Géométrie des Algèbres de Quaternions Réelles

Christopher-Lloyd Simon

Été 2020

Résumé

Ce document forme le support d'une série d'exposés ayant pour but l'exploration concrète, c'est-à-dire matricielle, des deux algèbres de quaternions réelles, à savoir les quaternions de Hamilton et de Coockle (endomorphismes d'un plan réel). L'objectif est d'en exhiber la richesse géométrique, adéquate à décrire (des espaces modélisant) notre univers physique. En particulier, l'orateur souhaitait convaincre les analystes de son auditoire à s'intéresser aux équations aux dérivées partielles sur ou à valeurs dans des espaces de quaternions. Les algèbres de quaternions sont intimement liées aux groupes SU_2 et SL_2 et ce texte peut également servir d'introduction, sur ces exemples motivés, des notions élémentaires de la théorie des groupes et des algèbres de Lie. Nous profiterons de l'occasion pour faire le lien entre l'identité de Jacobi et l'intersection des hauteurs d'un triangle sphérique ou hyperbolique. L'essentiel de ces notes se veulent accessibles aux non algébristes, voire aux non géomètres ou aux physiciens, en restreignant les pré-requis aux notions d'algèbre bilinéaire ou commutative de niveau Licence, rappelés en introduction et approfondis en appendice.

Table des matières

0 Introduction

Notations. Dans ce document, toutes les matrices seront carrées de taille 2×2, à coefficient entiers ou dans le corps des nombres réels ou complexes. Nous notons ${}^tM$ la transposée, M^* la transconjuguée et $M^\#$ la trancomatrice. Voici des notations pour nos matrices fétiches :

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad K = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \qquad L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Nous fixons le choix d'une racine $\sqrt{\text{-}1} \in \mathbb{C}$ de -1, cette notation évitera toute confusion avec la base i, j, k des quaternions de Hamilton qui pour nous sera définie par $i = I$, $j = \sqrt{\text{-}1}\, J$, $k = \sqrt{\text{-}1}\, K$.

Organisation du texte

Pour aborder sereinement les algèbres matricielles de dimension $4 = 2^2$, nous traitons dans un premier temps celles de dimension $1 = 2^0$ et $2 = 2^1$. Expédions immédiatement en quelques remarques banales le cas de l'unique algèbre matricielle de dimension 1, que nous pouvons réaliser comme $\mathbb{R}[\mathbb{1}]$. Elle admet au signe près, une seule forme quadratique non dégénérée $x.\mathbb{1} \mapsto \det(x\mathbb{1}) = x^2$, ayant pour signature $(1, 0)$. Sa sphère des unités $\mathbb{S}^0 = \{\pm\mathbb{1}\}$ coïncide avec les éléments inversibles de l'anneau des entiers, et forme un groupe, le seul de cardinal 2×2^0.

La section 1 règle le cas des algèbres matricielles de dimension 2. Nous rappelons d'abord la définition du corps des complexes comme extension quadratique des réels, en exhibant l'isomorphisme avec l'algèbre des homothéties et rotations du plan réel qui préserve une forme quadratique de signature $(2, 0)$ et engendrée par une matrice elliptique I. Nous poursuivons avec une autre extension quadratique des réels, isomorphe au produit cartésien $\mathbb{R} \times \mathbb{R}$ donc non intégre, formant une algèbre d'homothéties et rotations hyperboliques du plan préservant une forme quadratique de signature $(1, 1)$. Elle peut être engendrée par une matrice hyperbolique, mais aussi par une réflexion comme J ou K. On termine par un exemple intermédiaire et dégénéré, ou l'algèbre n'est même pas réduite, celle des homothéties et transvections du plan préservant une forme quadratique dégénérée de signature $(1, 0)$. Elle peut être engendrée par une matrice parabolique L, non inversible comme celle d'un projecteur sur un axe, ou même nilpotente. Ces exemples classifient les extensions quadratiques de $\mathbb{R}$, tout en les réalisant par des algèbres de matrices. Cette classification, donné par le signe du discriminant du polynôme caractéristique, reflète la présence de rotations hyperboliques, elliptiques ou paraboliques.

Dans la section 2 nous décorticons la structure de l'algèbre $\mathrm{M}_2(\mathbb{C})$ des matrices complexes, en tant que $\mathbb{R}$-algèbre de dimension 8 muni de trois involutions ${}^t, *, \#$ pour en dégager ses sous algèbres de dimension 4 réelles. Nous définirons en particulier le corps le corps des quaternions de Hamilton comme le lieu $M^* = M^\#$ ainsi que l'algèbre des matrices réelles $\mathrm{M}_2(\mathbb{R})$, initialement découvertes par Coockle sous le nom de « coquaternions », obtenues comme le lieu $M^* = {}^tM$.

Les sections 3 et 4 consistent en une étude géométrique concrète et détaillée des quaternions de Hamilton et des endomorphismes du plan réel. C'est l'objectif et l'aboutissement des exposés.

Bien que ces remarque ne soient pas nécessaires pour comprendre la suite, nous pouvons résumer le caractère systématique de l'approche de la façon suivante. Nous aurons à faire à des algèbres $\mathscr{A}$ de matrices formant des extensions multi-quadratiques non commutatives de $\mathbb{R}$. Elle seront munies d'un anti-morphisme d'ordre deux $x \mapsto x^{\#}$ fixant uniquement le centre de l'algèbre, réduit à la droite des scalaires $\mathbb{R}\mathbb{1}$. On définit la norme $\det(x) = x^{\#}x$ et la trace $\operatorname{tr}(x) = x^{\#} + x$ à partir des lois multiplicative et additive. Ce sont respectivement une forme quadratique non-dégénérée et une forme linéaire non nulle. La sphère des éléments de norme unité $\mathfrak{G} = \{\det = 1\}$ est un groupe de Lie dont l'algèbre est le noyau de la trace $\mathfrak{g} = \{\operatorname{tr} = 0\}$. On obtient alors une décomposition de notre algèbre $\mathscr{A} = \mathbb{R}\mathbb{1} \oplus (\ker \operatorname{tr})$ qui est orthogonale pour la norme. La structure entière permet de considérer l'ensemble U des éléments entiers de norme ± 1 : c'est un groupe d'ordre 2×2^2 et de centre ± 1, pour lequel l'inversion coïncide avec la restriction de l'involution # (ainsi qu'avec le changement de signe sur les éléments non-centraux). De plus deux de ses éléments non opposés sont orthogonaux pour la norme det : on peut donc en choisir la moitié pour former une base orthonormée.

Ensuite commence le travail d'exploration géométrique et arithmétique. Il s'agit en particulier de déterminer la topologie du groupe des unités, son lien avec le groupe des isométries de la norme ou des automorphismes de l'algèbre. Viennent ensuite l'étude de l'algèbre de Lie avec la métrique induite, son intersection avec le groupe de Lie et l'interprétation géométrique de la formule de Jacobi. Enfin les propriétés de l'application exponentielle

Enfin la section 5 reviendra sur $\mathrm{M}_2(\mathbb{C})$, pour en évoquer la structure d'algèbre de quaternions complexe, c'est à dire de $\mathbb{C}$-algèbre simple centrale de dimension 4, et surtout pour revenir sur sa structure réelle. En effet, l'association deux sections précédentes permettra d'unifier dans un même contexte géométrique, l'action du groupe d'isométries $\mathrm{SL}_2(\mathbb{R})$ du plan hyperbolique sur le modèle du demi-plan de Poincaré dans $\mathbb{CP}^1$ et de Cayley-Klein dans $\mathbb{RP}^2$.

En appendice. Une première section contient quelques rappels et approfondissments d'algèbre bilinéaire. Elles permettront non seulement d'avoir un meilleur recul sur le corps du texte, mais également de pouvoir le situer vis à vis des cours introductifs aux groupes et algèbres de Lie.

Le seconde consiste en une excursion arithmétique déclinant les considérations géométriques, et en les appliquant à l'étude des formes quadratiques binaires entières. Nous y classifions les extensions quadratiques engendrées par une matrice pour en décortiquer l'arithmétique des idéaux. Nous dressons ensuite la correspondance entre formes quadratiques binaires entières et matrices entières dans $\mathfrak{sl}_2(\mathbb{Z})$.

Des tenseurs aux matrices.

Déchargeons nous d'une discussion légèrement abstraite afin de se ramener comme promis mais sans remords à la manipulation de matrices.

Nous ne travaillerons qu'avec des $\mathbb{Z}$-modules libres ou des espaces vectoriels sur $\mathbb{K}$ le corps des réels ou des complexes. Rappelons qu'un $\mathbb{Z}$-module libre V donne lieu par extension des scalaires à un espace vectoriel $V(\mathbb{K}) = V \otimes \mathbb{K}$. Réciproquement, le choix d'une base d'un tel espace vectoriel modulo changement de base à coefficients entiers (conjugaison par $\mathrm{GL}_n(\mathbb{Z})$) permet d'en retrouver la structure entière.

Une forme bilinéaire non-dégénérée $\beta \colon V \times V \to \mathbb{Z}$ sur un $\mathbb{Z}$-module libre permet de l'identifier à son dual $V^* = \mathrm{Hom}(V, \mathbb{Z})$ par la formule $v \mapsto \phi(v) = \beta(v, \cdot)$. L'espace $\mathrm{End}\, V = V^* \otimes V$ est alors muni de l'opérateur adjoint $\mathrm{End}(V) \to \mathrm{End}(V^*) \to \mathrm{End}(V)$ donné par l'échange des facteurs suivi de $\phi \otimes \phi^{-1}$: l'adjoint de $f \in \mathrm{End}(V)$ est donc l'unique $f^* \in \mathrm{End}(V)$ tel que $\beta(v, fw) = \beta(f^*v, w)$. Tout cela fonctionne également sur $\mathbb{R}$ ou $\mathbb{C}$ par extension des scalaires.

