit $G \subset \mathrm{GL}_n(\mathbb{R})$ un groupe de Lie linéaire. On appelle *algèbre de Lie de* $G$ et on note $\mathrm{Lie}(G)$ l'ensemble $\mathfrak{g} = \{X \in \mathrm{M}_n(\mathbb{R}) \text{ t.q. } \exp(tX) \in G \text{ pour tout } t \in \mathbb{R}\}$.

Si on sait qu'un groupe de Lie linéaire est une sous-variété de $\mathrm{GL}_n(\mathbb{R})$, on peut aussi définir son algèbre de Lie comme l'espace tangent en l'élément identité. Cette définition montre en particulier que $\mathrm{Lie}(G)$ ne dépend que d'un voisinage de l'identité dans $G$ ; par exemple $\mathrm{Lie}\,\mathrm{O}_n(\mathbb{R}) = \mathrm{Lie}\,\mathrm{SO}_n(\mathbb{R})$.

**3.3.3 Exemples.** (1) Si $G = \mathrm{GL}_n(\mathbb{R})$ alors $\mathfrak{g} = \mathfrak{gl}_n(\mathbb{R}) := \mathrm{M}_n(\mathbb{R})$ (évident).

(2) Si $G = \mathrm{SL}_n(\mathbb{R})$ alors $\mathfrak{g} = \mathfrak{sl}_n(\mathbb{R})$ est l'ensemble des matrices de trace nulle. En effet, grâce à la formule $\det(\exp(M)) = \exp(\mathrm{tr}(M))$, l'identité $\det(\exp(tX)) = 1$ pour tout $t$ donne, à l'ordre 1, la condition $\mathrm{tr}(X) = 0$.

(3) Si $G = \mathrm{SO}_n(\mathbb{R})$ alors $\mathfrak{g} = \mathfrak{so}_n(\mathbb{R})$ est l'ensemble des matrices antisymétriques. En effet, l'identité $\exp(tX)\exp(tX^*) = \mathrm{Id}$ implique que $\exp(tX)$ et $\exp(tX^*)$ commutent donc $\exp(tX + tX^*) = \mathrm{Id}$ d'où, à l'ordre 1, la condition $X + X^* = 0$.

Sur ces exemples, on constate que $\mathrm{Lie}(G)$ est un $\mathbb{R}$-espace vectoriel stable par le crochet de Lie $[X, Y] := XY - YX$. C'est vrai en général et c'est un calcul assez facile pour lequel on renvoie à [MT], 3.4.1 ou [Fa], III.2.1 et II.2.4. Nous arrivons à cinq résultats importants concernant nos exemples.

**3.3.4 Théorème.** *L'application* $\exp : \mathfrak{gl}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ *est surjective.*

Ce résultat fondamental se trouve dans [Gou], problèmes du chap. 4, ou [BMP], exercice 4.17.

**Preuve :** Soit $M \in \mathrm{GL}_n(\mathbb{C})$ et $M = DU$ sa décomposition de Jordan-Chevalley multiplicative. D'après le théorème 3.2.1, il existe $N \in \mathrm{M}_n(\mathbb{C})$ telle que $\exp(N) = U$. De plus, l'expression explicite $N = \log(U)$ montre que $N$ est un polynôme en $U$ donc un polynôme en $M$. Notons $D = P^{-1}\,\mathrm{diag}(\lambda_1, \ldots, \lambda_n)P$ la partie diagonalisable. Comme $D$ est inversible, les $\lambda_i$ sont non nuls et la surjectivité de l'exponentielle complexe montre qu'il existe $\mu_i$ tel que $\exp(\mu_i) = \lambda_i$. Choisissons un polynôme d'interpolation $F$ tel que $F(\lambda_i) = \mu_i$ pour tout $i$. On a alors $D' := F(D) = P^{-1}\,\mathrm{diag}(\mu_1, \ldots, \mu_n)P$ est un polynôme en $D$, donc un polynôme en $M$, qui vérifie $\exp(D') = D$. Finalement $D'$ et $N$ sont des polynômes en $M$ donc elles commutent entre elles, et $\exp(D' + N) = \exp(D')\exp(N) = DU = M$. □

**3.3.5 Théorème.** *L'application* $\exp : \mathfrak{so}_n(\mathbb{R}) \to \mathrm{SO}_n(\mathbb{R})$ *est surjective.*

Ce résultat n'est pas vraiment énoncé dans [MT] même s'il est dans l'air ([MT], 2.6.4 montre que $\mathrm{SO}_n(\mathbb{R})$ est connexe en utilisant la réduction des endomorphismes orthogonaux comme nous le ferons ci-dessous, et [MT] 3.4.3.2 calcule l'algèbre de Lie $\mathfrak{so}_n(\mathbb{R})$).

