Leçons 158 et 170

Stéphane Lamy

Lundi 12 novembre

Table des matières

Développements discutés lors de la séance

Réduction des endomorphismes auto-adjoints et décomposition polaire

[CG13, p. 162 & p. 201], [RW07, p. 196], [Szp09, p. 342], [Gou09, p. 240] voir aussi pdf d'Antoine Ducros

Leçons :

- 106. Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E). Applications
- 108. Exemples de parties génératrices d'un groupe. Applications

Peut-être un peu osé, mettre la décomposition polaire en avant...

- 155. Endomorphismes diagonalisables en dimension finie

Les matrices symétriques sont diagonalisables dans une base orthonormée, et à valeurs propres réelles.

- 158. Matrices symétriques réelles, matrices hermitiennes
- 160. Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie)
- 161. Distances et isométries d'un espace affine euclidien

Lemme. *Une matrice A hermitienne (et donc en particulier une matrice symétrique réelle) a toutes ses valeurs propres réelles.*

Preuve. Soit $\lambda \in \mathbb{C}$ une valeur propre de A, et v un vecteur propre. On note $\langle \cdot, \cdot \rangle$ le produit hermitien standard sur $\mathbb{C}^n$. On a

$$\lambda\langle v, v\rangle = \langle v, \lambda v\rangle = \langle v, Av\rangle = \langle A^* v, v\rangle = \langle Av, v\rangle = \langle \lambda v, v\rangle = \bar{\lambda}\langle v, v\rangle,$$

d'où $\lambda = \bar{\lambda}$ comme attendu. □

Théorème. *Soit $E, \langle \cdot, \cdot \rangle$ un espace euclidien (resp. hermitien), et $f : E \to E$ un endomorphisme auto-adjoint. Alors il existe une base orthonormée de vecteurs propres de f, et les valeurs propres de f sont réelles.*

Preuve. On procède par récurrence sur la dimension n de E, le cas $n = 1$ étant clair. Supposons le résultat acquis pour les espaces de dimension $n - 1$. Soit λ une valeur propre de f, par le lemme $\lambda \in \mathbb{R}$. Soit e_1 un vecteur propre associé à λ, on peut supposer e_1 de norme 1. Notons $H \subset E$ l'orthogonal de e_1, et $e_2, \cdots, e_n$ une base orthonormée quelconque de H. La matrice de f dans la base $(e_1, \cdots, e_n)$ est symétrique (resp. hermitienne), et diagonale par bloc (car $\operatorname{Vect} e_1$ invariant par f implique $e_1^\perp$ invariant par f), d'où l'on tire que la matrice de $f|_H$ dans la base $(e_2, \cdots, e_n)$ est également symétrique (resp. hermitienne). Par hypothèse de récurrence on peut choisir la base $(e_2, \cdots, e_n)$ formée de vecteurs propres, ce qui termine la preuve. □

Corollaire. *Toute matrice M symétrique (resp. hermitienne) positive admet une unique racine carrée, i.e. une matrice symétrique (resp. hermitienne) positive N tel que $N^2 = M$.*

Preuve. Par le théorème on peut écrire $M = PDP^{-1}$ où $D = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$ et $P^{-1} = P^t$. Alors $N = P\sqrt{D}P^{-1}$ convient, où $\sqrt{D} := \mathrm{diag}(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_n})$.

Pour l'unicité, supposons que $N^2 = M$, avec N positive, et considérons une base de vecteurs propres pour N. Dans cette base, M est également diagonale, de la forme $\mathrm{diag}(\lambda_1, \dots, \lambda_n)$ avec les $\lambda_i \geqslant 0$. Cela implique que dans cette base $N = \mathrm{diag}(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_n})$. □

Remarque. On trouve dans la littérature agrégative ([Gou09]...) des preuves excessivement longues et poussives des résultats précédents.

Théorème (Décomposition polaire, [RW07, p. 302], [CG13, p. 202], [MT86, p. 19])**.** *Si $A \in \mathrm{GL}_n(\mathbb{R})$, il existe O orthogonale et S symétrique définie positive uniques tel que $A = OS$. Plus précisément la multiplication matricielle induit un homéomorphisme*

$$\begin{array}{rccc} \mu\colon & \mathrm{O}(n,\mathbb{R}) \times S_n^{++}(\mathbb{R}) & \to & \mathrm{GL}_n(\mathbb{R}) \\ & (O \quad , \quad S) & \mapsto & OS \end{array}$$

Preuve. Si $A = OS$, $A^t = SO^{-1}$ et $A^tA = S^2$. Donc S est l'unique racine carrée de la matrice symétrique définie positive A^tA, et $O = AS^{-1}$ vérifie bien $O^t = O^{-1}$. Ceci montre que μ est surjective (car O et S existent) et injective (car S, et donc aussi O, sont uniquement déterminés).

