Canad. J. Math. Vol. **54** (3), 2002 pp. 449–467

Théorème de Voronoï dans les espaces symétriques

H. Akrout

Résumé. On démontre un théorème de Voronoï (caractérisation des maxima locaux de l'invariant d'Hermite) pour les familles de réseaux paramétrées par les espaces symétriques irréductibles non exceptionnels de type non compact.

Abstract. We prove a theorem of Voronoï type (characterisation of local maxima of the Hermite invariant) for the lattices parametrized by irreducible nonexceptional symmetric spaces of noncompact type.

1 Introduction

L'étude de l'invariant d'Hermite des réseaux euclidiens débute dans les lettres d'Hermite à Jacobi dans les années 1850. Au début du siècle, G. Voronoï [Vo] utilise une notion variationnelle pour déterminer les maxima locaux de cet invariant. En particulier, il donne une caractérisation des formes *extrémales* en fonctions des vecteurs minimaux. L'interprétation des formes quadratiques en termes de réseaux ramène le problème à un problème de géométrie sur l'espace symétrique P_n des réseaux marqués de déterminant 1. Sur cet espace, l'invariant d'Hermite s'exprime simplement comme un minimum fini de fonctions de classe $\mathcal{C}^\infty$ qui représentent les longueurs des vecteurs dans le réseau.

Un autre problème naturel plus récent provenant de la géométrie consiste à maximiser la systole des surfaces de Riemann sur l'espace de Teichmüller. P. Schmutz [Sch] a donné une caractérisation des maxima locaux de la systole en fonction des géodésiques fermées réalisant la systole. De même que l'invariant d'Hermite, la systole apparait naturellement sur cet espace comme une fonction qui est minimum de fonctions analytiques représentant les longueurs des géodésiques sur la surface marquée.

Récemment, Ch. Bavard [Ba] a unifié ces deux problèmes dans un cadre plus général qui s'étend à d'autres exemples de fonctions généralisant ces deux cas particuliers. Il donne en particulier une condition pour avoir un *Théorème de Voronoï*. La réalisation de celle-ci apparait alors comme un problème naturel lorsqu'on travaille avec des fonctions de type "invariant d'Hermite".

On se place dans le cadre général suivant : si V est une variété Riemanienne, une systole généralisée sur V est une fonction qui s'exprime localement comme minimum fini de fonctions de classe $\mathcal{C}^\infty$. Plus précisément, soit $(l_u)_{u\in\mathcal{C}}$ une famille de

Reçu par la rédaction le 25 juillet, 2000; revu le 5 janvier, 2002.
Classification (AMS) par sujet: 11H06, 53C35.
Mots clés: réseaux, théorème de Voronoï, espaces symétriques.

https://doi.org/10.4153/CJM-2002-015-1 Published online by Cambridge University Press

fonctions $\mathcal{C}^\infty$ sur V. Pour tout point p de V et pour tout réel K, on pose $\mathcal{C}_p^{\leq K} = \{u \in \mathcal{C}, l_u(p) \leq K\}$. La fonction $\mu = \inf_{u \in \mathcal{C}} l_u$ est une *systole géneralisée* si pour tout point p de V et tout réel K, il existe un voisinage W de p tel que l'ensemble $E_p^K = \bigcup_{q \in W} \mathcal{C}_q^{\leq K}$ soit fini. Remarquons que μ s'exprime sur W comme minimum des fonctions de l'ensemble fini E_p^K. En particulier, μ est continue. Pour tout point p, l'ensemble $S(p) = \{u \in \mathcal{C}, l_u(p) = \mu(p)\}$ est appelé *ensemble des longueurs minimales*.

Exemples

- Soit P_n l'espace des matrices symétriques de déterminant 1, on représente les vecteurs de $\mathbb{R}^n$ par des matrices colonnes. Considérons sur cet espace les fonctions suivantes paramétrées par $\mathbb{Z}^n$ ou $\mathbb{R}^n$:

$$l_u(A) := {}^t uAu.$$

  Cette fonction est la longueur du vecteur associé à u dans le réseau marqué représenté par A. L'invariant d'Hermite d'un réseau est alors le minimum des longueurs l_u pour $u \in \mathbb{Z}^n \setminus \{0\}$. Remarquons que l_u est bien définie sur P_n (grâce au marquage) mais pas sur l'ensemble $\mathrm{SL}(n, \mathbb{Z}) \setminus P_n$ des réseaux non marqués.
- Soit X une surface de Riemann marquée. À toute classe γ d'homotopie libre de courbes (classe de conjugaison du groupe fondamental de X), on associe la longueur $l_\gamma(X)$ de l'unique géodésique fermée représentant γ. Il est bien connu que les fonctions l_γ sont analytiques et strictement convexes [Wo] sur l'espace de Teichmüller. Là encore, l_γ n'est pas définie sur l'espace des modules.
- La restriction d'une systole généralisée à une sous-variété reste une systole généralisée. Par exemple, soit G un sous-groupe de Lie connexe de $\mathrm{SL}(n, \mathbb{R})$ stable par transposition, l'orbite dans P_n de l'identité sous l'action de G définie par

$$g.A := gA^t g$$

  est une sous-variété totalement géodésique de P_n [Eb]. La restriction de l'invariant d'Hermite à ces sous-variétés reste une systole généralisée.