**Preuve :** Soit $M \in \mathrm{SO}_n(\mathbb{R})$. Notons

$$R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

la matrice de rotation. On sait que c'est l'exponentielle de $\theta I$ où

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathfrak{so}_2(\mathbb{R}).$$

D'après le théorème de réduction des matrices orthogonales, il existe $P \in \mathrm{O}_n(\mathbb{R})$ telle que

$$PMP^{-1} = \mathrm{diag}(\mathrm{Id}_r, R_{\theta_1}, \ldots, R_{\theta_s}).$$

C'est donc l'exponentielle de la matrice diagonale par blocs antisymétrique :

$$Q = \mathrm{diag}(0_r, \theta_1 I, \ldots, \theta_s I).$$

Comme l'exponentielle respecte la conjugaison, $M$ est donc l'exponentielle de la matrice $P^{-1}QP$. Comme $P$ est orthogonale, il est immédiat de vérifier que cette matrice est encore antisymétrique. □

**3.3.6 Corollaire.** *Les groupes de Lie* $\mathrm{GL}_n(\mathbb{C})$ *et* $\mathrm{SO}_n(\mathbb{R})$ *sont connexes par arcs.*

Ceci se déduit immédiatement de 3.3.4 et 3.3.5 puisque les espaces vectoriels $\mathfrak{gl}_n(\mathbb{C})$ et $\mathfrak{so}_n(\mathbb{R})$ sont connexes par arcs et exp est une application continue.

**3.3.7 Théorème.** *L'application* $\exp : \mathfrak{gl}_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})$ *n'est pas surjective.*

Ce résultat est clair, car $\det(\exp(M)) = \exp(\mathrm{tr}(M)) > 0$ donne l'inclusion $\exp(\mathfrak{gl}_n(\mathbb{R})) \subset \mathrm{GL}_n^+(\mathbb{R})$. On peut préciser en montrant que les matrices qui sont dans l'image de l'exponentielle sont celles qui sont le carré d'une autre matrice, voir [BMP], exercice 4.17.

**3.3.8 Théorème.** *L'application* $\exp : \mathfrak{sl}_n(\mathbb{C}) \to \mathrm{SL}_n(\mathbb{C})$ *n'est pas surjective.*

Ce résultat peut être démontré avec les outils dont nous disposons (notamment la décomposition de Jordan-Chevalley) mais nous n'en dirons pas plus ici. Nous renvoyons à la note [Ro].

# 4 L'algèbre $\mathbb{H}$ des quaternions de Hamilton

Cette section donne la construction et les propriétés de base de l'algèbre des quaternions. Le livre de Perrin [Per] est une excellente référence. Attention : le contenu de la sous-section 4.2 est assez exotique et sa lecture est déconseillée. L'auteur s'est amusé à décrire les sous-algèbres de $\mathbb{H}$ et ne s'est pas astreint à écrire des choses directement utiles pour l'agrégation.

## 4.1 Définition et premières propriétés

**4.1.1 Construction 1.** Pour définir l'algèbre des quaternions $\mathbb{H}$, on fixe un $\mathbb{R}$-espace vectoriel de dimension 4 et une base que l'on note $\{1, i, j, k\}$, donc $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$. On définit une application $\mathbb{R}$-bilinéaire $\mathbb{H} \times \mathbb{H} \to \mathbb{H}$ pour laquelle 1 est élément neutre, en posant :

$$i^2 = j^2 = k^2 = -1 \quad ; \quad ij = -ji = k \quad ; \quad ik = -ki = -j \quad ; \quad jk = -kj = i \ ,$$

et en étendant à $\mathbb{H} \times \mathbb{H}$ par bilinéarité. On peut vérifier, mais c'est un peu fastidieux, que cette multiplication munit $\mathbb{H}$ d'une structure de $\mathbb{R}$-algèbre associative.

**4.1.2 Exercice.** Montrez que les relations qui définissent le produit dans $\mathbb{H}$ sont équivalentes aux relations (plus sympathiques du point de vue mnémotechnique) : $i^2 = j^2 = k^2 = ijk = -1$.

**4.1.3 Construction 2.** On a signalé en 1.3.3 une autre manière de procéder : on peut définir $\mathbb{H}$ comme la sous-$\mathbb{R}$-algèbre de $\mathrm{M}_4(\mathbb{R})$ engendrée par les matrices

$$i = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{et} \quad j = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} .$$

On pose $k = ij$. L'associativité est alors automatique, mais on doit montrer que $\mathbb{H}$ a pour base $\{1, i, j, k\}$ car la sous-$\mathbb{R}$-algèbre engendré pourrait a piori être de dimension $> 4$. Ceci n'est pas très difficile, si lors des calculs de produits on veille à bien exploiter le fait que les matrices n'ont qu'un coefficient non nul par ligne et par colonne.