Pour β une forme *antisymétrique* sur un plan (entier, réel ou complexe), comme le déterminant dans une certaine base, l'adjoint de f est $f^\#$, la transposée de la comatrice. Pour β un produit scalaire Euclidien sur V on retrouve ainsi la transposée (n'ayant pas de connotation matricielle tant que nous n'avons pas choisi de base). Rappelons que les formes bilinéaires *symétriques* non dégénérées sont uniquement caractérisées, à un changement de base près, par la signature sur $\mathbb{R}$ (tandis que sur $\mathbb{C}$ elle est unique).

La donnée d'un espace vectoriel complexe V revient à celle d'un espace vectoriel réel W de dimension double muni d'un endormorphisme $\iota \colon v \mapsto \iota(v)$ tel que $\iota^2 = -\mathbb{1}$, la multiplication par $\sqrt{\text{-}1}$ correspond à l'action par ι. Un produit scalaire Euclidien sur W préservée par ι équivaut à celle d'un produit scalaire Hermitien sur V (qui est donc aussi caractérisée par la signature).

Lorsqu'un $\mathbb{Z}$-module W est muni d'un tel endomorphisme ι de carré $-\mathbb{1}$, on peut définir de manière analogue l'adjoint selon une forme ι-sesquilinéaire-Hermitienne. Dans cas, l'isomorphisme $\phi \colon V \to V^*$ est Hermitien (échangeant les structures ι et $-\iota$) et $\iota^* = -\iota$.

Tout cela fonctionne également sur $\mathbb{R}$ par extension des scalaires, puis sur $\mathbb{C}$ en laissant agir $\sqrt{\text{-}1}$ par ι (et non pas par extension des scalaire, ici W devient un $\mathbb{C}$-espace vectoriel de dimension moitié). L'adjoint selon un produit scalaire Hermitien correspond à la transconjuguée (n'ayant pas de connotation matricielle à ce stade). Les formes sesquilinéaires Hermitiennes sont également caractérisées à changement de base près par le rang et la signature.

Un intérêt de cette discussion est de montrer que la notion de transposée nécessite l'introduction d'une structure Euclidienne, celle de transconjuguée d'un produit Hermitien et celle de transcomatrice (ou du déterminant) d'une structure symplectique. Notons qu'en rang 2, une structure entière détermine une structure symplectique privilégiée : une base d'éléments entiers engendre un pavé de volume unitaire. En revanche, il y a plusieurs formes quadratiques binaires entières définies positives non isomorphes, et le choix d'un produit scalaire Euclidien (ou Hermitien) compatible avec la structure entière revient à celui d'une base d'éléments entiers (éventuellement complétée par son image par ι) que l'on déclare orthonormale.

Afin d'exprimer tous ces tenseurs géométriques (endomorphismes, formes bilinéaires, etc.) en termes de matrices, nous allons fixer un $\mathbb{Z}$-module de rang deux, et en choisir une base de manière à l'identifier une bonne fois pour toutes avec $\mathbb{Z}^2$, pour considérer ensuite les espaces vectoriels $\mathbb{R}^2$ et $\mathbb{C}^2$ munis des structures entières qui en résultent. Nous pouvons donc désormais identifier $\mathrm{End}_{\mathbb{Z}}(V) = \mathrm{M}_2(\mathbb{Z})$, ainsi que $\mathrm{End}_{\mathbb{K}}(V) = \mathrm{M}_2(\mathbb{K})$ pour $\mathbb{K} = \mathbb{R}, \mathbb{C}$; et la base étant fixée, la transposée et la transconjuguée retrouvent leur signification usuelle pour les matrices.

1 Algèbres réelles de dimension deux

Nous commençons par des exemples d'algèbres quadratiques réelles de dimension deux. Dans chaque sous section, nous choisissons $M \in \mathrm{M}_2(\mathbb{R})$ et analysons la nature géométrique de l'algèbre $\mathbb{R}[M]$ suivant l'approche systématique décrite en introduction.

1.1 Le corps des nombres complexes, et rotations elliptiques.

Le corps des nombres complexes est une extension quadratique du corps des réels, définie en adjoignant une racine $\sqrt{\text{-}1}$ de -1, donc algébriquement isomorphe à $\mathbb{R}[X]/(X^2+1)$. Comme la matrice I de rotation d'un quart de tour dans le sens trigonométrique satisfait $I^2+1=0$, on peut représenter $\mathbb{C} \to \mathbb{R}[I]$ comme le groupe des homothéties et translations du plan $\mathbb{R}^2$. Si l'on note un nombre complexe $z = t + u\sqrt{\text{-}1}$, il agit sur le plan comme la matrice $M = t\mathbb{1} + uI$. Examinons à quoi correspondent, via cet isomorphisme, la conjugaison complexe, les parties réelle et imaginaire ainsi que le carré du module.

La conjugaison complexe, unique automorphisme non-trivial du groupe de Galois de l'extension $\mathbb{C}/\mathbb{R}$, échange $\sqrt{\text{-}1}$ et $-\sqrt{\text{-}1}$ et se prolonge $\mathbb{R}$-linéairement en $z^* = t - u\sqrt{\text{-}1}$. Elle correspond donc au prolongement $\mathbb{R}$-linéaire de $I \mapsto -I$, autrement dit à $M^\# = t - uI$.

Ces involutions sont des symétries des $\mathbb{R}$-espaces vectoriels $\mathbb{C} \simeq \mathbb{R}[I]$ par rapport à la droite fixe : le corps des réels; et parallèlement à la droite imaginaire pure : le noyau de la forme linéaire $z \mapsto z + z^*$ ou $M \mapsto M + M^\#$, sur lequel la symétrie agit donc comme moins l'identité. La projection associée à ces symétries (parallèlement au même sous espace et sur l'espace fixe) correspond à la partie réelle d'un nombre complexe $z \in \mathbb{C}$, ou encore la trace de la matrice $M \in \mathbb{R}[I]$, et s'obtiennent comme la moitié de la forme linéaire (construite en ajoutant un nombre avec son symétrique). De manière analogue, on peut également multiplier un nombre avec son symétrique pour définir la forme quadratique $zz^* = t^2 + u^2 = MM^\#$ de signature $(2,0)$ et qui correspond au carré du module $|z|^2$ ou au déterminant $\det(M)$. Sa racine carré correspond à la longueur. Notons que la projection sur l'axe réel est orthogonale pour la forme quadratique, et on a la décomposition orthogonale $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}\sqrt{\text{-}1}$ ou $\mathbb{R}[S] = \mathbb{R}\mathbb{1} \oplus \mathbb{R}I$.

La sphère des unités pour la forme quadratique est un groupe $\mathfrak{G}$ pour la multiplication, le groupe de Lie $\mathrm{U}(1)$ des nombres complexes de module 1, ou le groupe des rotations elliptiques, matrices réelles orthogonales de déterminant 1, dénoté $\mathrm{SO}(2)$. Il est homéomorphe à un cercle, donc en particulier compact, témoignant de fait que la forme quadratique est définie positive. L'algèbre du groupe de Lie, est construite sur l'espace vectoriel tangent au groupe de Lie en l'identité. Cet espace correspond au noyau de l'application linéaire tangente à la forme quadratique $zz^* = MM^\#$ définissant implicitement le groupe de Lie comme hypersurface de niveau. On cherche donc le noyau de $z + z^* = M + M^\#$ qui est la trace, à savoir la droite imaginaire pure. Le groupe est abélien donc son algèbre aussi et son crochet est null : $[\theta_1 I, \theta_2 I] = 0$.

L'exponentielle définit un morphisme $\exp\colon (\mathfrak{g}, +) \to (\mathfrak{G}, \times)$ paramétrisant périodiquement le cercle par le tore $\mathbb{R}/2\pi\mathbb{Z}$, en coordonnées $\exp(\theta I) = \cos(\theta) + \sin(\theta) I$. En renormalisant un élément non nul par sa longueur, on tombe dans la sphère, ce qui permet de retrouver la décomposition polaire d'une similitude comme le produit d'une matrice scalaire par une matrice de rotation $M = \rho \exp(\theta I)$ avec $\rho \in \mathbb{R}_+^*$ et $\theta \in \mathbb{R}/2\pi\mathbb{Z}$ analogue à celle des nombres complexes, que l'on peut aussi écrire $M = \sqrt{\det(M)}\exp(\arg M)$ avec $\arg(M) \in \mathfrak{g}$ bien défini $\mod 2\pi I$.

Notons que l'intersection du groupe et de son l'algèbre de Lie $\{\det = 1\} \cap \{\mathrm{tr} = 0\}$ est réduit aux matrices à coefficients entiers $\{\pm I\}$ qui forment un groupe isomorphe à $\mathbb{Z}/2$.

1.2 Le produit cartésien $\mathbb{R} \times \mathbb{R}$, et rotations hyperboliques.

Considérons désormais la matrice K, qui vérifie $K^2 = \mathbb{1}$. L'algèbre $\mathbb{R}[K]$ est donc isomorphe à $\mathbb{R}[X]/(X^2-1)$, or le polynôme X^2-1 se factorise sur $\mathbb{R}$ comme le produit $(X-1)(X+1)$ et par le lemme chinois l'algèbre $\mathbb{R}[K]$ se factorise en un produit d'algèbres $\mathbb{R}[X]/(X-1) \times \mathbb{R}[X]/(X+1)$. Comme chaque facteur est isomorphe à $\mathbb{R}$ (l'unique $\mathbb{R}$-algèbre de dimension 1), on en déduit que $\mathbb{R}[K] \simeq \mathbb{R} \times \mathbb{R}$ est une algèbre non intègre.