On a un problème naturel associé à ces objets: caractériser les points p de la variété où μ est un maximum local (*les points extrêmes*). Ce problème a été résolu dans le cas des deux premiers exemples précédents (par G. Voronoï [Vo] pour le premier et par P. Schmutz [Sch] pour le second). A. M. Bergé et J. Martinet ont étendu ce résultat aux familles de réseaux stables sous l'action d'un groupe fini ainsi qu'aux réseaux orthogonaux et symplectiques [B-M2], [B-M3]. Citons aussi le k-invariant d'Hermite étudié tout d'abord par R. A. Rankin [Ra] puis repris par A. M. Bergé, J. Martinet [B-M1] et R. Coulangeon [Co]. Dans tous ces exemples, on a une caractérisation simple de ces points en fonction de critères sur les longueurs minimales.

Dans le cadre des systoles généralisées, on cherche à caractériser les points extrêmes par des considérations sur les gradients des fonctions minimales en ce point (*gradients minimaux*). Rappelons les résultats dans ce domaine. Pour plus de détails, on pourra se reporter à [Ba].

Un point p de V est dit *parfait* si les gradients minimaux engendrent affinement l'espace tangent en p, *semi-eutactique* si le vecteur nul appartient à l'enveloppe convexe des gradients minimaux, *eutactique* si le vecteur nul appartient à l'intérieur affine de cette enveloppe convexe. Par abus de langage, on dira semi-eutactique pour "semi-eutactique non eutactique". Un point extrême est un maximum local de μ et un point strictement extrême est un maximum local strict de μ.

On dit alors que μ vérifie un "*Théorème de Voronoï*" si les assertions suivantes sont équivalentes:

(1) p est extrême.
(2) p est parfait et eutactique.
(3) p est strictement extrême.

En fait, on sait que seule l'implication (1) $\Rightarrow$ (2) peut être fausse en général. Avoir un théorème de Voronoï se résume donc à "*Tout point extrême est parfait et eutactique*".

On s'intéresse ici au problème de détermination des points extrêmes dans un cas particulier de l'exemple 3. Plus précisément, les espaces symétriques irréductibles de type non compact se plongent dans P_n sous l'action de certains sous-groupes de $\mathrm{SL}(n,\mathbb{R})$. Le but de cet article est de montrer le théorème suivant:

Théorème 1 *L'invariant d'Hermite restreint à un espace symétrique irréductible non exceptionnel de type non compact vérifie un théorème de Voronoï.*

On sait comment réaliser les espaces symétriques irréductibles de type non compact dans P_n comme orbites de l'identité sous l'action de sous-groupes de $\mathrm{SL}(n,\mathbb{R})$. E. Cartan a donné la liste de ces sous-groupes.

L'orbite de l'identité sous l'action de chaque sous-groupe, et donc chaque espace symétrique irréductible, correspond ainsi à une image isométrique d'une famille de réseaux marqués muni de certaines structures algébriques (voir section 3.1). Les notations sont celles de Helgason [He] :

- $P_n = \mathrm{SL}(n,\mathbb{R})/\mathrm{SO}(n)$, $\mathrm{SL}(n,\mathbb{C})/\mathrm{SU}(n)$ et $\mathrm{SU}^*(2n)/\mathrm{Sp}(n)$ paramètrent les familles de réseaux sur des anneaux d'entiers. C'est un cas particulier de réseaux stables sous l'action d'un sous-groupe discret de $\mathrm{SL}(n,\mathbb{R})$.
- $\mathrm{SO}_0(p,q)/\mathrm{SO}(p)\times\mathrm{SO}(q)$, $\mathrm{SU}(p,q)/S(U_p\times U_q)$, $\mathrm{Sp}(p,q)/\mathrm{Sp}(p)\times\mathrm{Sp}(q)$ correspondent à des familles de réseaux isoduaux réels, complexes et quaternioniques, c'est à dire munis d'une isométrie de carré id du réseau sur son dual pour certaines formes sesquilinéaires.
- $\mathrm{SO}(n,\mathbb{C})/\mathrm{SO}(n)$ et $\mathrm{SO}^*(2n)/U(n)$ paramètrent les réseaux autoduaux complexes et quaternioniques.
- $\mathrm{Sp}(n,\mathbb{R})/U(n)$ et $\mathrm{Sp}(n,\mathbb{C})/\mathrm{Sp}(n)$ sont formés par les réseaux symplectiques réels et complexes. C'est-à-dire munis d'une isométrie de carré $-$id du réseau sur son dual.