**4.1.4 Quaternions réels et imaginaires purs. Centre.** Le sous-espace vectoriel de $\mathbb{H}$ engendré par 1 est noté simplement $\mathbb{R}$ ; c'est une sous-algèbre. Le sous-espace vectoriel de $\mathbb{H}$ engendré par $i, j, k$ est noté $P$ ; il n'est pas stable par multiplication. Un quaternion de $\mathbb{R}$ est dit *réel* et un quaternion de $P$ est dit *imaginaire pur*. On a évidemment $\mathbb{H} = \mathbb{R} \oplus P$ donc on peut parler de la *partie réelle* et de la *partie imaginaire* d'un quaternion.

L'algèbre $\mathbb{H}$ n'est pas commutative. Son centre $Z(\mathbb{H})$, défini comme la sous-algèbre des éléments $q \in \mathbb{H}$ qui commutent avec tous les éléments de $\mathbb{H}$, est la sous-algèbre $\mathbb{R}$ des quaternions réels. Ceci se voit en écrivant qu'un quaternion $q = a + bi + cj + dk$ commute à tous les éléments de $\mathbb{H}$ si et seulement s'il commute avec $i$, $j$ et $k$.

**4.1.5 Conjugaison et norme.** Il y a sur $\mathbb{H}$ une *conjugaison* qui est définie ainsi : si $q = a+bi+cj+dk$ alors son conjugué est $\overline{q} = a - bi - cj - dk$. Bien sûr on a $\overline{\overline{q}} = q$. De plus, on vérifie aisément que la conjugaison est un anti-automorphisme, c'est-à-dire que c'est un automorphisme d'espace vectoriel et que $\overline{q_1 q_2} = \overline{q_2}\,\overline{q_1}$.

On définit ensuite la *norme* d'un quaternion $q \in \mathbb{H}$ par $N(q) = q\overline{q}$. On vérifie que si $q = a+bi+cj+dk$ alors $N(q) = a^2+b^2+c^2+d^2$. On en déduit que $N(q) \in \mathbb{R}$ et $N(\overline{q}) = N(q)$. Notez que l'application $N : \mathbb{H} \to \mathbb{R}$ est une forme quadratique, en particulier *ce n'est pas* une norme d'espace vectoriel puisque pour $\lambda \in \mathbb{R}$ on a $N(\lambda q) = \lambda^2 N(q)$, et non pas $N(\lambda q) = |\lambda| N(q)$.

On voit aussi que $N(q) = 0$ si et seulement si $q = 0$. Il s'ensuit que si $q \neq 0$, alors $N(q)^{-1}\overline{q}$ est inverse à gauche et à droite pour $q$. Donc $\mathbb{H}$ est ce que l'on appelle une *algèbre à division*, ou *corps gauche*, c'est-à-dire un anneau dans lequel tout élément non nul est inversible.

Enfin on a $N(q_1q_2) = q_1q_2\overline{q_1q_2} = q_1q_2\overline{q}_2\overline{q}_1 = q_1N(q_2)q_1 = N(q_1)N(q_2)$ puisque $N(q_2)$ est central. L'application $N : \mathbb{H} \to \mathbb{R}$ est donc multiplicative et elle induit un morphisme de groupes $\mathbb{H}^* \to \mathbb{R}^*$ qui est surjectif. On note $G$ son noyau, le groupe des *quaternions de norme 1.*

**4.1.6 Caractérisations de $\mathbb{R}$ et $P$.** On dispose des caractérisations utiles suivantes :

(i) $q \in \mathbb{R} \iff \overline{q} = q \iff q^2 \in \mathbb{R}_{\geqslant 0}$.

(ii) $q \in P \iff \overline{q} = -q \iff q^2 \in \mathbb{R}_{\leqslant 0}$.