Toute matrice $M \in \mathbb{R}[K]$ s'écrit $M = t + uK$, et sa conjuguée $M^\# = t - uK$. Notons bien que le produit dans $\mathbb{R}[K]$ n'est pas donné par le produit terme à terme des coefficient (t, u), mais des coefficients $(t+u, t-u)$, comme indiqué par l'isomorphisme précédent. Son déterminant vaut $\det(M) = MM^\# = t^2 - u^2$, c'est une forme quadratique de signature $(1, 1)$ dont les droites isotropes ont pour équation $t = \pm u$. Ce sont les directions tangentes à l'hyperbole $\{\det(M) = 1\}$, qui est la sphère unité de la norme. Cette « sphère » est à nouveau un groupe de Lie unidimensionel $\mathrm{SO}(1, 1)$, isomorphe à $\mathbb{R} \times \mathbb{Z}/2$, mais cette fois-ci non compact, témoignant du caractère indéfini de la forme quadratique. La forme trace $\mathrm{tr}(M) = M + M^\# = 2t$ a pour noyau la droite $\{\mathrm{tr}(M) = 0\}$ des vecteurs « purs » portée par K, qui correspond à nouveau à l'espace vectoriel tangent à la sphère en l'identité du groupe, dont c'est l'algèbre de Lie (abélienne : crochet null).

L'application exponentielle $\exp\colon \mathfrak{g} \to \mathfrak{G}$, toujours définie par la même série entière (solution formelle de $\partial \exp = \exp$) n'est pas surjective puisque le groupe $\mathfrak{G}$ n'est pas connexe, mais elle est injective et son image coïncide avec la demi-branche d'hyperbole passant par $\mathbb{1}$. Ses éléments $\exp(\theta K) = \cosh(\theta) + \sinh(\theta)K$ sont les rotations hyperboliques ; contemplez en l'action sur les droites isotropes, puis sur l'hyperbole : elle tourne. Tout élément M non isotrope (en dehors des tangentes à l'hyperbole unité) peut être divisé par la racine de sa norme en valeur absolue, pour tomber dans l'une des quatre branches des deux hyperboles $\{\det(M) = \pm 1\}$ (formant le groupe des éléments de norme unitaire $\det(M) \in \mathrm{U}$). Si $\det(M) > 0$ et $\mathrm{tr}(M) > 0$, on a la décomposition polaire $M = \sqrt{\det(M)}\exp(\arg M)$ avec $\arg(M) \in \mathfrak{g}$ uniquement défini.

Notons enfin que l'intersection du groupe $\{\det = \pm 1\}$ et de son l'algèbre de Lie $\{\mathrm{tr} = 0\}$ est réduit aux matrices à coefficients entiers $\{\pm K\}$ qui forment un groupe isomorphe à $\mathbb{Z}/2$.

Expliquons pourquoi les matrices suivantes engendrent également des algèbres isomorphes au produit carthésien $\mathbb{R} \times \mathbb{R}$.

$$J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad P = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \qquad E = \begin{pmatrix} e^{-1} & 0 \\ 0 & e \end{pmatrix}$$

C'est évident pour la première, qui est comme K la symétrie par rapport à une droite : elle vérifie la même relation algébrique $J^2 = \mathbb{1}$; le lemme chinois fournit une factorisation similaire, et la forme quadratique déterminant a la même expression en coordonnées (t, u).

La seconde est la matrice d'un projecteur sur la droite portée par le second vecteur colonne, il vérifie comme tout projecteur la relation $P^2 = P$. Mais comme $\mathbb{R}[P]$ contient la matrice $K = 2P - I$, un changement de variables montre que $\mathbb{R}[P] = \mathbb{R}[K]$.

Enfin, la matrice $E = \exp(K)$ appartient à $\mathbb{R}[K]$ (c'est une limite de polynnômes en K, donc d'éléments de $\mathbb{R}[K]$, qui est un sous espace vectoriel fermé de $\mathrm{M}_2(\mathbb{R})$), et comme E n'est pas scalaire, elle engendre une extension quadratique qui est donc égale à $\mathbb{R}[K]$.

En fait, toute matrice hyperbolique de $\mathrm{SL}_2(\mathbb{R})$, c'est-à-dire telle que $\mathrm{tr}^2(M) > 2$, engendre une algèbre isomorphe à celle considérée dans ce paragraphe. Son étude géométrique (forme quadratique, groupe et algèbre de Lie) sera donc la même (il suffit d'un simple changement de variables pour la diagonaliser et mettre en évidence l'hyperbole et ses asymptotes).

1.3 L'algèbre des nombres infinitésimaux, et rotations paraboliques.

Considérons enfin une matrice nilpotente $N = L - \mathbb{1}$, qui vérifie donc $N^2 = 0$, engendrant ainsi une algèbre de matrices $\mathbb{R}[N]$ isomorphe à $\mathbb{R}[X]/(X^2)$. Elle est *irréductible* au sens où l'on ne peut la factoriser en produit d'algèbres, mais elle n'est pas *réduite* car elle admet des éléments nilpotents non nuls, en particulier elle n'est pas intègre. On l'appelle parfois l'algèbre des nombres infinitésimaux car si $\mathbb{R}[X]$ est l'algèbre des fonctions polynomiales sur la droite affine, alors X^2 engendre l'idéal des fonctions qui s'annulent en 0 à l'ordre au moins deux, et $\mathbb{R}[X]/(X^2)$ correspond à l'algèbre des jets à l'ordre 1. Elle permet donc de manipuler des fonctions à l'ordre $o(X^2)$ en 0, c'est à dire ne retenant que la valeur t, et la dérivée u à l'origine.

Si $M = t + uN$, l'involution $N^\# = -N$ se prolonge par linéarité en $M^\# = t - uN$. La norme $\det(M) = MM^\# = t^2$ est une forme quadratique dégénérée de signature $(1, 0)$, ayant une seule droite isotrope $t = 0$ (qui compte double), parallèle à la paire de droites $t = \pm 1$ formant la « sphère » unité $\{\det(M) = 1\}$. Cette sphère est encore un groupe de Lie, isomorphe à $\mathbb{Z}/2 \times \mathbb{R}$, non compact et non connexe. La trace $\operatorname{tr}(M) = M + M^\# = 2t$, a pour noyau la droite $\{\operatorname{tr}(M) = 0\}$ porté par N, l'espace vectoriel tangent à la sphère en l'identité du groupe, et qui est abélienne.

L'application exponentielle $\exp\colon \mathfrak{g} \to \mathfrak{G}$ n'est pas surjective puisque le groupe $\mathfrak{G}$ n'est pas connexe, mais elle est injective et son image coïncide avec la droite $t = 1$ passant par $\mathbb{1}$. Ses éléments $\exp(\theta N) = \mathbb{1} + \theta N$ sont les transvections (ou rotations paraboliques, cas dégénéré entre les rotations elliptiques et hyperboliques). Comme avant, elles fixent la droite isotrope, tout en faisant « tourner la sphère » dans le sens trigonométrique, il est également instructif d'en visualisez l'action sur les droites passant par l'origine. Tout élément M non isotrope ($t \neq 0$) peut être divisé par la racine de sa norme, pour tomber dans l'une des deux droites $\{\det(M) = 1\}$. Si $\operatorname{tr}(M) > 0$, on obtient sa décomposition polaire $M = \rho \exp(\theta N) = \rho(1 + \theta N)$ avec $\rho = t$ et $\theta = u/t$, que l'on peut toujours écrire $M = \sqrt{\det(M)} \exp(\arg M)$ avec $\arg(M) \in \mathfrak{g}$ uniquement défini.

Cette fois, l'intersection du groupe et de son l'algèbre de Lie $\{\det = 1\} \cap \{\operatorname{tr} = 0\}$ est vide.

Bien sûr, l'algèbre engendrée par la matrice parabolique $L = \mathbb{1} + N$ est la même.

1.4 Classification sur le corps des réels

Vérifions désormais que les trois exemples étudiés couvrent toutes les possibilités et fournissent la classification des extensions quadratiques réelles.

Soit $M \in \mathrm{M}_2(\mathbb{R})$, non scalaire pour qu'elle engendre une extension non triviale. D'après le théorème de Cayley-Hamilton, elle est annulé par son polynôme caractéristique, qui est donc son polynôme minimal, et l'algèbre $\mathbb{R}[M]$ est isomorphe au quotient $\mathbb{R}[X]/\left(X^2 - \operatorname{tr}(M)X - \det(M)\right)$. Notons que dans le cas présent, les relations $\operatorname{tr}(M) = M + M^\#$, et $\det(M) = MM^\#$ rendent cette identité $M^2 - (M + M^\#)M + MM^\# = 0$ évidente. La nature de $\mathbb{R}[M]$ à isomorphisme de $\mathbb{R}$-algèbres près dépend des propriétés de factorisations sur $\mathbb{R}$ du polynôme annulateur de M, dont le nombre de racines dépend uniquement de la valeur de son discriminant $\Delta = \operatorname{tr}^2(M) - 4\det(M)$ dans $\mathbb{R}/(\mathbb{R}^*)^2$, soit encore dans l'ensemble $\{-1, 0, 1\}$.

Si $\Delta = 0$, il a une racine réelle double α donc $(M - \alpha)^2 = 0$ et le changement de variables $M' = M - \alpha\mathbb{1}$ donne $\mathbb{R}[M']$ isomorphe à $\mathbb{R}[X]/(X^2)$. Si $\Delta < 0$, il a deux racines complexes conjuguées distinctes α, α^* donc $M - \Re(\alpha)M + (\Re(\alpha)^2 + \Im(\alpha)^2) = 0$ et en complétant le carré, on constate que le changement de variables $M' = (M - \Re(\alpha)/2) \div \Im(\alpha)/2$ donne $\mathbb{R}[M'] \simeq \mathbb{R}[X]/(X^2 - 1)$. Si $\Delta > 0$, il a deux racines réelles distinctes α, α' donc $(M - \alpha)(M - \alpha') = 0$ et le changement de variables $M' = (M - \frac{1}{2}(\alpha + \alpha')) \div \frac{1}{2}(\alpha - \alpha')$ donne $\mathbb{R}[M'] \simeq \mathbb{R}[X]/(X^2 - 1)$.