Dans un premier temps, on donne des conditions générales pour avoir un théorème de Voronoï. Ensuite, on applique ces critères pour les espaces symétriques irréductibles. Remarquons que le théorème de Voronoï était connu pour les familles P_n, $\mathrm{SO}_0(p,q)/\mathrm{SO}(p)\times\mathrm{SO}(q)$, $\mathrm{Sp}(n,\mathbb{R})/U(n)$ et pour les G-réseaux. On le démontre ici pour tous les autres cas ci-dessus.

https://doi.org/10.4153/CJM-2002-015-1 Published online by Cambridge University Press

2 Critères généraux pour un théorème de Voronoï

La démonstration du théorème se fait de manière indirecte en utilisant la condition suivante (*condition C*) donnée par Ch. Bavard [Ba].

Définition 1 On dit que $\mu = \min_{u \in \mathcal{C}} l_u$ vérifie la condition C au point p si pour tout sous-ensemble T de $S(p)$ et pour tout vecteur tangent X qui annule les différentielles des longueurs de T, il existe une courbe c telle que $c(0) = p$, $\dot{c}(0) = X$ et pour tout $u \in T$, la longueur l_u est strictement croissante le long de c.

D'après [Ba, p. 102], on a alors la proposition suivante, utile pour vérifier qu'une systole généralisée vérifie un théorème de Voronoï :

Proposition 2.1 *Lorsque la condition C est vérifiée en tout point extrême, μ vérifie un théorème de Voronoï.*

On démontre le théorème en vérifiant la condition C pour les différents sous-groupes ci-dessus.

2.1 Cas de longueurs quelconques

On se place dans le cadre ci-dessus. Compte tenu du caractère local du problème, le lemme suivant est immédiat :

Lemme 2.1 *La condition C est invariante par difféomorphisme local.*

En particulier, il est clair que pour que celle-ci soit vérifiée en p, il est nécessaire et suffisant qu'elle le soit pour une carte centrée en p. De plus, puisque toutes les longueurs minimales ont la même valeur en p, on peut supposer que cette valeur est nulle. On peut ainsi ramener le problème à des longueurs définies au voisinage de 0 dans $\mathbb{R}^n$, toutes nulles en 0.

On note $d_0^i f$ la dérivée i-ième de f en 0 et pour $x_1, x_2, \ldots, x_r$ dans $\mathbb{R}^n$, on note $x_1^{k_1} x_2^{k_2} \cdots x_r^{k_r}$ le vecteur

$$(\underbrace{x_1, \ldots, x_1}_{k_1 \text{ fois}}, \underbrace{x_2, \ldots, x_2}_{k_2 \text{ fois}}, \ldots, \underbrace{x_r, \ldots, x_r}_{k_r \text{ fois}})$$

de $(\mathbb{R}^n)^{k_1 + \cdots + k_r}$.

Lemme 2.2 *Soit $f\colon (\mathbb{R}^n, 0) \to (\mathbb{R}, 0)$ une fonction $\mathcal{C}^\infty$ et $c(t) = t\mathbf{x} + t^2\mathbf{y}(t)$ une courbe. On pose*

$$y_k = \frac{\mathbf{y}^{(k)}(0)}{k!}$$

et

$$E_{i,m} = \Big\{ (\alpha_{-1}, \alpha_0, \ldots, \alpha_{m-2}) \in \mathbb{N}^m, \sum_{k=-1}^{m-2} \alpha_k = i, i + \sum_{k=0}^{m-2} (k+1)\alpha_k = m \Big\}.$$

https://doi.org/10.4153/CJM-2002-015-1 Published online by Cambridge University Press

Alors la dérivée m-ième ($m \geq 2$) de $f \circ c$ en 0 est

$$a_m = m! \sum_{i=1}^{m} \sum_{(\alpha_{-1},\alpha_0,\dots,\alpha_n)\in E_{i,m}} \frac{1}{\alpha_{-1}! \cdots \alpha_n!} d_0^{(i)} f.x^{\alpha_{-1}} \Pi_{k=0}^{m-2} y_k^{\alpha_k}.$$

Preuve On écrit les développements limités à l'ordre m de f et de c en 0 et on regarde le coefficient de t^m dans le développement de $f \circ c$. Le reste n'est qu'un long calcul. ■

Donnons ici les premiers a_i:

$$\begin{aligned} a_1 &= d_0 f.x \\ a_2 &= 2d_0 f.y_0 + d_0^2 f.x^2 \\ a_3 &= 6d_0 f.y_1 + 6d_0^2 f.xy_0 + d_0^3 f.x^3 \\ a_4 &= 24 d_0 f.y_2 + 12 d_0^2 f.y_0^2 + 24 d_0^2 f.xy_1 + 12 d_0^3 f.x^2 y_0 + d_0^4 f.x^4. \end{aligned}$$

Dans toute la suite de ce paragraphe, on se donne une famille finie $S(0) = \{l_u, u \in \mathcal{C}\}$ de fonctions $\mathcal{C}^\infty$ au voisinage de 0 toutes nulles en 0.