L'application μ est clairement continue, reste à voir que la réciproque μ^{-1} est également continue. Soit (A_p) une suite de $\mathrm{GL}_n(\mathbb{R})$ qui converge vers A, et notons $A_p = O_pS_p$ la décomposition polaire de A_p. Comme $\mathrm{O}_n(\mathbb{R})$ est compact, pour toute valeur d'adhérence O de la suite (O_p) il existe une sous-suite (O_{p_i}) qui converge vers la matrice O. Alors la sous-suite S_{p_i} converge vers $S := O^{-1}A$, et cette matrice est symétrique définie positive car

$$O^{-1}A \in \mathrm{GL}_n(\mathbb{R}) \cap \overline{S_n^{++}(\mathbb{R})} = \mathrm{GL}_n(\mathbb{R}) \cap S_n^{+}(\mathbb{R}) = S_n^{++}(\mathbb{R}).$$

Ainsi (O, S) est un antécédent de A par μ, par injectivité de μ on conclut que O est la seule valeur d'adhérence de (O_p) qui est donc convergente, et finalement la suite (S_p) est elle aussi convergente vers S, comme attendu. □

Remarque. De la même manière on prouve qu'il existe un homéomorphisme

$$\begin{array}{rccc} \mu\colon & \mathrm{U}(n,\mathbb{C}) \times H_n^{++}(\mathbb{C}) & \to & \mathrm{GL}_n(\mathbb{C}) \\ & (U \quad , \quad H) & \mapsto & UH \end{array}$$

Corollaire ([CG13, p. 204])**.** *Pour tout $A \in \mathrm{GL}_n(\mathbb{R})$, on a $\|A\| = \sqrt{\rho(A^tA)}$*

Preuve. Pour S symétrique, en diagonalisant en base orthonormée, on trouve $\|S\| = \rho(S)$. Maintenant on écrit une décomposition polaire $A = OS$, et on trouve d'une part $\|A\| = \|S\|$, et d'autre part

$$\|S\| = \rho(S) = \sqrt{\rho(S^2)} = \sqrt{\rho(A^tA)}.$$ □

On peut simplifier encore un peu la décomposition polaire grâce à la

Proposition ([CG13, p. 208])**.** *L'application* $\exp\colon S_n(\mathbb{R}) \to S_n^{++}(\mathbb{R})$ *est un homéomorphisme, et en particulier $S_n^{++}(\mathbb{R}) \simeq \mathbb{R}^{n(n+1)/2}$.*

Preuve. Le fait que $\exp(S_n(\mathbb{R})) = S_n^{++}(\mathbb{R})$ se voit en diagonalisant en base orthornormée. Pour l'injectivité, on peut montrer à l'aide de polynômes interpolateurs de Lagrange que A est un polynôme en $\exp A$ (NB : il est vrai aussi que $\exp A$ est un polynôme en A, mais ça ne semble pas suffir ici), ainsi si $\exp A = \exp A'$ elle est simultanément diagonalisable avec A et A', et les coefficients diagonaux de $A = A'$ sont uniquement déterminés. Reste à voir la continuité de l'inverse : si $B_p = \exp A_p$ converge vers $B = \exp A$, montrons que $A_p \to A$. Comme les B_p convergent et sont définies positives, leur spectre est contenu dans un compact $K = [C', C] \subset]0, +\infty[$ indépendant de p. On en déduit la même propriété pour le spectre des A_p, avec le compact $[\ln C', \ln C]$. Par le corollaire la suite A_p est donc de norme bornée. On termine en constatant que A est la seule valeur d'adhérence de A_p, par injectivité de l'exponentielle, et une suite bornée avec une seule valeur d'adhérence est convergente. □

Remarque. La preuve de la continuité dans le théorème s'adapte pour obtenir le résultat suivant concernant une décomposition polaire pour une matrice non forcément inversible : toute matrice $M \in \mathcal{M}_n(\mathbb{R})$ s'écrit comme un produit $M = OS$ avec O orthogonale et S symétrique positive. Cette écriture n'est pas unique (la restriction de O à un supplémentaire orthogonal de l'image de S est une application orthogonale arbitraire). Pour voir cela, on écrit M comme une limite de matrices inversibles $M_p = O_p S_p$, on prend O une valeur d'adhérence de O_p dans le groupe compact $\mathrm{O}_n(\mathbb{R})$, et on pose $S = O^{-1}M \in S_n^+$ qui est la limite des $S_p = O_p^{-1} M_p \in S_n^{++}$.