En conclusion, pour toute matrice $M \in \mathrm{M}_2(\mathbb{R})$ non scalaire, l'algèbre $\mathbb{R}[M]$ est isomorphe au quotient de $\mathbb{R}[X]$ par l'un des trois polynômes X^2+1, X^2+1 et X^2. Notons que ces trois algèbres sont engendrées par une matrice dont le carré vaut -1, 1 et 0 (par exemple S, K et N), ou encore par leurs exponentielles, à savoir une matrice elliptique, hyperbolique et parabolique (par exemple $\exp(2\pi S) = S$, $\exp(K) = E$ et $\exp(N) = L$). Attention : il n'est pas vrai que l'isomorphisme $\mathbb{R}[A] \simeq \mathbb{R}[B]$ entraîne l'égalité $\mathbb{R}[A] = \mathbb{R}[B]$: il se peut très bien que $A \notin \mathbb{R}[B]$ comme c'était le cas pour les matrices J et K de l'exemple précédent.

Notons que le résultat est encore valable pour $M \in \mathrm{M}_2(\mathbb{C})$ pourvu que son polynôme caractéristique soit à coefficients réels, ce qui revient à demander $\mathrm{tr}(M) = M + M^\# \in \mathbb{R}$ et $\det(M) \in \mathbb{R}$. Cela implique qu'elle est en fait conjuguée dans $\mathrm{M}_2(\mathbb{C})$ à un élément de $\mathrm{M}_2(\mathbb{R})$. En effet, l'hypothèse signifie que ses valeurs propres sont toutes deux réelles ou complexes conjuguées. Il suffit alors de distinguer selon le cas où M est diagonalisable ou non.

Résumons les caractéristiques des trois classes d'isomorphismes dans un tableau comparatif.

Algèbre	$\mathbb{R}[I]$: Corps	$\mathbb{R}[K]$: semi-simple	$\mathbb{R}[N]$: non réduite
Involution $M^\#$	$t-uI$	$t-uK$	$t-uN$
$\det(M) = MM^\#$	t^2+u^2	t^2-u^2	t^2
Signature	$(2,0)$	$(1,1)$	$(1,0)$
Espaces isotropes	Point	Droites sécantes	Droite double
Conique unités $\mathfrak{G}$	Ellipse	Hyperbole	Deux droites
$\mathfrak{G}^\pm = \{\det = \pm 1\}$	Ellipse	Deux Hyperboles	Deux droites
$\mathrm{tr}(M) = M + M^\#$	$\ker \mathrm{tr} = \mathfrak{g} = \mathbb{R}I$	$\ker \mathrm{tr} = \mathfrak{g} = \mathbb{R}K$	$\ker \mathrm{tr} = \mathfrak{g} = \mathbb{R}N$
$\mathfrak{g} \cap \mathfrak{G}^\pm$	$\pm I$	$\pm K$	$\emptyset$
$\exp\colon\ \mathfrak{g} \to \mathfrak{G}^\pm$	$\ker = 2\pi I\mathbb{Z}$ $\mathrm{coker} = 0$	$\ker = 0$ $\mathrm{coker} = (\mathbb{Z}/2)^2$	$\ker = 0$ $\mathrm{coker} = \mathbb{Z}/2$
$\sqrt{\det M}\exp(\arg M)$	$\cos(\theta) + \sin(\theta) I$	$\cosh(\theta) + \sinh(\theta) K$	$t(1 + (u/t)N)$

Une petite image avec trois vignettes qui comparent les trois géométries.

Reformulons cela dans un language un peu plus algébrique, rien que pour permettre la lecture de références plus abstraites. Rappelons (pour les adeptes du language algébrique) qu'une algèbre est *à division* si tous les éléments non nuls admettent un inverse, c'est à dire si elle n'a pas d'idéaux à gauche ; qu'une algèbre est *simple* si elle n'a pas d'idéaux bilatères non-triviaux, et qu'une algèbre *semi-simple* de dimension finie sur un corps de caractéristique nulle, se décompose en un produit d'algèbres simples (nous pouvons prendre cela comme définition de la semi-simplicité). Notons qu'une algèbre à division est toujours simple, et qu'une algèbre simple est semi-simple. Dans ces termes, nous avons trois extensions quadratiques de $\mathbb{R}$: une algèbre à division $\mathbb{C}$, qui est même un corps puisqu'il est commutatif (comme toute extension de degré 2) ; une algèbre semi-simple $\mathbb{R} \times \mathbb{R}$ mais non intègre, et une algèbre non réduite.

2 L'algèbre des endomorphismes du plan complexe

Dans cette section nous allons décortiquer la structure de l'algèbre $\mathrm{M}_2(\mathbb{C})$ des matrices complexes, en tant que $\mathbb{R}$-algèbre de dimension 8. Nous avons déterminé en section 1 ses sous algèbres réelles de dimension 2 : ce sont des extensions quadratiques réelles engendrées par un élément conjugué à une matrice non-scalaire dans $\mathrm{M}_2(\mathbb{R})$, et nous en avons décrit les géométries possibles. Nous allons désormais, en nous aidant des trois involutions sur $\mathrm{M}_2(\mathbb{C})$, en dégager ses trois sous algèbres de dimension 4 réelles, chacunes munies de deux involutions. En particulier l'algèbre à division des quaternions de Hamilton et l'algèbre simple des coquaternions de Cookle, qui feront chacune l'objet d'un étude géométrique dans les sections 3 et 4.

2.1 Trois involutions

On appelle anti-morphisme d'algèbre une application linéaire qui inverse l'ordre de multiplication, on en déduit les notions d'anti-isomorphisme et d'anti-automorphisme. Une involution est un anti-automorphisme d'ordre deux (c'est-à-dire de carré l'identité).

Trois involutions. Considérons, sur l'algèbre des matrices $\mathrm{M}_2(\mathbb{C})$ les trois opérations suivantes : la transposition, prendre la comatrice, et la conjugaison complexe. La transposition est une involution, ceci est vrai en toute dimension et sur n'importe quel anneau des scalaires. Prendre la comatrice est un automorphisme qui est d'ordre deux en dimension 2. Enfin la conjugaison complexe est un automorphisme réel d'ordre deux, l'élément non trivial du groupe de Galois de l'extension quadratique du corps des scalaires $\mathbb{C}/\mathbb{R}$; il faut préciser automorphisme réel car il n'est pas $\mathbb{C}$-linéaire mais Hermitien.

En composant l'involution de transposition avec la comatrice et la conjugaison complexe, on obtient donc deux autres involutions : la transcomatrice $M \mapsto M^\#$, et la transconjuguée $M \mapsto M^*$; précisons que la première est une involution sur $\mathbb{R}$ ou $\mathbb{C}$ tandis que la seconde ne l'est que sur $\mathbb{R}$, car elle est $\mathbb{C}$-Hermitienne. Dans cette section, nous allons nous concentrer sur la structure de $(\mathrm{M}_2(\mathbb{C}), {}^tM, M^\#, M^*)$ en tant que $\mathbb{R}$-algèbre de dimension 8 munie de trois involutions (qui commutent et sont indépendants au sens où ils engendrent un groupe $(\mathbb{Z}/2)^3$ d'automorphismes, mais pas tous involutifs). Parmi ces trois involutions, la transcomatrice mérite qu'on lui accorde plus d'intérêt, parce le théorème de Cayley-Hamilton $M - \mathrm{tr}(M)M + \det(M)\,\mathbb{1} = 0$ correspond à l'égalité $M - (M^\# + M)M + M^\# M = 0$, et notre étude géométrique se focalisera sur #.

Trois formes quadratiques. La trace et le déterminant s'obtiennent par addition et multiplication avec la transcomatrice : $M^\# + M = \mathrm{tr}(M)$ et $M^\# M = \det(M)$. Ce sont respectivement des formes linéaire et quadratique complexes. La sphère unité $\mathrm{SL}_2(\mathbb{C})$ du déterminant a pour espace tangent en l'identité le noyau $\mathfrak{sl}_2(\mathbb{C})$ de la trace.

On peut également considérer la forme quadratique $M \mapsto {}^tMM$ de sphère $\mathrm{O}_2(\mathbb{C})$ et dont la forme linéaire tangente $M \mapsto {}^tM + M$ a pour noyau le sous espace des matrices antisymétriques.

La forme quadratique hermitienne $M \mapsto M^*M$ a pour sphère le groupe U_2 dont la forme linéaire tangente $M \mapsto M^* + M$ a pour noyau le sous espace des matrices anti-hermitiennes.

Ces trois formes quadratiques ont signature $(4,4)$ sur $\mathbb{R}$, les deux premières sont $\mathbb{C}$-linéaires.

2.2 Trois sous algèbres.

Etudions désormais les trois sous algèbres réelles de dimension 4 de $(\mathrm{M}_2(\mathbb{C}),{}^tM, M^\#, M^*)$, définies comme le lieu d'égalité de deux involutions parmi les trois.