Pour chaque longueur l_u, le lemme précédent donne une famille de coefficients $a_k(u)$ qui sont les dérivées de l_u le long de la courbe c et qui dépendent des variables y_i, $i \leq k$.

Lemme 2.3 *Soit $T \subset S(0)$ et $X \in \mathbb{R}^n$ annulant les différentielles des longueurs de T,*

(1) *On suppose qu'il existe une famille d'entiers $m(u)$, $u \in T$ telle que le système*

$$\mathcal{S} \begin{cases} a_k(u) = 0 & si\ k < m(u) \\ a_{m(u)} > 0 \end{cases}$$

admette une solution en y_k. Alors la condition C est vérifiée pour X et T.

(2) *On suppose que la condition C est vérifiée, alors pour tout X et T comme ci-dessus, le système*

$$\begin{cases} a_k(u) = 0 & si\ k < m(u) \\ a_{m(u)} \geq 0 \end{cases}$$

admet une solution en y_k.

Preuve (1) Une solution y_k donne la courbe $c(t) = tx + t^2(\sum_k t^k y_k)$ réalisant la condition C.

(2) Si c est une courbe réalisant la condition C, la première dérivée non nulle de $l_u \circ c$ ne peut pas être strictement négative puisque cette fonction est strictement croissante. On en déduit le lemme. ■

https://doi.org/10.4153/CJM-2002-015-1 Published online by Cambridge University Press

Remarques

(1) Si X est orthogonal aux gradients de T, les coefficients $a_1(u)$ sont nuls pour tout $u \in T$. Il suffit de résoudre le système pour les $k \geq 2$.
(2) Lorsque les longueurs sont analytiques, le système $\mathcal{S}$ donne une condition nécessaire et suffisante pour réaliser la condition C par une courbe analytique. En effet, il doit forcément y avoir une dérivée non nulle pour que $f \circ c$ le soit.

L'écriture de $\mathcal{S}$ à l'ordre 2 et 4 sera utile pour vérifier la condition C dans les sous-variétés de P_n.

$\mathcal{S}$ ***à l'ordre 2***

$$2d_0 l_u.y_0 + d_0^2 l_u.x^2 > 0$$

$\mathcal{S}$ ***à l'ordre 4***

$$a_2 = 2d_0 f.y_0 + d_0^2 f.x^2 = 0$$
$$a_3 = 6d_0 f.y_1 + 6d_0^2 f.xy_0 + d_0^3 f.x^3 = 0$$
$$a_4 = 24d_0 f.y_2 + 12d_0^2 f.y_0^2 + 24d_0^2 f.xy_1 + 12d_0^3 f.x^2 y_0 + d_0^4 f.x^4 > 0$$

On peut aussi se limiter au cas $c(t) = tx + t^2 y$, auquel cas, le système à l'ordre 4 se simplifie en:

$$a_2 = 2d_0 f.y + d_0^2 f.x^2 = 0$$
$$a_3 = 6d_0^2 f.xy + d_0^3 f.x^3 = 0$$
$$a_4 = 12d_0^2 f.y^2 + 12d_0^3 f.x^2 y + d_0^4 f.x^4 > 0.$$

2.2 Cas de longueurs convexes

On suppose maintenant que V est muni d'une métrique riemanienne.

On rappelle qu'une fonction est dite convexe si elle l'est le long de toute géodésique paramétrée par longueur d'arc. En particulier, elle est radialement convexe dans la carte exponentielle centrée en tout point. De plus, si W est une sous-variété totalement géodésique de V, la restriction à W d'une fonction convexe reste évidemment convexe. Dans le cas de P_n, les longueurs sont des exponentielles de fonctions de Busemann [Ba], donc sont convexes. Dans le cas des longueurs géodésiques sur les surfaces de Riemann, celles-ci sont strictement convexes le long des géodésiques de Weil-Petersson [Wo]. La convexité permet de simplifier la réalisation de la condition C. Par exemple, cette dernière est trivialement vérifiée lorsque la convexité est stricte puisqu'il suffit de choisir la géodésique définie par (p, X). On peut aussi se limiter à supposer seulement la stricte convexité radiale par rapport au gradient (c'est-à-dire convexité le long des géodésiques orthogonales au gradient de la fonction).

On note $\nabla_u(0)$ ou plus simplement ∇_u le gradient de l_u en 0, H_u (respectivement H_u^+) l'orthogonal de $\nabla_u(0)$, (respectivement le demi-espace positif défini par $\nabla_u(0)$), et N_u le cône isotrope de la dérivée seconde de l_u en 0. Si ∇_u est nul, $H_u = \mathbb{R}^n$ et H_u^+ est vide.

Lemme 2.4 *On suppose que les longueurs sont convexes. Pour $T \subset S(0)$ et pour X orthogonal aux gradients de T, on pose*

$$T_1(X) := \{u \in T, X \in N_u\}.$$

On suppose que pour tout X orthogonal aux gradients des longueurs de T,

$$\bigcap_{u \in T_1(X)} H_u^+ \neq \varnothing$$

alors la condition C est vérifiée.