Corollaire ([CG13, p. 205])**.** *Tout sous-groupe compact de* $\mathrm{GL}_n(\mathbb{R})$ *qui contient le groupe orthogonal* $\mathrm{O}_n(\mathbb{R})$ *est égal à* $\mathrm{O}_n(\mathbb{R})$*.*

Preuve. Soit G un groupe compact contenant $\mathrm{O}_n(\mathbb{R})$, et soit $g \in G$. On écrit la décomposition polaire $g = os$, et on a $s = o^{-1}g \in G$, donc également $s^k \in G$ pour tout $k \in \mathbb{Z}$. Comme G est compact, la suite s^k doit admettre une valeur d'adhérence, et en particulier le rayon spectral de s et de s^{-1} doit être égal à 1. Comme les valeurs propres de s sont réelles, on en déduit que 1 est l'unique valeur propre de s, et comme s est diagonalisable, on a $s = \mathrm{id}$, et finalement $g = o \in \mathrm{O}_n(\mathbb{R})$. □

Application ([MT86, p. 63])**.** Le groupe $\mathrm{O}_n(\mathbb{C})$ est homéomorphe au produit $\mathrm{O}_n(\mathbb{R}) \times \mathbb{R}^{n(n-1)/2}$.

Preuve. On va obtenir l'homéomorphisme comme restriction de la décomposition polaire complexe à $\mathrm{O}_n(\mathbb{C})$. Soit $M \in \mathrm{O}_n(\mathbb{C})$, qui s'écrit de façon unique $M = UH$ avec $U \in \mathrm{U}_n(\mathbb{C})$ et H hermitienne définie positive. On a

$$I_n = M^t M = H^t U^t U H \implies (U^t U)H = (H^t)^{-1}.$$

Par unicité de la décomposition polaire on obtient $U^t U = I_n$ et $H = (H^t)^{-1}$, c'est-à-dire $U \in \mathrm{O}_n(\mathbb{R})$ et $H = \exp(iA)$ avec A antisymétrique réelle. Reste à remarquer que l'espace des matrices antisymétrique réelles est homéomorphe à $\mathbb{R}^{n(n-1)/2}$. □

Compléments topologiques :

Proposition. *L'application* $\sqrt{\ }: S^+ \to S^+$ *est continue.*

Preuve. Soit A_p une suite de matrices dans S^+ convergeant vers M, on veut montrer que $\sqrt{A_n}$ converge vers $\sqrt{M}$. Soit B une valeur d'adhérence de $\sqrt{A_p}$ (il y en a au moins une, la suite étant bornée), il s'agit de voir que $B = \sqrt{M}$. Par continuité de la mise au carré, B^2 est une valeur d'adhérence de la suite convergente $(\sqrt{A_p})^2$, d'où $B^2 = M$. On conclut par unicité de la racine carrée. □

Proposition. *L'application* $\sqrt{\ }: S^{++} \to S^{++}$ *est de classe* $\mathcal{C}^\infty$*.*

Preuve. On sait que $A \mapsto A^2$ est une bijection $\mathcal{C}^\infty$ de S^{++} vers S^{++}. Par le théorème d'inversion locale, il suffit de vérifier que la différentielle $H \mapsto HA + AH$ est inversible en tout $A \in S^{++}$. Comme S^{++} est de dimension finie, il suffit de prouver l'injectivité. Supposons donc que H vérifie $HA + AH = 0$. Pour toute valeur propre λ de A (on a $\lambda > 0$ par hypothèse) et vecteur propre associé x, on a $(HA + AH)(x) = \lambda H(x) + AH(x) = 0$, d'où $H(x) = 0$ car sinon $H(x)$ serait un vecteur propre de A associé à $-\lambda$, contredit $A \in S^{++}$. Comme il existe une base formée de vecteurs propres de A, on obtient $H = 0$ comme attendu. □

Lemme de Morse

[BMP05, p. 14], [Rou03, p. 321, 344], [Pha99, p.31-38]

Leçons :

- 158. Matrices symétriques réelles, matrices hermitiennes
- 170. Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications

Le rapport 2018 appelle explicitement à parler d'isotropie en géométrie différentielle.

