Agrégation interne. Cours P. Caldero.
Algèbre et géométrie.

# LA FAUTE A DESCARTES

En bons disciples de Descartes que nous sommes, nous cherchons à coder les objets mathématiques afin de les traiter à l'aide d'outils de calcul. C'est un programme très fécond, mais qui pose un problème de poids : le choix que l'on fait au moment du codage. Par exemple, lorsqu'on veut faire de la géométrie plane, on code les points en coordonnées, mais pour cela, on choisit un repère et ce choix est souvent déterminant. Tout mathématicien sait, parfois même jusqu'à la névrose, que tout choix se paye à un moment ou à un autre, en tout cas dans les problèmes théoriques. C'est pour cela, dans un même ordre d'idée que l'on préfére les énoncés du type "il existe un unique" que seulement "il existe". Dans le texte qui suit, nous exposons trois exemples classiques de codages. On introduira la notion d'invariant afin d'unifier les trois exemples dans un survol du programme d'algèbre linéaire.

Tous les espaces vectoriels seront supposés de dimension finie sur un corps $\mathbb{K}$. Les résultats qui suivent sont à bien connaître, et on notera l'influence de la nature du corps sur les résultats.

## 1 Applications linéaires.

Soit $\phi$ une application linéaire d'un espace vectoriel $E$ vers un espace vectoriel $F$ de dimensions respectives $m$ et $n$. L'application $\phi$ peut être "codée" en un nombre fini de données. Soit $\underline{e} := (e_j)_{1\leq j\leq m}$ une base de $E$ et $\underline{f} := (f_i)_{1\leq j\leq n}$ une base de $F$. On va coder $\phi$ à l'aide de la matrice $m\times n$ $\mathrm{Mat}_{\underline{e},\underline{f}}(\phi)$ donnée par [1]

$$\boxed{\text{CODAGE : } \mathrm{Mat}_{\underline{e},\underline{f}}(\phi) := (a_{ij}), \text{ avec } \phi(e_j) = \textstyle\sum_i a_{ij} f_i}$$

Comme on dit dans les milieux rapaces, il ne faut pas lacher la proie pour l'ombre : le bon objet est l'application linéaire, la matrice n'est que le moyen de l'étudier. On arrive naturellement à la question suivante :

$$\boxed{\text{QUESTION : A quelle condition deux matrices codent la même application linéaire?}}$$

[1]Pourquoi cette définition est-elle sans ambiguïté?

Le mot "même" suggère une relation d'équivalence : on dit que deux matrices $m \times n$ $A$ et $B$ sont équivalentes (pas très original!) si $A = \mathrm{Mat}_{\underline{e},\underline{f}}(\phi)$ et $B = \mathrm{Mat}_{\underline{e}',\underline{f}'}(\phi)$ pour des bases $\underline{e}$, $\underline{e}'$ de $E$, $\underline{f}$, $\underline{f}'$, de $F$ et une application linéaire $\phi$ de $E$ vers $F$. On notera $A \sim B$. Cette définition est, je le rappelle naturelle et même fondamentale, mais on a besoin de la formuler de facon plus concrète. On le fait grâce aux fameuses matrices de passage. Dans la suite $P$ représente la matrice de passage de $\underline{e}$ vers $\underline{e}'$ et $Q$ celle de $\underline{f}$ vers $\underline{f}'$.

$$\boxed{A \sim B \Leftrightarrow B = Q^{-1}AP,\ P \in \mathrm{GL}(E),\ Q \in \mathrm{GL}(F)}$$

Attention, on a répondu à la question, mais ce n'est pas gagné car pour voir que deux matrices $A$ et $B$ sont équivalentes, il faut résoudre l'équation $B = Q^{-1}AP$, d'inconnues $Q$ et $P$, c'est à dire que l'on doit résoudre un systeme à $m^2 + n^2$ inconnues. Cette formulation calculatoire de l'équivalence est utile dans certains problèmes mais n'est pas encore satisfaisante. On va introduire pour cela la notion d'*invariant*. Un invariant est un objet que l'on peut associer à une classe d'équivalence, en fait il ne varie pas selon l'élément choisi dans sa classe.
Soit $f$ une application de l'ensemble des matrices $m \times n$ vers un ensemble quelconque. C'est un invariant si

$$\boxed{f \text{ est un invariant : } A \sim B \Rightarrow f(A) = f(B)}$$

$$\boxed{f \text{ est un invariant total : } A \sim B \Leftrightarrow f(A) = f(B)}$$