Preuve On choisit $y = y_0$ dans cette intersection et les autres y_i nuls. Si u n'est pas dans $T_1(X)$, la dérivée seconde de l_u agissant sur X est strictement positive par convexité donc, quitte à réduire y, on peut supposer que les coefficients $a_2(u)$ sont positifs pour $u \notin T_1(X)$. Si $u \in T_1(X)$, on a $a_2(u) = d_0 l_u . y > 0$ par choix de y . On obtient ainsi une solution de $\mathcal{S}$ à l'ordre 2. ■

Remarquons que cette condition est vérifiée en tout point non semi-eutactique.
Par définition, le noyau d'une forme multilinéaire symétrique F est l'ensemble

$$\{x \in \mathbb{R}^n, (y_1, \dots, y_p) \mapsto F(x, y_1, \dots, y_p) \equiv 0\}.$$

Proposition 2.2 *On suppose les longueurs convexes. Pour $T \subset S(0)$ et X orthogonal aux gradients de T, on pose $T_1(X) = \{u \in T, X \in N_u\}$. On suppose que pour tous T et X, on a les conditions suivantes:*

(1) *Pour tout $u \in T_1(X)$, N_u contient le noyau des dérivées de l_u d'ordre supérieur ou égal à 2.*
(2) *L'ensemble*

$$E = \Big[\bigcap_{u \in T_1(X)} H_u^+ \Big] \cup \Big[\Big(\bigcap_{u \in T_1(X)} H_u \Big) \cap \Big(\bigcap_{u \in T_1(X)} (\mathbb{R}^n \setminus N_u) \Big) \Big]$$

est non vide.

Alors la condition C est vérifée.

Preuve On choisit y dans E et on regarde $\mathcal{S}$ à l'ordre 4. Remarquons que E est stable par multiplication par un scalaire strictement positif et que E ne contient pas le vecteur nul.

Si u n'est pas dans $T_1(X)$, par convexité, on a $d_0^2 l_u . X^2 > 0$ et on peut choisir $\varepsilon > 0$ tel que $2\varepsilon d_0 l_u . y + d_0^2 l_u . X^2 > 0$.

Si $u \in T_1(X)$ et $y \in \bigcap_{u \in T_1(X)} H_u^+$, alors

$$2\varepsilon d_0 l_u.y + d_0^2 l_u.X^2 = 2\varepsilon d_0 l_u.y > 0.$$

Supposons donc que $u \in T_1(X)$ et que

$$y \in \Big(\bigcap_{u \in T_1(X)} H_u\Big) \cap \Big(\bigcap_{u \in T_1(X)} (\mathbb{R}^n \setminus N_u)\Big)$$

d'après l'hypothèse (1), le système $\mathbb{S}$ s'écrit:

$$a_2 = 0$$
$$a_3 = 0$$
$$a_4 = d_0^2 f.y^2 > 0 \quad \text{par convexité.}$$

La courbe $c(t) = tX + t^2 y$ réalise alors la condition C. ■

3 La condition C dans les sous-variétés totalement géodésiques de P_n

3.1 Généralités

On note P_n l'espace des matrices de Gram des réseaux marqués de déterminant 1, c'est-à-dire l'espace des matrices symétriques définies positives de déterminant 1. Cet espace est muni de la métrique

$$\langle X, Y\rangle_A = \mathrm{Tr}(A^{-1}XA^{-1}Y).$$

Pour cette métrique, on a une action transitive par isométries du groupe $\mathrm{SL}(n, \mathbb{R})$ définie par $g.A := gA^t g$ et P_n s'identifie à l'espace symétrique

$$\mathrm{SL}(n, \mathbb{R}) / \mathrm{SO}(n).$$

Les longueurs sont paramétrées par $\mathbb{Z}^n$ (ou $\mathbb{R}^n$) et sont définies sur cet espace par

$$l_u(A) := {}^t uAu.$$

Lorsque u est entier, l_u représente la longueur du vecteur associé à $u \in \mathbb{Z}^n$ dans le réseau marqué correspondant à A.

Soit G un sous-groupe de Lie connexe de $\mathrm{SL}(n, \mathbb{R})$, on s'intéresse à l'orbite de I sous l'action de G induite par celle de $\mathrm{SL}(n, \mathbb{R})$. Lorsque G est stable par transposition, on obtient une sous-variété totalement géodésique de P_n (*cf.* [Eb, p. 131]) isométrique à l'espace des paramètres de certaines familles de réseaux. Remarquons que G agit par isométries sur P_n et sur $G.I$. Par transitivité, on se ramène dans tous les cas à étudier la condition C en l'identité pour des longueurs paramétrées par $\mathbb{R}^n$.