- 171. Formes quadratiques réelles. Coniques. Exemples et applications
- Quelques leçons d'analyse : au moins 214 (Inversion locale) et 215 (Applications différentiables)

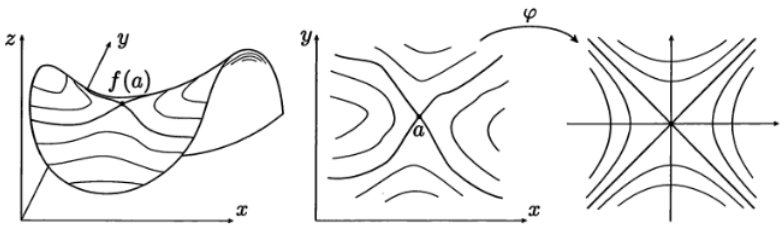

FIGURE 1 – Figure extraite de [BMP05, p. 14]

Lemme ([Rou03, Ex. 66 p. 201])**.** *Soit S_n l'espace des matrices symétriques $n \times n$, et $A_0 \in S_n$ inversible. Alors il existe un voisinage V de A_0 dans S_n tel que toute matrice $A \in V$ est équivalente à A_0 : il existe M (dépendant de A) tel que $A = M^t A_0 M$. De plus M est unique, et l'application $A \mapsto M$ est un difféomorphisme local.*

Preuve. La différentielle en I de $\varphi\colon M \mapsto M^t A_0 M$ est $D\varphi(I)(H) = (A_0 H)^t + A_0 H$. Donc le noyau de $D\varphi(I)$ est formé des matrices H tel que $A_0 H$ soit antisymétrique. Donc l'image de $D\varphi(I)$ a la même dimension que les matrices symétriques (l'espace des matrices est la somme directes des symétriques et antisymétriques), donc $D\varphi(I)$ est surjective.

Le sous-espace F des matrices M tel que $A_0 M$ soit symétrique est donc un supplémentaire du noyau de $D\varphi(I)$, et de plus $I \in F$. On applique alors le théorème d'inversion locale à ψ la restriction de φ à F : on obtient un voisinage U de I dans F (qui peut être pris suffisamment petit pour ne contenir que des matrices inversibles) tel que $M \in U \mapsto A = M^t A_0 M \in S_n$ est un difféo local. □

Théorème. *Soit $U \subseteq \mathbb{R}^n$ un ouvert contenant l'origine, et $f\colon U \to \mathbb{R}^n$ une application de classe $\mathcal{C}^3$. Supposons $df(0) = 0$ et $df^2(0)$ non dégénérée de signature $(p, n-p)$. Alors il existe un difféomorphisme $\varphi = (\varphi_1, \dots, \varphi_n)$ entre deux voisinages de 0 tel que $\varphi(0) = 0$ et*

$$f(v) - f(0) = \varphi_1^2(v) + \cdots + \varphi_p^2(v) - \varphi_{p+1}^2(v) - \cdots - \varphi_n^2(v).$$

Remarque. Terminologie pour la condition $df(a) = 0$: on dit que a est un point critique pour f. Dans l'énoncé du théorème de Morse on a donc supposé que 0 est un point critique de f. Si la forme quadratique $d^2 f(a)$ est non dégénérée on dit que le point critique a est non dégénéré.

Preuve. [Rou03, p. 345]. La formule de Taylor à l'ordre 1 avec reste intégral donne

$$f(x) - f(0) = x^t Q(x) x$$

avec $x \mapsto Q(x)$ de classe $\mathcal{C}^1$. Par le lemme, pour x proche de 0 on peut écrire

$$Q(x) = M(x)^t Q(0) M(x)$$

avec $M(0) = I_n$, $M(x)$ inversible et $x \mapsto M(x)$ de classe $\mathcal{C}^1$. On conclut en mettant Q_0 sous forme normale

$$P^t Q_0 P = \mathrm{diag}(I_p, -I_{n-p}),$$

et en posant $\varphi(x) = PM(x)x$, qui est un difféomorphisme local puisque de différentielle $PM(0)$ inversible. □