Le but du jeu est maintenant clair : trouver un invariant total pour la relation $\sim$ et un algorithme de calcul de cet invariant. La réponse est la suivante :

$$\boxed{\text{Le rang est un invariant total pour } \sim \text{ sur } M_{m,n}(\mathbb{K})}$$

Dit autrement, deux matrices sont équivalentes si et seulement si elles ont même rang et ce, *sur n'importe quel corps* . Le fait que le rang soit un invariant est une chose simple : on ne change pas le rang en multipliant par une matrice inversible à droite ou à gauche. La réciproque est un peu plus dure : c'est un théorème que l'on trouve dans tout bon livre d'algèbre linéaire et qui utilise de facon essentielle le théorème de la base incomplète. Le rang a en plus l'avantage de se calculer facilement à l'aide de mineurs, ou surtout d'une méthode de type pivot.

# 2 Endomorphismes.

La section qui suit est sur la même trame. On ramène la problématique du codage des endomorphisme à un problème d'invariant. Mais le théorème qui donne l'invariant total est en bordure de programme (les fameux invariants de similitudes).
Soit $\phi$ un endomorphisme d'un espace vectoriel $E$ (vers lui-même donc) de dimension $n$. L'application $\phi$ peut encore être "codée" en un nombre fini de données. Soit $\underline{e} := (e_j)_{1 \leq j \leq m}$ une base de $E$. On va coder $\phi$ à l'aide de la matrice $n \times n$ $\mathrm{Mat}_{\underline{e}}(\phi)$ donnée par

$$\boxed{\text{CODAGE : } \mathrm{Mat}_{\underline{e}}(\phi) := (a_{ij}), \text{ avec } \phi(e_j) = \sum_i a_{ij} e_i}$$

On constate que la seule vraie différence avec le chapitre précédent est que cette fois-ci, on s'impose que les bases $\underline{e}$ et $\underline{f}$ sont identiques, ce qui promet un problème plus difficile. On arrive ainsi à la question suivante :

$$\boxed{\text{QUESTION : A quelle condition deux matrices codent le même endomorphisme?}}$$

On définit alors une relation d'équivalence : on dit que deux matrices $n \times n$ $A$ et $B$ sont semblables si $A = \mathrm{Mat}_{\underline{e}}(\phi)$ et $B = \mathrm{Mat}_{\underline{e}'}(\phi)$ pour des bases $\underline{e}$, $\underline{e}'$ de $E$, et un endomorphisme $\phi$ de $E$. On notera $A \simeq B$.
Dans la suite $P$ représente la matrice de passage de $\underline{e}$ vers $\underline{e}'$.

$$\boxed{A \simeq B \Leftrightarrow B = P^{-1}AP,\ P \in \mathrm{GL}(E)}$$

Pour voir que deux matrices $A$ et $B$ sont semblables, il faut résoudre l'équation $B = P^{-1}AP$, d'inconnue $P$, c'est à dire que l'on doit résoudre un système à $n^2$ inconnues. Encore une fois, on va devoir chercher des invariants. Encore une fois, il faut trouver un invariant total pour la relation $\simeq$ et un algorithme de calcul de cet invariant. Mais le problème est que la réponse réside dans les invariants de similitudes et ceux-ci sont hors programme. Il va falloir bricoler. On va donc d'une part chercher des invariants (non totaux) sur $M_n(\mathbb{K})$, d'autre part, chercher une partie "assez grande" de $M_n(\mathbb{K})$ sur laquelle on peut définir un invariant total.

Voici quelques invariants. Il est vivement conseillé de chercher des preuves des faits qui suivent.

$$\boxed{\text{Le rang est un invariant pour } \simeq \text{ sur } M_n(\mathbb{K})}$$

$$\boxed{\text{Le polynôme caractéristique est un invariant pour } \simeq \text{ sur } M_n(\mathbb{K})}$$

$$\boxed{\text{Le spectre est un invariant pour } \simeq \text{ sur } M_n(\mathbb{K})}$$

$$\boxed{\text{Le polynôme minimal est un invariant pour } \simeq \text{ sur } M_n(\mathbb{K})}$$

Dit autrement, deux matrices sont semblables ont même rang, le même polynôme caractéristique, le même spectre (ensemble des valeurs propres avec multiplicités), le même polynôme minimal et ce, *sur n'importe quel corps* . La propriété sur le rang est une consequence immédiate du chapitre qui précède, et les autres propriétés découlent des propriétés de base du déterminant. Le déterminant se calcule à l'aide d'algorithmes comme par exemple le developpement par rapport à une ligne ou une colonne. Malheureusement, ces invariants, même à eux quatre, ne consituent pas un invariant total, comme l'indique le contre-exemple

ci-dessous :
**Contre-exemple.** On considère les matrices $A$ et $B$ suivantes

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \ B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