Plus précisément, si $\Lambda = {}^t P_0.\mathbb{Z}^n$ est un réseau marqué, les matrices de Gram de la famille $G.\Lambda$ parcourent l'image isométrique $P_0(G.I)^t P_0$ de $G.I$. Par transitivité, il

https://doi.org/10.4153/CJM-2002-015-1 Published online by Cambridge University Press

est alors équivalent d'étudier l'invariant d'Hermite restreint à cette sous-variété et d'étudier le minimum sur $G.I$ des fonctions $l_{{}^tP_0.u}$, $u \in \mathbb{Z}^n \setminus \{0\}$.

En prenant différents sous-groupes, on obtient des sous-variétés totalement géodésiques de P_n isométriques aux espaces symétriques irréductibles de type non compact.

L'espace tangent en I à P_n est l'espace $S_n^0(\mathbb{R})$ des matrices réelles symétriques de trace nulle et la carte exponentielle en I est donné par l'exponentielle habituelle des matrices. L'expression des longueurs dans cette carte est donné par

$$\tilde{l}_u(X) = {}^t u e^X u.$$

On note $I_{p,q}$, J_{2n}, L_{4n}, $K_{p,q}$ et T_{2n} les matrices suivantes :

$$I_{p,q} = \begin{pmatrix} -I_p & 0 \\ 0 & I_q \end{pmatrix}$$

$$J_{2n} = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}$$

$$L_{4n} = \begin{pmatrix} J_{2n} & 0 \\ 0 & -J_{2n} \end{pmatrix}$$

$$K_{p,q} = \begin{pmatrix} I_{p,q} & 0 \\ 0 & I_{p,q} \end{pmatrix}$$

$$T_{2n} = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}.$$

Si G est un sous-groupe de $\mathrm{SL}(n,\mathbb{C})$, on plonge naturellement G comme sous-groupe de $\mathrm{SL}_{2n}(\mathbb{R})$ par l'application

$$\begin{array}{cccc} \Phi_{\mathbb{C}}\colon & M_n(\mathbb{C}) & \longrightarrow & M_{2n}(\mathbb{R}) \\ & Z = X + iY & \longmapsto & \begin{pmatrix} X & -Y \\ Y & X \end{pmatrix} \end{array}$$

et on regarde l'action de G sur P_n donnée par $\Phi_{\mathbb{C}}(G)$.

On note aussi $\theta_{\mathbb{C}}$ l'application de $\mathbb{C}^n \to \mathbb{R}^{2n}$ définie par

$$\theta_{\mathbb{C}}(x_1 + iy_1, \dots, x_n + iy_n) = (x_1, \dots, x_n, y_1, \dots, y_n).$$

Rappelons ici les propriétés de $\Phi_{\mathbb{C}}$ et $\theta_{\mathbb{C}}$ utiles par la suite :

Lemme 3.1 *Soient Z_1, Z_2 des matrices de $M_n(\mathbb{C})$,*

(1) $\Phi_{\mathbb{C}}$ *est injective.*
(2) $\Phi_{\mathbb{C}}(Z_1 Z_2) = \Phi_{\mathbb{C}}(Z_1)\Phi_{\mathbb{C}}(Z_2)$.
(3) ${}^t\Phi_{\mathbb{C}}(Z_1) = \Phi_{\mathbb{C}}({}^t\overline{Z_1})$.
(4) ${}^t\theta_{\mathbb{C}}(\mathbf{z}_1)\Phi_{\mathbb{C}}(Z)\theta_{\mathbb{C}}(\mathbf{z}_2) = \Re({}^t\overline{\mathbf{z}_1} Z \mathbf{z}_2)$.

https://doi.org/10.4153/CJM-2002-015-1 Published online by Cambridge University Press

(5) *$\theta_{\mathbb{C}}$ est un isomorphisme de $\mathbb{R}$-espaces vectoriels.*
(6) $\det\bigl(\Phi_{\mathbb{C}}(Z)\bigr) = |\det(Z)|^2$, *en particulier,* $\Phi_{\mathbb{C}}\bigl(\mathrm{SL}(n,\mathbb{C})\bigr)$ *est un sous-groupe de* $\mathrm{SL}(2n,\mathbb{R})$.

Soit $\mathbb{H}$ le corps des quaternions, pour $h \in \mathbb{H}$, on écrit $h = z_1 + jz_2$ avec $z_1, z_2 \in \mathbb{C}$. On note $\pi(z_1 + jz_2) = z_1$. On décompose de même les vecteurs de $\mathbb{H}^n$ et les matrices de $M_n(\mathbb{H})$. On pose

$$\begin{aligned} \Phi_{\mathbb{H}}\colon \quad M_n(\mathbb{H}) &\longrightarrow M_{2n}(\mathbb{C}) \\ Z_1 + jZ_2 &\longmapsto \begin{pmatrix} Z_1 & -\overline{Z_2} \\ Z_2 & \overline{Z_1} \end{pmatrix} \end{aligned}$$

$$\theta_{\mathbb{H}}(z_1 + jz_2) = (z_1, z_2)$$

$$i(z_1 + jz_2) = z_1 + j\overline{z_2}.$$

Les propriétés de $\theta_{\mathbb{H}}$ et $\Phi_{\mathbb{H}}$ suivantes sont immédiates :

Lemme 3.2 *Soit $H \in M_n(\mathbb{H})$ et $h \in \mathbb{H}^n$*

(1) $\Phi_{\mathbb{H}}(H)\theta_{\mathbb{H}}(h) = \theta_{\mathbb{H}}(Hh)$
(2) ${}^t\overline{\theta_{\mathbb{H}}(h_1)}T\theta_{\mathbb{H}}(h_2) = \pi\bigl(-j\,{}^t i(h_1)h_2\bigr)$.