Remarque. [Rou03, p. 321] propose une preuve dans le cas de $n = 2$ variables qui évite le recours au lemme. A la place, il fait un argument direct par "algorithme de Gauss". Il explicite aussi un peu plus l'usage de la formule de Taylor. On note (x, y) les coordonnées dans $\mathbb{R}^2$, et on écrit la formule de Taylor à l'origine avec reste intégral :

$$\begin{aligned} f(x,y) - f(0,0) &= \partial_x f(0,0)x + \partial_y f(0,0)y + \int_0^1 (1-t) d^2 f(tx,ty)((x,y),(x,y))dt \\ &= \alpha(x,y)x^2 + 2\beta(x,y)xy + \gamma(x,y)y^2. \end{aligned}$$

et on peut expliciter les fonctions α, β, γ en intégrant les dérivées partielles secondes correspondantes, par exemple

$$\alpha(x,y) = \int_0^1 (1-t)\partial^2_{x^2} f(tx,ty)dt.$$

On considère ensuite plusieurs cas, correspondant à l'algorithme de Gauss. Par exemple, considérons le cas $\alpha(0,0) > 0$ et $d^2 f(0,0)$ de signature $(1,1)$. Alors localement on peut écrire

$$\alpha x^2 + 2\beta xy + \gamma y^2 = \alpha\left(x + \frac{\beta}{\alpha}y\right)^2 - \frac{\beta^2 - \alpha\gamma}{\alpha}y^2,$$

et on pose

$$\varphi_1 = \sqrt{\alpha}\left(x + \frac{\beta}{\alpha}y\right)$$
$$\varphi_2 = \sqrt{\frac{\beta^2 - \alpha\gamma}{\alpha}}y$$

Réciprocité quadratique... via les formes quadratiques

[CG13, p. 185]

Leçons :

- 101. Groupe opérant sur un ensemble. Exemples et applications

Plausible, à défendre...

- 104. Groupes finis. Exemples et applications

Il y a bien l'action du groupe $\mathbb{Z}/p\mathbb{Z}$, mais bon, pas idéal pour cette leçon quand même...

- 120. Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications
- 121. Nombres premiers. Applications
- 123. Corps finis. Applications
- 126. Exemples d'équations en arithmétique

A la rigueur, mais il faut (vraiment) avoir réfléchi aux applications...

- 150. Exemples d'actions de groupes sur les espaces de matrices

Demande un laïus sur l'interprétation en termes orbites sous action d'un groupe de la relation de congruence pour des matrices symétriques...

- 159. Formes linéaires et dualité en dimension finie. Exemples et applications

Ultra douteux. Justifié seulement parce que le mot "hyperplan" apparaît dans la preuve ? ?

- 170. Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications

Enfin un développement qui n'est pas un simple copier-coller depuis les choix de 171. Formes quadratiques réelles. Coniques. Exemples et applications ...

- 190. Méthodes combinatoires, problèmes de dénombrements

Ok car fait intervenir une action de groupe via la formule des classes et l'idée de dénombrer une même quantité suivant deux points de vue.

Théorème. *Soit p et q deux nombres premiers impairs distincts. Alors :*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Preuve. L'idée est de calculer de deux façons différentes le cardinal de la conique définie sur $\mathbb{F}_q$:

$$X = \{(x_1, \dots, x_p) \in (\mathbb{F}_q)^p;\ \sum x_i^2 = 1\}.$$

On fait agir $\mathbb{Z}/p\mathbb{Z}$ par permutation cyclique sur $\mathbb{F}_q^p$:

$$\bar{k} \cdot (x_1, \dots, x_p) = (x_{1+k}, \dots, x_{p+k})$$

où les indices sont vus modulo p. Les orbites sont de deux types : les singletons $(x, \dots, x)$ (chacun stabilisé par $\mathbb{Z}/p\mathbb{Z}$), et les autres orbites qui sont de cardinal p (le stabilisateur d'un point dans une telle orbite est trivial). Attention, c'est dit à l'envers dans [CG13] ! Le nombre de singletons est égal au nombre de solutions x à l'équation $px^2 = 1$ dans $\mathbb{F}^q$: il y en a 2 ou 0, selon si p est un carré on non dans $\mathbb{F}_q$, autrement dit il y en a $\left(\frac{p}{q}\right) + 1$. En écrivant l'équation aux classes on obtient une première équation