On calcule "facilement" le rang, le polynôme caractéristique, le spectre et le poynôme minimal de $A$ et $B$ : que

$$\mathrm{rg}(A) = 4 = \mathrm{rg}(B),\ \chi_A = (X-1)^4 = \chi_B,\ \mathrm{Spec}(A) = (1,1,1,1) = \mathrm{Spec}(B),\ \mu_A = (X-1)^2 = \mu_B.$$

Pourtant, $A$ et $B$ ne sont pas semblables. Montrons le : si $A$ et $B$ étaient semblables, alors on aurait une matrice $P$ inversible telle que $B = P^{-1}AP$. Cela impliquerait $B - Id = P^{-1}(A - Id)P$, donc que $A - Id$ et $B - Id$ sont semblables et ont donc ont même rang. Or, on vérifie que $\mathrm{rg}(A - Id) = 2 \neq 3 = \mathrm{rg}(B - Id)$.

Notons $D_n(\mathbb{K})$ l'ensemble des matrices diagonalisables de $\mathbb{K}$. C'est effectivement une partie assez grande de $M_n(\mathbb{K})$ : par exemple, si $\mathbb{K} = \mathbb{C}$ alors, on sait que $D_n(\mathbb{C})$ est une partie dense de $M_n(\mathbb{C})$ pour sa topologie d'espace vectoriel normé.

$$\boxed{\text{Le polynôme caractéristique est un invariant pour } \simeq \text{ sur } D_n(\mathbb{C})}$$

Cela se prouve facilement : soient $A$ et $B$ deux matrices diagonalisables complexes. Si elles ont même polynôme caractéristique, elle ont même spectre, et comme elles sont toutes deux diagonalisables, elles sont toutes deux équivalentes à une matrice diagonale donnée par leur spectre. Comme elles sont semblables à une matrice commune, elles sont semblables entre elles.
On montre aussi que

$$\boxed{\text{Le polynôme caractéristique est un invariant pour } \simeq \text{ sur } D_n(\mathbb{R})}$$

Pour cela, il suffit de voir que deux matrices réelles ayant même polynôme caractéristique sont semblable sur $\mathbb{C}$ s'après ce qui précède. Or, un théorème (une belle application de la polynomialite du déterminant!) dit que deux matrices réelles semblables sur $\mathbb{C}$ sont semblables sur $\mathbb{R}$.
Il est toujours frustrant de terminer une section sans avoir achevé le problème que l'on s'était proposé. On l'a résolu le problème des invariants totaux pour les matrices diagonalisables. La décomposition de Dunford suggère de faire l'étude des invariants sur les matrices nilpotentes.

# 3 Formes quadratiques.

L'étude des formes quadratiques revient à l'etude des équations du second degré (á plusieurs variables). En caractéristique différente de 2, on s'aide de l'étude de la forme bilinéaire associée. L'étude est simple sur $\mathbb{C}$, plus ardue sur $\mathbb{R}$, pas si dure sur les corps finis (mais hors programme), complètement hors de portée sur $\mathbb{Q}$. Bref, l'importance du corps est capitale.

Soit $q$ une forme quadratique sur un espace vectoriel $E$ de dimension finie $n$ et $\phi$ la forme bilinéaire associée, *i.e.* $\phi(u, v) = 1/2(q(u + v) - q(u) - q(v))$. La forme $q$ peut alors être "codée" en un nombre fini de données. Soit $\underline{e} := (e_j)_{1 \leq j \leq m}$ une base de $E$. On va coder $q$ à l'aide la matrice $n \times n$ $\mathrm{Mat}_{\underline{e}}(q)$ donnée par

$$\boxed{\text{CODAGE : } \mathrm{Mat}_{\underline{e}}(q) := (a_{ij}),\text{ avec } \phi(e_i, e_j) = a_{ij}}$$

On arrive toujours à la même question :

$$\boxed{\text{QUESTION : A quelle condition deux matrices codent la même forme quadratique?}}$$

On dira que deux matrices $n \times n$ $A$ et $B$ sont congruentes si $A = \mathrm{Mat}_{\underline{e}}(q)$ et $B = \mathrm{Mat}_{\underline{e}'}(q)$ pour des bases $\underline{e}$, $\underline{e}'$ de $E$, et une forme quadratique $q$ de $E$. On notera $A \equiv B$.
Dans la suite $P$ représente la matrice de passage de $\underline{e}$ vers $\underline{e}'$.