Quaternions de Hamilton. Commençons par définir l'algèbre des quaternions de Hamilton par $\mathbb{H} = \{M \in \mathrm{M}_2(\mathbb{C}) \mid M^\# = M^*\}$, elle est munie de l'involution $M^\# = M^*$, ainsi que ${}^tM$ d'importance moindre. Elle admet pour base les éléments :

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \qquad i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad j = \sqrt{\text{-}1}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad k = \sqrt{\text{-}1}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

qui satisfont les relations $i^2 = k^2 = j^2 = ijk = -1$ et $ij = -ji$, $jk = -kj$, $ki = -ik$. On donc la présenter comme une $\mathbb{R}$-algèbre engendrée par deux éléments j, k satisfaisant les relations ci-dessous ; ou de manière équivalente comme une $\mathbb{R}[i]$-algèbre Hermitienne engendrée par un élément j vérifiant $j^2 = -1$ (Hermitienne signifie que la conjugaison par le générateur j agit sur le corps $\mathbb{R}[i]$ comme l'involution Galoisienne : $jc = c^\# j$),

$$\mathrm{M}_2(\mathbb{R}) \simeq \frac{\mathbb{R}[j,k]}{(j^2 = k^2 = -1,\ jk = -kj)} \simeq \frac{\mathbb{R}[i]}{(j^2 = -1, ij = -ji)}.$$

Les éléments $\pm\{1, i, j, k\}$ forment le groupe des quaternions de Hamilton $\mathcal{Q}_8$, d'ordre 8 et de centre ± 1 (c'est le groupe des symétries d'un pavé spinoriel [1, Chap. 11]). On peut donc aussi définir $\mathbb{H}$ comme un $\mathbb{Z}/2$-quotient de l'algèbre du groupe des quaternions $\mathbb{R}[\mathcal{Q}_8]/(-1_{\mathbb{R}} = -1_{\mathcal{Q}_8})$ où l'on identifie l'action par multiplication des unités ± 1 de $\mathbb{R}$ avec celle du centre $\{\pm 1\} \subset \mathcal{Q}_8$.

On constate alors que l'involution # sur l'algèbre coïncide avec le prolongement par linéarité de l'inversion dans le groupe ; à la différence de la transposée, qui fixe j, k mais échange i en son inverse Elles agissent comme l'identité sur le projectifié $\mathbb{P}(\mathcal{Q}_8)$ pour sa structure de $\mathbb{Z}/2$ espace vectoriel (donnée par multiplication par un élément ± 1 du centre), formant le groupe $(\mathbb{Z}/2)^2$.

Coquaternions de Coockle. Cherchant des analogues à l'algèbre des quaternions de Hamilton, Coockle découvrit celle des matrices $\mathrm{M}_2(\mathbb{R}) = \{M \in \mathrm{M}_2(\mathbb{C}) \mid {}^tM = M^*\}$, qu'il baptisa coquaternions. Elle est munie de l'involution $M^\#$ ainsi que ${}^tM = M^*$ d'importance moindre et admet pour base vectorielle les éléments :

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \qquad I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad K = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

Les relations quadratiques $I^2 = -J^2 = -K^2 = -1$, de permutation $IJ = K$, $KJ = -I$, $KI = J$, (attention au signe pour la seconde) et d'anticommutation $IJ = -JI$, $JK = -KJ$, $IJ = -JI$ permettent de calculer aisément et d'obtenir une présentation algébrique comme extension multiquadratique des réels, et comme extension Hermitienne de l'extension quadratique réelle $\mathbb{R}[I]$ isomorphe au corps des complexes, par un élément J de carré $J^2 = 1$:

$$\mathrm{M}_2(\mathbb{R}) \simeq \frac{\mathbb{R}[J,K]}{(J^2 = K^2 = 1,\ JK = -KJ)} \simeq \frac{\mathbb{R}[I]}{(J^2 = 1, IJ = -JI)}$$

Comme pour les quaternions de Hamilton, les involutions se comportent comme $J^\# = -J$ et $K^\# = -K$ puis ${}^tJ = J$ et ${}^tK = K$ (mais attention au produit $I = KJ$ pour lequel on a $I^\# = -I = {}^tI$).

Les éléments $\pm\{\mathbb{1}, I, J, K\}$ forment le groupe diédral $\mathcal{D}_4$ des symétries du carré, d'ordre 8 et de centre ± 1. On peut donc aussi définir $\mathrm{M}_2(\mathbb{R})$ comme un $\mathbb{Z}/2$-quotient de l'algèbre du groupe diédral $\mathbb{R}[\mathcal{D}_4]/(-1_{\mathbb{R}} = -1_{\mathcal{D}_4})$ où l'on identifie l'action par multiplication des unités ± 1 de $\mathbb{R}$ avec celle du centre $\{\pm 1\} \subset \mathcal{D}_4$.

On constate que l'involution # sur l'algèbre coïncide avec le prolongement par linéarité de l'inversion dans le groupe ; à la différence de la transposée, qui fixe J, K mais échange I en son inverse. Elles agissent trivialement sur le projectifié $\mathbb{P}(\mathcal{D}_2)$ pour sa structure de $\mathbb{Z}/2$-espace vectoriel (donnée par multiplication d'un élément du centre), formant le groupe $(\mathbb{Z}/2)^2$.

Algèbre produit. Enfin, l'algèbre $\{M \in \mathrm{M}_2(\mathbb{C}) \mid {}^tM = M^\#\}$ des matrices égales à leur comatrices munie des involutions $M^\#$ et M^*, a pour base (toujours sur $\mathbb{R}$) les éléments $\mathbb{1}, I, \sqrt{\text{-}1}, \sqrt{\text{-}1}\, I$, qui satisfont les relations $I^2 = \sqrt{\text{-}1}^2 = -1$ et $I\sqrt{\text{-}1} = \sqrt{\text{-}1}\, I$. Cette $\mathbb{R}$-algèbre engendrée par deux éléments de carré -1 et qui commutent, n'est rien d'autre que $\mathbb{C}[I]$, isomorphe à $\mathbb{C} \times \mathbb{C}$: ce n'est donc pas une algèbre simple, seulement semi-simple.

Les éléments $\pm\{1, I, \sqrt{\text{-}1}, \sqrt{\text{-}1}\, I\}$ forment le groupe commutatif $(\mathbb{Z}/2) \times (\mathbb{Z}/4)$ d'ordre 8. Nous avons encore une fois $\mathbb{C}[I]$ isomorphe au $\mathbb{Z}/2$-quotient de l'algèbre de ce groupe où l'on identifie l'action par multiplication des unités ± 1 sur $\mathbb{R}$ et par le sous groupe ± 1 du facteur $\mathbb{Z}/4$. Cette fois c'est l'involution M^* qui coïncide avec le prolongement par linéarité de l'inversion dans le groupe ; tandis que $M^\#$ fixe $\sqrt{\text{-}1}$ mais échange I et $\sqrt{\text{-}1}\, I$ en leurs opposés. Elles agissent trivialement sur le quotient de $(\mathbb{Z}/2)^2$ par le sous groupe $\mathbb{Z}/2$ engendré par ± 1.

Décomposition en. Nous avons donc trouvé trois sous algèbres de dimension 4 dans $\mathrm{M}_2(\mathbb{C})$ à savoir $\mathbb{H}$, $\mathrm{M}_2(\mathbb{R})$ et $\mathbb{C}[I]$, qui sont respectivement une algèbre à division, une algèbre simple centrale (de centre $\mathbb{R}$) et une algèbre semi-simple (mais non simple). Il est aisé de déterminer leur position mutuelle pour avoir la suite exacte d'espaces vectoriels, qui n'est pas sans rappeler une suite de Mayer Vietoris puisque le noyau vaut l'intersection $\mathbb{H} \cap \mathrm{M}_2(\mathbb{R})$:

$$\mathbb{R}[I] \to \mathbb{H} + \mathrm{M}_2(\mathbb{R}) \to \mathrm{M}_2(\mathbb{C}) \to \mathbb{R}[\sqrt{\text{-}1}\, I]$$

Notons que la somme du noyau $\mathbb{R}[I]$ et du conoyau $\mathbb{R}[\sqrt{\text{-}1}\, I]$ donne la troisième algèbre $\mathbb{C}[I]$.

Nous pouvons également présenter cela sous la forme d'un carré dont les quatre cases sont des sous espaces vectoriels de dimension 2 et en somme directe dans $\mathrm{M}_2(\mathbb{C})$. La somme sur la première ligne horizontale donne $\mathrm{M}_2(\mathbb{R})$, celle de la première colonne $\mathbb{H}$ et la diagonale s'ajoute pour donner $\mathbb{C}[I]$. Laissons en exercice le plaisir d'étudier l'action des involutions, et multiplication par les divers éléments de nos bases favorites sur ce carré, ou cube...

$\mathbb{R}\mathbb{1} \oplus \mathbb{R}I$	$\mathbb{R}J \oplus \mathbb{R}K$
$\mathbb{R}i \oplus \mathbb{R}j$	$\mathbb{R}\sqrt{\text{-}1}\, I \oplus \mathbb{R}\mathbb{1}$

Algèbres d'entiers. Notons pour finir que tout ce que nous avons dit fonctionne sur $\mathbb{Z}$: toutes les équations polynômiales rencontrées étaient unitaires et à coefficients entiers. On peut donc définir les $\mathbb{Z}$-algèbres des entiers de Hamilton $\mathbb{H}(\mathbb{Z})$, des matrices entières $\mathrm{M}_2(\mathbb{Z})$, ou des bi-entiers de Gauss $Z[I, \sqrt{\text{-}1}]$, dont $\mathbb{H}$, $\mathrm{M}_2(\mathbb{R})$ et $\mathbb{C}[I]$ sont obtenus par produit tensoriel $\otimes_{\mathbb{Z}}\mathbb{R}$.

2.3 Définitions abstraites, approche systématique, retour au concret

Définitions équivalentes. Selon la définition moderne, une algèbre de quaternions H sur un corps $\mathbb{K}$ est une algèbre simple centrale de dimension 4 sur $\mathbb{K}$: cela signifie n'admet pas d'idéal bilatère non-trivial, et que son centre est égal à $\mathbb{K}$.