$$(\spadesuit) \qquad |X| = \left(\frac{p}{q}\right) + 1 \mod p.$$

Par ailleurs, si $a = (-1)^{(p-1)/2}$, les matrices suivantes dans $\mathcal{M}_p(\mathbb{F}_q)$

$$I_p = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \text{ et } A = \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & \ddots & & & \\ & & & 0 & 1 & \\ & & & 1 & 0 & \\ & & & & & \bar{a} \end{pmatrix}$$

sont symétriques, de déterminant 1 et rang maximal p, donc elles sont congruentes. En particulier, la conique X est en bijection avec la conique

$$X' = \{(y_1, \dots, y_d, z_1, \dots, z_d, t) \in (\mathbb{F}_q)^p;\ 2(y_1 z_1 + \cdots + y_d z_d) + \bar{a}t^2 = 1\},$$

où $d = (p-1)/2$. L'ensemble X' contient deux types de points :

- ceux où tous les y_i sont nuls : il faut $at^2 = 1$ ($1 + a^{(q-1)/2}$ tels t possibles), et les z_i arbitraires (q^d choix pour t fixé) ;
- ceux où l'un des y_i est non nul ($q^d - 1$ choix) : prendre t arbitraire (q choix), puis les z_i dans un hyperplan affine de $\mathbb{F}_q^d$ (q^{d-1} choix).

En rassemblant on obtient

$$|X'| = \left(1 + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) q^d + (q^d - 1) q q^{d-1}.$$

et en simplifiant (en se rappelant que $q^d = q^{(p-1)/2} = \left(\frac{q}{p}\right)$)

$$(\heartsuit) \qquad |X| = \left(\left(\frac{q}{p}\right) + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right)\left(\frac{q}{p}\right).$$

Finalement en rassemblant ($\spadesuit$) et ($\heartsuit$) :

$$\left(\left(\frac{q}{p}\right) + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right)\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) + 1 \mod p$$

En multipliant à droite et à gauche par $\left(\frac{q}{p}\right)$, puis en soustrayant $\left(\frac{q}{p}\right)$:

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \mod p.$$

Les deux côté de l'égalité sont égaux à ± 1, comme ils sont égaux modulo $p \geqslant 3$, ils sont donc égaux. □

Remarque. [CG13, p. 152]. Si $a, b \neq 0$ dans $\mathbb{F}_q^2$, montrer que l'équation $ax^2 + by^2 = 1$ admet au moins une solution dans $\mathbb{F}_q^2$.

Il y a $(q-1)/2$ carrés dans le groupe multiplicatif $\mathbb{F}_q^*$, qui forment l'image du morphisme $x \mapsto x^2$, de noyau ± 1. En ajoutant 0, il y a donc $(q+1)/2$ carrés dans $\mathbb{F}_q$, et donc $(q+1)/2$ valeurs possibles pour ax^2, et pour $1 - by^2$.

Comme $(q+1)/2 + (q+1)/2 = q + 1 > q$, il y a au moins une valeur commune, et donc il existe $x, y \in \mathbb{F}_q$, $ax^2 = 1 - by^2$ comme attendu.

Application : La forme quadratique de matrice $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ est équivalente à $\left(\begin{smallmatrix} 1 & 0 \\ 0 & c \end{smallmatrix}\right)$ pour un certain $c \in \mathbb{F}_q^*$.

En dimension n, par récurrence on se ramène à une matrice diagonale avec seulement des 1 sur la diagonale, sauf un coefficient $c \neq 0$. Si c est un carré, on peut le ramener à 1. Sinon, ayant choisi $\xi \in \mathbb{F}_q$ un non-carré, le produit ξc est un carré, et on peut ramener c à ξ.

Remarque. • En pratique, on a aussi besoin des deux lois de réciprocité complémentaires suivantes. Si p est un nombre premier impair, alors

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

- A titre d'exemple, calculons si 11 est un carré modulo 19. Par le théorème, on a

$$\left(\frac{11}{19}\right)\left(\frac{19}{11}\right) = (-1)^{5\cdot 9} = -1.$$

Par ailleurs $\left(\frac{19}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{2}{11}\right)^3$, et $\left(\frac{2}{11}\right) = (-1)^{(121-1)/8} = (-1)^{15} = -1$, et finalement $\left(\frac{11}{19}\right) = +1$. Effectivement $11 + 2 \cdot 19 = 49$ carré de 7.