Soit G un sous-groupe de Lie de $\mathrm{SL}(n,\mathbb{R})$, on note V_G l'orbite de l'identité sous l'action de G. Le stabilisateur de l'identité dans G est $G \cap O(n)$ et on obtient une sous-variété isométrique à

$$G/G \cap O(n).$$

Dans le cas d'un sous-groupe complexe, à travers $\Phi_{\mathbb{C}}$, on a $\mathrm{Stab}_G(I) = \{g \in G, {}^t\overline{g}g = I\} = G \cap U(n)$. L'espace tangent en I à V_G est donné par l'image de l'algèbre de Lie de G par l'application $g \mapsto {}^tg + g$. Dans le cas d'un sous-groupe de $\mathrm{SL}(n,\mathbb{C})$, l'espace tangent en I à V_G est l'image par $\Phi_{\mathbb{C}}$ de l'ensemble $\mathrm{Sym}(\mathfrak{g}) := \{{}^t\overline{g} + g, g \in \mathfrak{g}\}$, où $\mathfrak{g}$ est l'algèbre de Lie de G dans $\mathfrak{sl}(n,\mathbb{C}) = S_n^0(\mathbb{C})$.

Pour un sous-groupe de $\mathrm{SL}(n,\mathbb{R})$ qui donne une sous-variété totalement géodésique de P_n, on a le lemme suivant :

Lemme 3.3 *Soit X une matrice symétrique de trace nulle orthogonale aux gradients de $T \subset S(I)$, on suppose qu'il existe Y dans l'espace tangent en I à $G.I$ telle que*

$$\mathcal{S}_1 \begin{cases} {}^tuYu = 0 \\ Yu \neq 0 \end{cases}$$

pour tout $u \in S(I)$ tel que $Xu = 0$, alors $G.I$ vérifie la condition C.

Preuve On regarde la condition C dans la carte exponentielle en I, le système $\mathcal{S}$ à l'ordre 4 s'écrit

$$2\,{}^tuYu + |Xu|^2 = 0$$

$$6\,{}^tu(XY + YX)u + {}^tuX^3u = 0$$

$$24|Yu|^2 + 4\,{}^tu(X^2Y + XYX + YX^2)u + |X^2u|^2 > 0.$$

https://doi.org/10.4153/CJM-2002-015-1 Published online by Cambridge University Press

On remarque que $X \in N_u$ si et seulement si $Xu = 0$, donc que $u \in T_1(X)$ si et seulement si $Xu = 0$. Le vecteur X est alors dans le noyau des dérivées supérieures de l_u. On peut appliquer la proposition 2.2. La condition

$$Y \in \Big(\bigcap_{u \in T_1(X)} H_u \Big) \cap \Big(\bigcap_{u \in T_1(X)} (\mathbb{R}^n \setminus N_u) \Big)$$

s'écrit

$$tuYu = 0 \quad (Y \in H_u)$$
$$Yu \neq 0 \quad (Y \notin N_u)$$

pour tout $u \in T_1(X)$. ■

E. Cartan a donné la liste des espaces symétriques irréductibles. En étudiant chaque cas, on démontre le théorème suivant :

Théorème 3.1 *L'invariant d'Hermite restreint à un espace symétrique irréductible non exceptionnel de type III ou IV plongé dans P_n vérifie un théorème de Voronoï.*

Donnons de suite la liste des cas à considérer. Les notations pour les groupes sont celles de Helgason [He].

Type III $P_n = \mathrm{SL}(n,\mathbb{R})/\mathrm{SO}(n)$, $\mathrm{SU}^*(2n)/\mathrm{Sp}(n)$, $\mathrm{SU}(p,q)/S(U_p \times U_q)$, $\mathrm{SO}_0(p,q)/\mathrm{SO}(p)\times\mathrm{SO}(q)$, $\mathrm{SO}^*(2n)/U(n)$, $\mathrm{Sp}(p,q)/\mathrm{Sp}(p)\times\mathrm{Sp}(q)$, $\mathrm{Sp}(n,\mathbb{R})/U(n)$.

Type IV $\mathrm{SL}_n(\mathbb{C})/\mathrm{SU}(n)$, $\mathrm{SO}(n,\mathbb{C})/\mathrm{SO}(n)$, $\mathrm{Sp}(n,\mathbb{C})/\mathrm{Sp}(n)$.