On peut montrer qu'il existe un élément non scalaire $i \notin \mathbb{K}$ dont le carré appartient à $\mathbb{K}$, et qui engendre donc une extension quadratique $L = \mathbb{K}[i]$, dont H est elle même une extension quadratique hermitienne $H = L[j]$ avec $ji = i^*j$ où $i^* = -i$ est l'involution Galoisienne de $L/\mathbb{K}$, et $j^2 = a \in \mathbb{K}$. Il suffit alors de connaître l'extension quadratique L et le scalaire $a \in \mathbb{K}$ pour déterminer H à isomorphisme près (bien que le couple de soit pas unique), c'est parfois la définition que l'on trouve pour les algèbres de quaternions [2].

En caractéristique $\neq 2$, cela équivaut à une extension multiquadratique non commutative : plus précisément une algèbre de polynômes sur $\mathbb{K}$ à variables non commutatives qui est engendrée par deux éléments j, k vérifiant les relations quadratiques $j^2 = a, k^2 = b$ pour des scalaires $a, b \in \mathbb{K}$ et d'anticomutation $kj = -jk$. La structure de l'algèbre ne dépend que des propriétés arithmétiques de a et b, et plus précisément de l'équation diophantienne $ax^2 + by^2 = 1$ sur $\mathbb{K}$.

Approche systématique. Nous pouvons résumer le caractère systématique de l'approche de la façon suivante. Nos algèbres sont munies d'un unique anti-morphisme d'ordre deux $x \mapsto x^\#$ dont les points fixes sont la droite des scalaires $\mathbb{K}$. On définit la norme $\det(x) = x^\# x$ et la trace $\operatorname{tr}(x) = x + x^\#$ à partir des lois multiplicative et additive. Ce sont respectivement une forme quadratique non-dégénérée et une forme linéaire non nulle. La sphère des éléments de norme unité $G = \{\det = 1\}$ est un groupe de Lie dont l'algèbre de Lie est le noyau de la trace $g = \{\operatorname{tr} = 0\}$. On obtient alors une décomposition de notre algèbre $A = \mathbb{R} \oplus (\ker \operatorname{tr})$ qui est orthogonale pour la norme. La structure entière permet de de considérer l'ensemble U des éléments entiers de norme ± 1 : c'est un groupe d'ordre 2×2^2 et de centre ± 1, pour lequel l'inversion coïncide avec la restriction de l'involution # (ainsi qu'avec le changement de signe sur les éléments non-centraux). De plus deux de ses éléments non opposés sont orthogonaux pour la norme det : on peut donc en choisir la moitié pour former une base orthonormée. Ensuite commence le travail d'exploration géométrique et arithmétique.

Justification du modèle et des bases. Après avoir donné quelques définitions équivalentes des algèbres de quaternions, nous prenons le parti de travailler avec la plus concrète d'entre elles, à savoir celle des sous algèbres matricielles de $\mathrm{M}_2(\mathbb{C})$, définies comme lieu d'égalités de deux involutions. Nous travaillerons également avec nos bases favorites.

Ces choix ne servent pas qu'à la simplicité de l'exposition : le premier met en valeur le caractère privilégié des involutions ${}^tM, M^*, M^\#$ qui correspondent aux adjonctions pour les trois structures bilinéaires réelles non dégénérées (anti)-symétriques priviligiées sur un plan complexe : euclidienne, hermitienne et symplectique (voir l'appendice A). Cette trialité surgit également dans la classification des groupes de Lie complexes, ou de leurs formes rélles compactes.

Nos bases explicites peuvent alors être justifiées en considérant l'intersection $\mathbb{R}[I]$ des algèbres simples $\mathbb{H} \cap \mathrm{M}_2(\mathbb{R})$ ainsi trouvées, sa structure entière permet de sélectionner la paire $\pm I = \pm i$ de manière unique. Ensuite, on montre sans trop de peine pour chacune de nos algèbres, que la famille $\pm \mathbb{1}, \pm I$ se complète de manière unique en un groupe fini $\mathcal{U}$ d'ordre 8 constitué d'éléments entiers, tel que le choix d'un élément par orbite sous l'action de ± 1 forme une base de l'algèbre.

3 Quaternions de Hamilton et $\mathfrak{su}_2$

3.1 Symétries et coordonnées

Avant de se lancer dans l'étude géométrique à proprement parler, prenons nos marques avec le groupe des quaternions, et la représentation matricielle.

Automorphismes du groupe des quaternions. Commençons par déterminer les symétries du groupe $\mathcal{Q}_8 = \pm\{\mathbb{1}, i, j, k\}$ des quaternions. Comme $\mathbb{H}(\mathbb{Z})$ est donné par le produit tensoriel de $\mathbb{Z}/2$ algèbres $\mathbb{Z} \otimes \mathcal{Q}_8$ où l'action de $\mathbb{Z}/2$ correspond à la multiplication par ± 1 dans chacune, cela permettra d'en déduire les automorphismes de $\mathbb{H}$ respectant sa structure entière.

Déterminons d'abord les automorphismes du quotient par le centre $\mathbb{Z}/2 \to \mathcal{Q}_8 \to (\mathbb{Z}/2)^2$. Comme ce quotient correspond au projectifié de $(\mathbb{Z}/2)^3$ (pour la structure de $\mathbb{Z}/2$ espace vectoriel sur $\mathcal{Q}_8$ donnée par multiplication par un élément ± 1 du centre), son groupe d'automorphismes vaut $\mathrm{PGL}_3(\mathbb{Z}/2)$ et se manifeste comme le groupe symétrique sur $\{\pm i, \pm j, \pm k\}$, donc est isomorphe à $\mathfrak{S}_3$. Nous vérifions sans peine que toutes ces symétries se relèvent en des automorphismes de $\mathcal{Q}_8$ (mais ce n'est pas automatique, et nous verrons que cette propriété tombe en défaut pour $\mathcal{D}_4$).

A cela il faut ajouter les automorphismes du noyau $\mathrm{Aut}(\mathcal{Q}_8) \to \mathrm{Aut}(\mathbb{P}(\mathcal{Q}_8))$, c'est-à-dire celles qui agissent uniquement par changement de signes. Le signe de $\mathbb{1}$ est fixé, tandis que celui des trois autres élément est libre. Elles forment un groupe $(\mathbb{Z}/2)^2$, formé par la transposée (qui fixe j, k mais échange i en son inverse), et ses conjugués par le sous groupe $\mathbb{Z}/3 \subset \mathfrak{S}_3$. Rappelons que l'échange des signes de i, j, k correspond à l'inversion du groupe (ce n'est donc pas un automorphisme mais un anti-automorphisme du groupe) et se prolonge par linarité à l'involution # de l'algèbre.

Nous avons donc une description complète des symétries $\mathrm{Aut}(\mathcal{Q}_8)$ du groupe des quaternions comme un produit semi-direct $(\mathbb{Z}/2)^2 \rtimes \mathfrak{S}_3$, qui n'est autre que le groupe des isométries linéaires $\mathrm{GL}_3(\mathbb{Z}/2) = (\mathbb{Z}/2)^2 \rtimes \mathrm{PGL}_2(\mathbb{Z}/2)$ de l'espace tridimensionel sur le corps $\mathbb{Z}/2$, également isomorphe au groupe des symétries $\mathfrak{S}_4$ de l'octaèdre.

Reprenons le raisonement d'un point de vue plus algébrique. Nous avons d'abord déterminé les automorphismes du quotient de $\mathcal{Q}_8$ par son centre, c'est à dire ses automorphismes extérieurs. Après avoir vérifié que ce groupe $\mathfrak{S}_3$ se relève en un sous groupe des automorphismes de $\mathrm{Aut}(\mathcal{Q}_8)$, autrement dit que la suite exacte $\mathrm{Inn}(\mathcal{Q}_8) \to \mathrm{Aut}(\mathcal{Q}_8) \to \mathrm{Out}(\mathcal{Q}_8)$ est scindée, et sachant que le éléments non triviaux de $\mathrm{Inn}(\mathcal{Q}_8)$ correspondent à la conjugaison par les éléments non centraux i, j, k, nous avons déterminé la nature du produit semi direct $\mathrm{Aut}(\mathcal{Q}_8) = (\mathbb{Z}/2)^2 \rtimes \mathfrak{S}_3$ pour en déduire que $\mathrm{Aut}(\mathcal{Q}_8) = \mathfrak{S}_4$, forme les symétries de l'octaèdre.

Coordonnées complexes. $(x + yI)J$

- Décomposition dans la base favorite (déduite de section 1 et 2) - seconde justification unique base entière groupe - Isomorphisme vectoriel avec $\mathbb{C}^2$ - Involution d'algèbre

Proposition. *Il y a une unique base othonormée à conjugaison près. Il y en a une unique qui est entière, à permutation de ses éléments près (permutation alternée si l'on demande de plus qu'elle soit directe).*

Il y a une unique base directe B telles que $\pm B$ forme un groupe, toujours à conjugaison près.

Dans chaque cas, si l'on fait intervenir la structure entière en demandant une base entière, il n'y a pas besoin de quotienter par l'action de conjugaison pour avoir unicité

3.2 Norme et Groupe des unités

- signature de la forme quadratique - topologie de la sphère unité - action double translation rpz $\mathfrak{G}^2$ dans $\mathrm{SO}(\mathbb{H}, \det)$ de dim 4 (annonce Skolem Noether) - la base privilégiée est unitaire orthonormale (justif 3) (attention signe) - Attention à l'autre involution (métrique de Minkowski)

3.3 Agèbres des quaternions purs de trace nulle

- (la base est compatible avec la somme R+V)
- expression du produit : (Killing et Crochet : produit scalaire et produit vectoriel)
- restriction de la norme, sphère
- action par conjugaison automorphsimes $\mathrm{SO}(\mathfrak{su}_2, \det) = \mathrm{SO}(3)$ (cite spinorial Penrose)
- espace symétrique (intersection groupe algèbre, $s^2 = -1$, topologie $\mathbb{S}^2 = \mathbb{CP}^1$ (revet $\mathbb{RP}^2$?)
- interprétation géométrique de la formule de Jacobi sur l'espace symétrique

3.4 Exponentielle et décomposition polaire

- décomposition polaire - Fibration de Hopf - Tores de Clifoors et cercles de Villarceau

4 Coquaternions de Cockle et $\mathfrak{sl}_2(\mathbb{R})$

4.1 Représentation matricielle

: - Décomposition dans la base favorite (déduite de section 1 et 2) - seconde justification unique base entière groupe - Isomorphisme vectoriel avec $\mathbb{C}^2$ - Involution d'algèbre

Proposition. *Il y a une unique base othonormée à conjugaison près. Il y en a une unique qui est entière, à permutation de ses éléments près (permutation alternée si l'on demande de plus qu'elle soit directe).*

Il y a une unique base directe B telles que $\pm B$ forme un groupe, toujours à conjugaison près.