$$\boxed{A \equiv B \Leftrightarrow B =^t PAP,\ P \in \mathrm{GL}(E)}$$

Encore une fois, il faut résoudre l'équation $B =^t PAP$, d'inconnue $P$, c'est à dire que l'on doit résoudre un système a $n^2$ inconnues. On repart donc sur la recherche d'invariants.

$$\boxed{\text{Le rang est un invariant pour } \equiv \text{ sur } M_n(\mathbb{K})}$$

Cela provient toujours du fait qu'on ne change pas le rang en multipliant à droite ou à gauche par une matrice inversible.

Sur $\mathbb{C}$, et en fait plus généralement sur un corps algébriquement clos, on a la réciproque:

$$\boxed{\text{Le rang est un invariant total pour } \equiv \text{ sur } M_n(\mathbb{C})}$$

Dit autrement, deux matrices sont congruentes sur $\mathbb{C}$ si et seulement si elles ont même rang . C'est un théorème que l'on trouve aussi dans tout bon livre d'algèbre linéaire et qui utilise une récurrence sur la dimension, on se ramène de $n$ a $n + 1$ en utilisant l'orthogonal pour la forme bilinéaire et le fait que tout nombre complexe est un carré. Il est peut etre utile de rappeler qu'un nombre réel est un carré ssi il est positif, donc sur $\mathbb{R}$ deux réels sont égaux modulo un carré si et seument si ils sont de même signe. Sur $\mathbb{C}$, tous les complexes sont égaux modulo un carré, donc le discriminant ne discrimine rien!.

Sur $\mathbb{R}$ le rang ne suffit pas, comme le montre le contre-exemple suivant (pas la peine d'aller chercher loin en fait)

**Contre-exemple.** Soit$A$ et $B$ les matrices réelles :

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Tout d'abord $A$ et $B$ ont même rang égal a 2 (elles sont donc congruentes sur $\mathbb{C}$). Maintenant, supposons que $A$ et $B$ sont congruentes sur $\mathbb{R}$, alors il existe une matrice inversible *réelle* $P$ telle que $B =^t PAP$, et donc $\det B = \det({}^tPAP) = \det({}^tP)\det(A)\det(P) = \det(P)^2\det(A)$. Or, $\det(A) = 1$ et $\det(B) = -1$, cela donne $\det(P)^2 = -1$, ce qui est impossible car $P$ est réelle.

Cela suggère un nouvel invariant : on dit que $A$ et $B$ ont même *discriminant* si elles ont même determinant modulo un carré. et exemple se généralise aisément pour donner

$$\boxed{\text{Le discriminant est un invariant pour } \equiv \text{ sur } M_n(\mathbb{K})}$$

Il est intéressant de comprendre quel est le lien entre cette définition du discriminant et la définition du discriminant de l'équation du second degré. Voici une réponse : l'équation du second degré est l'équation $ax^2+bx+c = 0$ ou $a \neq 0$. On voit facilement que la résoudre dans $\mathbb{R}$ (mais ça marche aussi sur un corps quelconque) revient à résoudre l'équation homogène $ax^2 + bxy + cy^2 = 0$ dans $\mathbb{R}^2$, ou pour être plus précis, il y a correspondance bijective entre les points solutions de la première avec les droites solutions de la seconde. Cela revient donc à étudier la forme quadratique $q((x, y)) = 2ax^2 + 2bxy + 2cy^2 = 0$, et dans la base canonique de $\mathbb{R}^2$ sa matrice est donnée par

$$A = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}.$$

Le discriminant revient à regarder si le déterminant de cette matrice est ou non un carré, c'est à dire si $4ac - b^2$ est ou non un carré. On retrouve, au signe près, le bonne vieille problématique du discriminant de seconde.
Le discriminant est bien pratique quand on en reste aux matrices réelles $2 \times 2$ et c'est même un invariant total si on en reste aux matrices $2 \times 2$ inversibles, mais ce n'est pas un invariant total si on passe aux matrices $3 \times 3$. Voici un contre-exemple :

**Contre-exemple.** Soit$A$ et $B$ les matrices réelles :

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Tout d'abord $A$ et $B$ ont même rang égal a 3. De plus, $\det(A) = -1$ et $\det(B) = -1$, les déterminants sont bien égaux modulo le carré 1.