(Noter que la relation d'ordre total de $\mathbb{R}$ ne s'étend pas à $\mathbb{H}$ en un ordre compatible aux structures d'algèbre ; on évite donc d'écrire des choses comme $q \geqslant 0$.) Démontrons que $\overline{q} = q \iff q^2 \in \mathbb{R}_{\geqslant 0}$. Si $q = \overline{q}$, en multipliant par $q$ on obtient $q^2 = q\overline{q} = N(q) \in \mathbb{R}_{\geqslant 0}$. Réciproquement si $q^2 = \lambda \in \mathbb{R}_{\geqslant 0}$, en prenant les normes on trouve $\lambda^2 = N(q)^2$ d'où $\lambda = N(q)$ puis $q^2 = N(q) = q\overline{q}$. On en déduit que $q = \overline{q}$ (traiter à part le cas $q = 0$, et diviser par $q$ lorsque $q \neq 0$). La preuve des autres équivalences est similaire ou plus simple ; nous la laissons en exercice.

**4.1.7 L'équation $X^2 + 1 = 0$.** Cherchons les racines du polynôme $X^2 + 1$ c'est-à-dire les $q \in \mathbb{H}$ tels que $q^2 = -1$. On rappelle que $G$ désigne le sous-groupe de $\mathbb{H}^*$ formé des quaternions de norme 1. On a $q^2 = -1$ ssi on a simultanément $q^2 \in \mathbb{R}_{\leqslant 0}$ et $q \in G$. D'après ce que l'on a dit plus haut, cela veut donc dire que $q \in P \cap G$. L'espace vectoriel euclidien $P$ est de dimension 3 et $S := P \cap G$ est sa sphère unité. Ainsi l'équation $X^2 + 1 = 0$ possède dans $\mathbb{H}$ un ensemble de solutions en bijection avec la sphère $S^2$.

Rappelons le fait bien connu que les racines des polynômes en une variable à coefficients dans un corps *commutatif* sont en nombre fini, inférieur ou égal au degré. Il est remarquable que c'est très loin d'être le cas pour l'équation $X^2 + 1 = 0$ dans $\mathbb{H}$. La non-commutativité du corps $\mathbb{H}$ a pour conséquence que de nombreux résultats de la théorie des corps commutatifs ne sont plus valables !

## 4.2 Sous-algèbres de $\mathbb{H}$

**4.2.1 Formes polaires.** Tout quaternion non nul peut s'écrire $q = tp$ où $t = N(q) \in \mathbb{R}_{>0}$ et $p \in G$. Cette écriture peut être appelée la *forme polaire* de $q$, en analogie avec le cas complexe.

Tout quaternion non réel peut se décomposer en partie réelle et partie imaginaire $q = r + q'$, avec $r \in \mathbb{R}$ et $q' \in P$ non nul. En considérant la forme polaire $q' = tp$ on obtient $q = r + tp$ avec $r \in \mathbb{R}$, $p \in P \cap G$, et $t = N(q - r) \in \mathbb{R}_{>0}$.

**4.2.2 Sous-algèbres monogènes.** Soit $q \in \mathbb{H}$. Si $q \in \mathbb{R}$, son polynôme minimal sur $\mathbb{R}$ est $X - q$ et ce cas est peu intéressant. Supposons maintenant que $q \notin \mathbb{R}$.

Notons $n = N(q) = q\overline{q}$ et $t = q + \overline{q}$ la norme et la trace de $q$. Ce sont deux nombres réels. Alors $q$ est racine du polynôme à coefficients réels $X^2 - tX + n$ car celui-ci n'est rien d'autre que $(X - q)(X - \overline{q})$. (On se méfie des polynômes à coefficients dans un corps non commutatif, mais ce qui précède est tout de même vrai, par exemple parce que $q$ et $\overline{q}$ commutent.) On voit donc que $q \in \mathbb{H} \smallsetminus \mathbb{R}$ est algébrique de degré 2 sur $\mathbb{R}$. La sous-algèbre $\mathbb{R}[q] \subset \mathbb{H}$ est de dimension 2 sur $\mathbb{R}$.

On peut retrouver ce fait par un autre argument. Écrivons une forme polaire $q = r + tp$ avec $r \in \mathbb{R}$, $p \in P \cap G$, et $t = N(q - r) \in \mathbb{R}_{>0}$, comme au point précédent. Puisque $p = t^{-1}(q - r) \in \mathbb{R}[q]$ et $q = r + tp \in \mathbb{R}[p]$, on a $\mathbb{R}[q] = \mathbb{R}[p]$. Comme $p \in P \cap G$ est un élément de carré $-1$ (voir 4.1.7), on peut construire un isomorphisme $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1) \xrightarrow{\sim} \mathbb{R}[p]$ en envoyant $i$ sur $p$. On a montré que $\mathbb{R}[q]$ est isomorphe au corps des complexes.