- Autre exemple : 13 est-il un carré modulo 43 ? On a $\left(\frac{13}{43}\right)\left(\frac{43}{13}\right) = +1$, et $\left(\frac{43}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{2}{13}\right)^2 = +1$. Donc $\left(\frac{13}{43}\right) = +1$, et effectivement $13 + 9 \cdot 43 = 400$ carré de 20.

Leçons où l'on peut envisager ces développements

101. Groupe opérant sur un ensemble. Exemples et applications

- Réciprocité quadratique... via les formes quadratiques
- ...

102. Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications

- ...

103. Exemples de sous-groupes distingués et de groupes quotients. Applications

- ...

104. Groupes finis. Exemples et applications

- ...

105. Groupe des permutations d'un ensemble fini. Applications

- ...

106. Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E). Applications

- Réduction des endomorphismes auto-adjoints et décomposition polaire
- ...

107. Représentations et caractères d'un groupe fini sur un C-espace vectoriel. Exemples

- ...

108. Exemples de parties génératrices d'un groupe. Applications

- Réduction des endomorphismes auto-adjoints et décomposition polaire
- ...

110. Structure et dualité des groupes abéliens finis. Applications

- ...

120. Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications

- Réciprocité quadratique... via les formes quadratiques
- ...

121. Nombres premiers. Applications

- Réciprocité quadratique... via les formes quadratiques
- ...

122. Anneaux principaux. Applications

- ...

123. Corps finis. Applications

- Réciprocité quadratique... via les formes quadratiques
- ...

125. Extensions de corps. Exemples et applications

- ...

126. Exemples d'équations en arithmétique

- ...

141. Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

- ...

142. PGCD et PPCM, algorithmes de calcul. Applications

- ...

144. Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications

- ...

150. Exemples d'actions de groupes sur les espaces de matrices

- Réciprocité quadratique... via les formes quadratiques
- ...

151. Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications

- ...

152. Déterminant. Exemples et applications

- ...

153. Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications

- ...

154. Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications

- ...

155. Endomorphismes diagonalisables en dimension finie

- Réduction des endomorphismes auto-adjoints et décomposition polaire
- ...

156. Exponentielle de matrices. Applications

- ...

157. Endomorphismes trigonalisables. Endomorphismes nilpotents

- ...

158. Matrices symétriques réelles, matrices hermitiennes

- Réduction des endomorphismes auto-adjoints et décomposition polaire
- Lemme de Morse
- ...

159. Formes linéaires et dualité en dimension finie. Exemples et applications

- ...

160. Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie)

- Réduction des endomorphismes auto-adjoints et décomposition polaire
- ...

161. Distances et isométries d'un espace affine euclidien

- Réduction des endomorphismes auto-adjoints et décomposition polaire
- ...

162. Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques

- ...

170. Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications

- Réciprocité quadratique... via les formes quadratiques
- Lemme de Morse
- ...

171. Formes quadratiques réelles. Coniques. Exemples et applications

- Lemme de Morse
- ...

181. Barycentres dans un espace affine réel de dimension finie, convexité. Applications

- ...

182. Applications des nombres complexes à la géométrie.

- ...

183. Utilisation des groupes en géométrie

- ...

190. Méthodes combinatoires, problèmes de dénombrements

- Réciprocité quadratique... via les formes quadratiques
- ...

Références

[BMP05] V. Beck, J. Malick & G. Peyré. *Objectif agrégation*. H&K, 2005. 3, 4

[CG13] P. Caldero & J. Germoni. *Histoires hédonistes de groupes et de géométries, Tome premier*. Calvage & Mounet, 2013. 1, 2, 3, 5, 6

[Gou09] X. Gourdon. *Algèbre*. Ellipses, 2009. 1, 2

[MT86] R. Mneimné & F. Testard. *Introduction aux groupes de Lie classiques*. Herman, 1986. 2, 3

[Pha99] F. Pham. *Géométrie et calcul différentiel sur les variétés (2de éd.)*. Dunod, 1999. 3

[Rou03] F. Rouvière. *Petit guide de calcul différentiel à l'usage de la licence et de l'agrégation*. Cassini, 2003. 3, 4

[RW07] J.-P. Ramis & A. Warusfel. *Mathématiques Tout-en-un pour la Licence, Niveau L2*. Dunod, 2007. 1, 2

[Szp09] A. Szpirglas, editor. *Mathématiques L3 Algèbre*. Pearson Education, 2009. 1