Pourtant elles ne sont pas congruentes, pour des raisons un peu plus subtiles. Supposons que $A$ et $B$ codent la même forme quadratique $q$, alors en regardant la matrice $A$, on voit que $q((x, y, z) = -x^2 - y^2 - z^2$, et donc $-q$ est une forme définie positive, c'est à dire que tout $q(v)$ est strictement négatif sauf pour $v = 0$. En regardant la matrice $B$ on voit que les deux premiers vecteurs de la base dans laquelle $B$ est codée sont positifs pour $q$. Absurde.

Cela donne l'idée d'un autre invariant : soit $s$ la dimension maximale d'un sous-espace de $E$ sur laquelle $q$ est positive et soit $t$ la dimension maximale d'un sous-espace de $E$ sur laquelle $q$ est négative. Alors, $(s, t)$ est appelée *signature* de $q$. Par exemple, dans l'exemple qui précède, la forme quadratique que code $A$ est de signature $(0, 3)$ (rappelant la victoire de l'équipe de France en 1998), alors que pour $B$ la signature est $(2, 1)$ (rappelant sa défaite en 2006 et le coup de boule de Zizou). Le théorème d'inertie de Sylvester assure que nous sommes tombés sur le bon invariant :

$$\boxed{\text{Le rang et la signature constituent un invariant total pour } \equiv \text{ sur } M_n(\mathbb{R})}$$

Essayons d'en donner une application concrète. Si on veut résoudre l'équation du second degré à trois variables dans $\mathbb{R}$ $q(u) = a$, $u \in \mathbb{R}^3$, où $q$ est de rang 3 (non dégénérée). Alors les cas possibles, quitte à effectuer un changement de variables linéaires (=changement de base), on se ramène a une et une seule des équations suivantes :

$$X^2 + Y^2 + Z^2 = a \ (3, 0), \ X^2 + Y^2 - Z^2 = a \ (2, 1),$$

$$X^2 - Y^2 - Z^2 = a \ (1, 2), \ -X^2 - Y^2 - Z^2 = a \ (0, 3).$$

Il y a donc quatre cas non dégénérés, là ou il y en avait deux en dimension 2 (disciminant positif ou discriminant négatif). Si $a$ est strictement positif, alors cela signifie, qu'après changement de variable linéaire, l'ensemble des solutions est soit une sphère, une hyperboloïde à une nappe, une hyperboloïde à deux nappes, voir Figures 1 et 2, ou l'ensemble vide pour le dernier cas.

On peut regarder les inégalités remarquables sous l'angle du théorème de Sylvester. Par exemple, l'hyper-célèbre différence de deux carrés :

$$x^2 - y^2 = (x - y)(x + y)$$

A l'aide du changement de variables linéaire $X = x - y$, $Y = x + y$, on voit que l'on peut passer de la forme quadratique de $\mathbb{R}^2$ $x^2 - y^2$ à la forme quadratique $XY$ via un changement de variables linéaires. Cela implique qu'elles doivent avoir même rang et même signature. Effectivement, elles ont pour matrice respectivement $A$ et $B$ avec

$$A := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ B := \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}.$$

Il est facile de voir que leur rang et leur signature sont égaux (par exemple en calculant leurs valeurs propres, qui sont réelles, et en regardant leurs signes) : $r = 2$, $(s, t) = (1, 1)$.

On peut aussi regarder aussi la non moins célèbre égalité :

$$x^2 + 2xy + y^2 = (x + y)^2$$

A l'aide du changement de variables linéaire $X = x + y$, on voit que l'on peut passer de la forme quadratique de $\mathbb{R}^2$ $x^2 + 2xy + y^2$ à la forme quadratique $X^2$ via un changement de variables linéaires. Cela implique qu'elles doivent avoir même rang et même signature. Effectivement, elles ont pour matrice respectivement $A'$ et $B'$ avec

$$A' := \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \ B := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Il est facile de voir que leur rang et leur signature sont égaux : $r = 1$, $(s, t) = (1, 0)$.

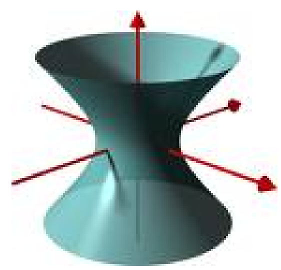

Figure 1: Hyperboloïde à une nappe

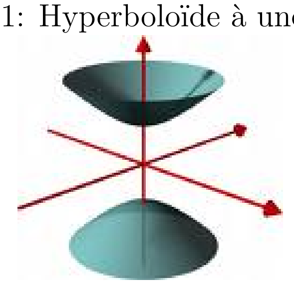

Figure 2: Hyperboloïde à deux nappes