Dans chaque cas, si l'on fait intervenir la structure entière en demandant une base entière, il n'y a pas besoin de quotienter par l'action de conjugaison pour avoir unicité

4.2 Norme et Groupe des unités

- signature de la forme quadratique - topologie de la sphère unité - action double translation rpz $\mathfrak{S}^2$ dans $\mathrm{SO}(\mathbb{H}, \det)$ de dim 4 (annonce Skolem Noether) - la base privilégiée est unitaire orthonormale (justif 3) (attention signe) - Attention à l'autre involution (métrique de Minkowski)

4.3 Agèbres des quaternions purs de trace nulle

- (la base est compatible avec la somme R+V)
- expression du produit : (Killing et Crochet : produit scalaire et produit vectoriel)
- restriction de la norme, sphère
- action par conjugaison automorphsimes $\mathrm{SO}(\mathfrak{su}_2, \det) = \mathrm{SO}(3)$ (cite spinorial Penrose)
- espace symétrique (intersection groupe algèbre, $s^2 = -1$, topologie $\mathbb{S}^2 = \mathbb{CP}^1$ (revet $\mathbb{RP}^2$?)
- interprétation géométrique de la formule de Jacobi sur l'espace symétrique

4.4 Exponentielle et décomposition polaire

- décomposition polaire - Fibration de Hopf - Tores de Clifoors et cercles de Villarceau

5 Géométrie projective complexe et $\mathfrak{sl}_2(\mathbb{C})$

5.1

Remarquons d'abord qu'en tant que $\mathbb{C}$-algèbre, elle n'admet pas d'idéaux bilatères non triviaux, c'est donc une algèbre simple de dimension 4. En effet soit B idéal non trivial ne peut ni contenir d'élément inversible, donc tous ses éléments sont de rank 1, et comme il est stable par conjugaison, on peut échelloner un élément.

Définition. *Une algèbre de quaternions sur $\mathbb{K}$ est une algèbre simple centrale de dimension 4 sur $\mathbb{K}$.*

Proposition. *Les matrices complexes $\mathrm{M}_2(\mathbb{C})$ est une algèbre simple centrale de dimension 4 sur $\mathbb{C}$.*

Trace et Norme. Commençons par quelques remarques et définitions d'ordre général. La trace et le déterminant s'obtiennent à partir de l'addition et multiplication avec la comatrice : $M^{\#} + M = \mathrm{tr}(M)$ et $M^{\#}M = \det(M)$. L'égalité $M - (M^{\#} + M)M + M^{\#}M = 0$ retrouve le théorème de Cayley-Hamilton $M - \mathrm{tr}(M)M + \det(M)\,\mathbb{1} = 0$.

Le déterminant est une forme quadratique complexe tandis que la trace est une forme linéaire complexe. La sphère unité du déterminant a pour espace tangent en l'identité le noyau de la trace : le groupe de Lie $\mathrm{SL}_2(\mathbb{C}) = \{M^{\#}M = \mathbb{1}\}$ des matrices de déterminant 1 a pour algèbre de Lie l'espace vectoriel $\mathfrak{sl}_2(\mathbb{C}) = \{M^{\#} + M = 0\}$ des matrices de trace nulle (il suffit de différentier l'équation de définition). Ils ont dimension 3-complexe.

Topologie de $\mathrm{SL}_2(\mathbb{C})$. Pour déterminer la topologie de $\mathrm{SL}_2(\mathbb{C})$, notons que les parties réelles et imaginaires du déterminant donnent lieu à une paire de formes quadratiques réelles sur $\mathrm{M}_2(\mathbb{C})$ toutes de même signature $(2, 2)$. Cette dernière peut se lire en développant l'expression usuelle en termes des parties réelles et imaginaires des coefficients de la base standard, ou de manière plus évidente dans notre base favorite. Sa sphère unitaire $\mathrm{SL}_2(\mathbb{C})$ est donc homéomorphe à $(\mathbb{D}^2 \times \mathbb{S}^1) \times (\mathbb{S}^1 \times \mathbb{D}^2)$.

Remarque. *On peut aussi dire $\mathrm{SL}_2(\mathbb{C}) = \mathrm{Spin}(3, 1)$ qui est un revement double de $\mathrm{SO}(4)$ donc est une sphère.*

A Elements d'algèbre linéaire et bilinéaire

Nous ne considérons que des $\mathbb{Z}$-modules libres ou des espaces vectoriels sur $\mathbb{K}$ le corps des réels ou des complexes, et laissons en exercice le loisir d'étendre les notions considérées sur un anneau (commutatif unitaire intègre) quelconque. Rappelons qu'un $\mathbb{Z}$-module libre V donne lieu par extension des scalaires à un espace vectoriel $V(\mathbb{K}) = V \otimes \mathbb{K}$. Réciproquement, le choix d'une base d'un tel espace vectoriel modulo changement de base à coefficients entiers (conjugaison par $\mathrm{GL}_n(\mathbb{Z})$) permet d'en retrouver la structure entière.

A.1 Espaces bilinéaires, involution adjointe, polarization

Modules bilinéaires. Un module bilinéaire sera la donnée d'un module V (sur $\mathbb{Z}$ ou $\mathbb{K}$) muni d'une forme bilinéaire non-dégénérée β. On appelle par exemple (V, β) un module quadratique (sur $\mathbb{Z}$ ou $\mathbb{K}$) lorsque la forme est symétrique, et un module symplectique lorsqu'elle est anti-symétrique ; ces deux notions étant regroupées sous la dénomination de module ϵ-symétrique avec $\epsilon = \pm 1$ respectivement.

Sur un $\mathbb{C}$-espace vectoriel V muni d'une forme β sesquilinéaire hermitienne, on parle de module Hermitien (nous n'imposons pas qu'elle soit un produit scalaire, à savoir définie positive). Notons qu'en restriction au sous espace réel $V_\mathbb{R}$ invariant par conjugaison complexe, la partie réelle de β le munit d'une structure de module quadratique, tandis que sa partie imaginaire celle d'un module symplectique.

Involution d'adjonction. Une forme bilinéaire non-dégénérée $\beta\colon V \times V \to \mathbb{Z}$ sur un $\mathbb{Z}$-module libre permet de l'identifier à son dual $V^* = \mathrm{Hom}(V, \mathbb{Z})$ par la formule $v \mapsto \phi(v) = \beta(v, \cdot)$. L'espace $\mathrm{End}\, V = V^* \otimes V$ est alors muni de l'opérateur adjoint $\mathrm{End}(V) \to \mathrm{End}(V^*) \to \mathrm{End}(V)$ donné par l'échange des facteurs suivi de $\phi \otimes \phi^{-1}$: l'adjoint de $A \in \mathrm{End}(V)$ est donc l'unique $A^* \in \mathrm{End}(V)$ tel que $\beta(v, Aw) = \beta(A^*v, w)$. Tout cela fonctionne également sur $\mathbb{R}$ ou $\mathbb{C}$ par extension des scalaires.

Notons que $*$ définit une involution de l'algèbre $\mathrm{End}(V)$ (toujours sur $\mathbb{Z}$ ou $\mathbb{K}$), c'est-à-dire une symétrie (application linéaire d'ordre deux) qui renverse la multiplication $(AB)^* = B^*A^*$. L'espace $\mathrm{End}(V)$ muni de cette symétrie est alors naturellement décomposé en la somme directe $\mathrm{End}_+(V, \beta) \oplus \mathrm{End}_-(V, \beta)$ de ses sous-espaces propres pour les valeurs ± 1 des endomorphismes autoadjoints $A^* = A$ et anti-autoadjoints $A^* = -A$ selon β. Tout endomorphisme $A \in \mathrm{End}(V)$ se décompose donc de manière unique en la somme de sa partie symétrique $A_+ = (A + A^*)/2$ et antisymétrique $A_- = (A - A^*)/2$, et l'adjoint agit comme $A^* = A_+ - A_-$. Notons que le produit d'éléments ϵ-autoadjoint et ϵ'-autoadjoint est $\epsilon\epsilon'$-autoadjoint (autrement-dit nous avons une décomposition $\mathbb{Z}/2$-graduée pour l'algèbre $\mathrm{End}(V)$), et le sous espace $\mathrm{End}_+(V, \beta)$ est une sous-algèbre.

Par exemple, pour β symétrique définie positive, on retrouve la décomposition en matrices ${}^tA = \pm A$ symétriques et antisymétriques. Pour une forme de signature (p, q), la décomposition est donnée par ${}^tA\, \mathbb{1}_{p,q} = \pm\, \mathbb{1}_{p,q}\, A$. Pour (V, β) hermitienne, la décomposition est analogue. Pour un module symplectique on obtient en posant $S = (I \otimes \mathbb{1}_n)$ les matrices ${}^tAS = \pm AS$. En rang 2, c'est-à-dire pour un plan symplectique, la décomposition correspond à celle des matrices vérifiant $M = \pm M^\#$, ou encore telles que $M^2 = \pm \det(M)$.