Ceci montre que n'importe quel sous-$\mathbb{R}$-espace vectoriel $E \subset \mathbb{H}$ contenant $\mathbb{R}$ et de dimension 2 est une sous-algèbre, c'est-à-dire est stable par multiplication. En effet, un tel sous-espace est égal à $\mathbb{R}[q]$, pour n'importe quel choix de $q \in E \smallsetminus \mathbb{R}$. Comme les plans $E \subset \mathbb{H}$ contenant $\mathbb{R}$ sont en bijection avec les droites de l'espace vectoriel quotient $\mathbb{H}/\mathbb{R}$, on voit que l'ensemble des l'ensemble des sous-algèbres de dimension 2 est en bijection avec l'espace projectif $\mathbb{P}(\mathbb{H}/\mathbb{R})$. Puisque $\dim(\mathbb{H}/\mathbb{R}) = 3$, il s'agit d'un plan projectif.

Enfin, on peut observer que la $\mathbb{R}$-algèbre $\mathbb{H}$ elle-même n'est pas monogène. Ceci est à comparer au fait que toute extension finie de corps commutatifs de caractéristique 0 (ou plus généralement toute extension finie séparable) est monogène, d'après le théorème de l'élément primitif. C'est donc une nouvelle subtilité de la théorie des corps non commutatifs.

**4.2.3 Sous-algèbres de $\mathbb{H}$.** Soit $A$ une sous-$\mathbb{R}$-algèbre de $\mathbb{H}$. Sa dimension appartient à $\{1, \dots, 4\}$. Si $\dim A = 1$ on a $A = \mathbb{R}$. Si $\dim A \geqslant 2$, il existe un quaternion non réel $q \in A$, et on a vu que $\mathbb{R}[q]$ est isomorphe à $\mathbb{C}$. L'inclusion $\mathbb{C} \simeq \mathbb{R}[q] \hookrightarrow A$ munit $A$ d'une structure de $\mathbb{C}$-algèbre. En particulier $A$ est un $\mathbb{C}$-espace vectoriel, et sa dimension réelle est nécessairement paire. Si $\dim A = 2$, on a $A = \mathbb{R}[q]$, et si $\dim A = 4$ on a $A = \mathbb{H}$. En résumé on a obtenu une description de toutes les sous-algèbres de $\mathbb{H}$ :

(i) dimension 1 : la sous-algèbre $\mathbb{R}$.

(ii) dimension 2 : ces sous-algèbres sont toutes isomorphes à $\mathbb{C}$ et sont paramétrées par le plan projectif $\mathbb{P}(\mathbb{H}/\mathbb{R})$.

(iii) dimension 4 : la sous-algèbre $\mathbb{H}$.

# Références


[BCGLLSS] A. Bostan, F. Chyzak, M. Giusti, R. Lebreton, G. Lecerf, B. Salvy, É. Schost, *Algorithmes Efficaces en Calcul Formel*, polycopié de cours disponible à l'adresse `perso.ens-lyon.fr/bruno.salvy/mpri/poly.pdf`

[BMP] V. Beck, J. Malick, G. Peyré, *Objectif Agrégation*, H & K, 2005.

[CEZ] D. Couty, J. Esterle, R. Zarouf, *Décomposition effective de Jordan-Chevalley*, Gazette des Mathématiciens no 129 (2011), 29–49, disponible à l'adresse `http://smf4.emath.fr/Publications/Gazette/2011/129/smf_gazette_129_29-49.pdf`

[CG2] Ph. Caldero, J. Germoni, *Histoires hédonistes de groupes et de géométries*, tome II, Calvage & Mounet, 2015.

[Fa] J. Faraut, *Analyse sur les groupes de Lie*, Calvage & Mounet, 2006.

[Gou] X. Gourdon, *Algèbre*, Ellipses, 2009.

[Me] J.-Y. Mérindol, *Nombres et algèbre*, EDP Sciences, 2006.

[MT] R. Mneimné, F. Testard, *Introduction à la théorie des groupes de Lie classiques*, Hermann, 1986, réédité en 2005.

[Per] D. Perrin, *Cours d'algèbre*, Ellipses, 1996.

[RB] J.-J. Risler, P. Boyer, *Algèbre pour la Licence 3*, Dunod, 2006.

[Ro] M. Romagny, *L'exponentielle de* $\mathrm{SL}_n(\mathbb{C})$ *n'est pas surjective*, note disponible à l'adresse `https://perso.univ-rennes1.fr/matthieu.romagny/agreg/dvt/exp_non_surjective.pdf`.

[RW] J.-P. Ramis, A. Warusfel, *Mathématiques Tout-en-un L2*, Dunod, 2007.

[Sz] A. Szpirglas, *Algèbre L3*, Pearson, 2009.

[Tau] P. Tauvel, *Algèbre*, Dunod, 2005.