Polarisation. Soit (V, β) un module ϵ-symétrique (quadratique ou symplectique), et β' une autre forme bilinéaire ϵ'-symétrique que l'on souhaite exprimer selon β. Notons $\sigma = \epsilon\epsilon'$ mesurant le défaut de symétrie. Alors il existe un endomorphisme $A \in \mathrm{End}^{\sigma}(V, \beta)$ qui est σ-autoadjoint selon β et tel que $\beta'(x, \cdot) = \beta(Ax, \cdot)$. L'endomorphisme A s'appelle une polarisation de β' par rapport à β ; lorsque β' est non dégénéré il est unique et donné par $A = \phi^{-1} \circ \phi'$.

Sur un module Euclidien (quadratique défini positif), on retrouve la représentation usuelle des formes quadratiques par des endomorphismes symétriques. Sur un module symplectique (V, ω) de rang 2, et pour toute forme quadratique Q non dégénérée, il existe un unique endomorphisme de trace nulle $s \in \mathfrak{sl}_2(\mathbb{Z})$ tel que $Q(x, y) = \det(x, sy)$. Un analogue est vrai sur (V, β) hermitien.

Pour une application plus abstraite, rappelons qu'une structure hermitienne sur un espace complexe V induit des structures quadratique et symplectique sur l'espace réel $V_{\mathbb{R}}$ sous-jacent : montrons la réciproque. Si V est un espace vectoriel réel muni d'une structure quadratique α et symplectique ω, alors la polarisation de ω par rapport à α fournit un endomorphisme (unique car α est aussi non dégénérée) $I \in \mathrm{End}(V_{\mathbb{R}})$ telle que $\phi_\alpha = \phi_\omega \circ I$ c'est-à-dire $\alpha(x, y) = \omega(Ix, y)$. On vérifie sans peine l'identité $I^2 = -\mathbb{1}$ caractérisant les structures complexes ; et nous avons donc montré l'équivalence souhaitée (et l'unicité de la structure complexe polarisant ω pour α).

Classifications. Pour finir, rappelons que sur $\mathbb{K}$ (un corps pour lequel $\mathbb{K}^*/(\mathbb{K}^*)^2$ est fini), il n'y a qu'un nombre fini de classes d'isomorphisme d'espaces quadratiques. Sur les réels ils sont donnés par sa signature (p, q), tandis que sur les complexes il n'y n a qu'un seul. De même les espaces hermitiens sont caractérisés par la signature. Il n'y a qu'un seul module symplectique (entier réel ou complexe), à dilatation par un facteur près. Sur les entiers, il y a beaucoup de modules quadratiques.

A.2 Algèbre des endomorphismes

Endomorphismes normaux. Les sous espaces d'un endormorphisme autoajoint ou anti-auto-adjoint sont orthogonaux. Plus généralement, un endormorphisme vérifiant cette propriété est appelé normal, et cela équivaut à dire A et A^* commutent. (En effet, A et A^* commutent lorsque A_+ et A_- commutent, ce qui arrive lorsque chacun préserve les sous espaces propres de l'autre, donc quand les sous espaces propres de A subdivisent ceux de A_+ et A_-.) Ainsi, A est normal lorsque $A^*A = A_+^2 - A_-^2$.

Forme de Killing. L'involution adjointe permet de définir une forme bilinéaire non dégénérée sur $\mathrm{End}(V)$, par la formule $\kappa(A, B) = \mathrm{tr}(A^*B)$, nomée d'après Killing. Comme la norme associée vaut $\mathrm{N}(A) = \mathrm{tr}(A_+^2) - \mathrm{tr}(A_-^2)$, la décomposition $\mathrm{End}_+(V, \beta) \oplus \mathrm{End}_-(V, \beta)$ lui est orthogonale. C'est en quelque sorte la norme associé à β : pour β un produit scalaire euclidien ou hermitien, on retrouve la norme quadratique des opérateurs, et pour une forme symplectique du plan on retrouve le déterminant.

Remarquons qu'il est naturel de considérer le plongement de V dans $\mathrm{End}(V) = V^* \otimes V$ par l'application $v \mapsto \beta(v, \cdot) \otimes v$, qui a un vecteur v associe la « projection orthogonale renormalisée » p_v sur la droite qu'il dirige. Comme p_v est autoadjoint et $p_v^2 = \beta(v, v)p_v$, on a $\mathrm{N}(p_v) = \beta(v, v)\,\mathrm{tr}(p_v) = \beta(v, v)^2$. De même $\kappa(p_v, p_w) = \beta(w, v)^2$. Par conséquent, nous avons un plongement non pas isométrique mais homogène de degré 2 entre les modules bilinéaires (V, β) et $(\mathrm{End}(V), \kappa)$.

Automorphismes. Le groupe $\mathfrak{G} = \mathrm{Aut}(\beta)$ des automorphismes linéaires de V préservant la forme β est un groupe de Lie. Il est constitué des éléments $A \in \mathrm{End}(V)$ tels que pour tout $v, w \in V$ on ait $\beta(v,w) = \beta(Av, Aw)$ donc $\beta(v, A^*Aw) = \beta(v,w) = \beta(A^*Av, w)$, ce qui revient à demander $A^*A = \mathbb{1}$ par non dégénérescence de β. Son algèbre de Lie $\mathfrak{g}$ correspond donc aux solutions de l'équation linéarisée $A^* + A = 0$ t coincide donc avec l'espace $\mathrm{End}_-(V)$ des endomorphisme anti-autoadjoints.

Le groupe de Lie est défini par l'annulation d'un certain nombre de formes quadratiques (autant que $\dim \mathrm{End}_+(V,\beta)$), c'est donc une intersection de quadriques, ce qui informe sur sa nature topologique, algébrique et dynamique. Il en est de même pour son intersection avec l'algèbre de Lie.

L'intersection de l'algèbre de Lie avec le groupe de Lie est formé des endomorphismes tels que $A^* + A = 0$ et $A^*A = \mathbb{1}$, ce qui implique $A^2 = -\mathbb{1}$ et deux relations déterminent la troisième. En particulier on travaille souvent dans l'espace vectoriel $\mathfrak{g} = \mathrm{End}_-(V,\beta)$ muni de la restriction de la norme $N(A) = \mathrm{tr}(A^*A) = -\mathrm{tr}(A^2)$, que l'on appelle la forme de Killing (et qui est l'unique forme quadratique non dégénérée invariante par). Dans cet espace, on repère donc les éléments du groupe comme ceux qui vérifient $A^2 = -\mathbb{1}$.

Espace symétrique BLABLABLA

Décomposer une forme linéaire comme la somme d'un partie symétrique et antisymétrique par rapport à β, puis polariser l'espace des formes β' ayant le même type de symétrie que β ou le type opposé.

B Discussions arithmétiques

B.1 Classification des extensions matricielles sur l'anneau des entiers

Soit $M \in \mathrm{M}_2(\mathbb{R})$, non scalaire pour qu'elle engendre une extension non triviale. D'après le théorème de Cayley-Hamilton, elle est annulé par son polynôme caractéristique, qui est donc son polynôme minimal, et l'algèbre $\mathbb{R}[M]$ est isomorphe au quotient $\mathbb{R}[X]/\left(X^2 - \mathrm{tr}(M)X - \det(M)\right)$. Notons que dans le cas présent, les relations $\mathrm{tr}(M) = M + M^\#$, et $\det(M) = MM^\#$ rendent cette identité $M^2 - (M + M^\#)M + MM^\# = 0$ évidente. La nature de $\mathbb{R}[M]$ à isomorphisme de $\mathbb{R}$-algèbres près dépend des propriétés de factorisations sur $\mathbb{R}$ du polynôme annulateur de M, dont le nombre de racines dépend uniquement de la valeur de son discriminant $\Delta = \mathrm{tr}^2(M) - 4\det(M)$ dans $\mathbb{R}/(\mathbb{R}^*)^2$, soit encore dans l'ensemble $\{-1, 0, 1\}$.

Si $\Delta = 0$, il a une racine réelle double α donc $(M - \alpha)^2 = 0$ et le changement de variables $M' = M - \alpha\,\mathbb{1}$ donne $\mathbb{R}[M']$ isomorphe à $\mathbb{R}[X]/(X^2)$. Si $\Delta < 0$, il a deux racines complexes conjuguées distinctes α, α^* donc $M - \Re(\alpha)M + (\Re(\alpha)^2 + \Im(\alpha)^2) = 0$ et en complétant le carré, on constate que le changement de variables $M' = (M - \Re(\alpha)/2) \div \Im(\alpha)/2$ donne $\mathbb{R}[M'] \simeq \mathbb{R}[X]/(X^2 - 1)$. Si $\Delta > 0$, il a deux racines réelles distinctes α, α' donc $(M - \alpha)(M - \alpha') = 0$ et le changement de variables $M' = (M - \frac{1}{2}(\alpha + \alpha')) \div \frac{1}{2}(\alpha - \alpha')$ donne $\mathbb{R}[M'] \simeq \mathbb{R}[X]/(X^2 - 1)$.

B.2 Formes quadratiques

B.3 Algèbres de quaternions sur les entiers

Notons que l'algèbre des quaternions est définie sur $\mathbb{Z}$: dans ces définitions, toutes les équations sont unitaires et à coefficients entiers ; on peut donc définir une $\mathbb{Z}$-algèbre des entiers de Hamilton $\mathbb{H}(\mathbb{Z})$, dont l'algèbre des quaternions est le produit tensoriel $\mathbb{H} = \mathbb{H}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R}$.

C Equations différentielles et quaternions

C.1 Equations de Cauchy-Riemann

C.2 Equations de Maxwell

C.3 Equations d'Euler

Références

[1] R. Penrose, *The road to reality (a complete guide to the laws of the universe)*, Jonathan Cape London, 2004.

[2] M.-F. Vigneras, *Arithmétique des algèbres de quaternions*, Springer, 1980.