Rappelons que dans tous les cas, par transitivité, on se ramène à une famille finie de longueurs paramétrées par $\mathbb{R}^n$ (plus précisément de la forme $l_{{}^tP_0u}(A)$, $u \in \mathbb{Z}^n \setminus \{0\}$, $A \in G.I$) au voisinage de l'identité.

On ne traitera pas le cas des espaces P_n, $\mathrm{SO}_0(p,q)/\mathrm{SO}(p)\times\mathrm{SO}(q)$, $\mathrm{Sp}(n,\mathbb{R})/U(n)$ pour lesquels la condition C est connue [Ba].

3.2 G-réseaux et réseaux sur des anneaux d'entiers

Soit ρ une représentation d'un groupe fini G dans $\mathrm{SL}(n,\mathbb{Z})$, on s'intéresse aux réseaux marqués invariants sous $\rho(G)$.

On se donne donc un sous-groupe de $\mathrm{SL}(n,\mathbb{Z})$ et on note E l'ensemble des réseaux marqués stables par G. Soit P une matrice de $\mathrm{SL}(n,\mathbb{R})$ qui commute avec G, alors le réseau ${}^tP.\mathbb{Z}^n$ est stable par G. Réciproquement, soit $\Lambda = {}^tP.\mathbb{Z}^n$ un réseau G-stable, alors ${}^tPg.\mathbb{Z}^n = g^tP.\mathbb{Z}^n$ et donc ${}^tP^{-1}g^{-1t}Pg \in \mathrm{SL}(n,\mathbb{Z})$ pour tout $g \in G$. Pour P suffisament petit, P doit donc appartenir au commutant de ${}^tG$ dans $\mathrm{SL}(n,\mathbb{R})$.

Réseaux complexes Soit (E,H) un espace Hermitien, on considère les $\mathbb{Z}[i]$-modules de rang maximal dans E. Tout $\mathbb{Z}[i]$-module est aussi un réseau dans l'espace Euclidien associé à (E,H) et la norme d'un tel réseau et égale à sa norme pour la forme Hermitienne H. Soit $P_n^{\mathbb{C}}$ l'espace des matrices de "Gram" complexes, c'est-à-dire l'espace des matrices Hermitiennes de déterminant 1 et soit $\mathcal{E}$ l'espace des $\mathbb{Z}[i]$-modules marqués. À une base $e_i = {}^t\overline{P}.\varepsilon_i$, on associe la matrice $P^t\overline{P} \in P_n^{\mathbb{C}}$. Ceci permet d'identifier $\mathcal{E}$ modulo isométries complexes à $P_n^{\mathbb{C}}$. D'autre part, à travers $\Phi_{\mathbb{C}}$, on vérifie que $P_n^{\mathbb{C}}$ s'identifie aussi à l'orbite de l'identité dans P_{2n} sous l'action du sous-groupe $\Phi_{\mathbb{C}}\big(\mathrm{SL}(n,\mathbb{C})\big)$ qui est le commutant dans $\mathrm{SL}(2n,\mathbb{R})$ de la matrice J_{2n}.

On peut identifier ces réseaux aux réseaux stables pour la représentation de $G = \mathbb{Z}/4\mathbb{Z}$ définie par $\rho(1) = J_{2n}$.

Les $\mathbb{Z}[i]$-modules marqués sont ainsi paramétrés par

$$V_{\mathrm{SL}(n,\mathbb{C})} = \mathrm{SL}(n,\mathbb{C}).I.$$

On regarde le stabilisateur de l'identité pour cette action. On a

$$\mathrm{Stab}_{\mathrm{SL}(n,\mathbb{C})}(I) = \mathrm{SL}(n,\mathbb{C}) \cap U(n) = \mathrm{SU}(n)$$

et

$$V_{\mathrm{SL}(n,\mathbb{C})} \simeq \mathrm{SL}(n,\mathbb{C})/\,\mathrm{SU}(n).$$

Puisque ${}^tJ_{2n} = -J_{2n}$, ce sous-groupe est stable par transposition.

Réseaux quaternioniques De même, soit (E,S) un espace vectoriel quaternionique à droite munit d'une forme sesquilinéaire. Par définition, le déterminant d'une matrice de $M_n(E)$ sera celui de la matrice complexe associée à travers $\Phi_{\mathbb{H}}$. On considère alors les $\mathbb{Z}[i,j,k]$-modules à droite de rang n. Ces modules peuvent être considérés en particulier comme des $\mathbb{Z}[i]$-modules de rang $2n$. De la même manière que pour les réseaux complexes, on peut identifier l'espace de ces $\mathbb{Z}[i,j,k]$-modules avec un sous-espace de $P_{2n}^{\mathbb{C}}$. Cet espace s'identifie à l'ensemble des matrices qui commutent avec la multiplication à droite par j, on vérifie que c'est l'orbite de l'identité sous l'action de $\mathrm{SU}^*(2n)$ dans $P_{2n}^{\mathbb{C}}$ où $\mathrm{SU}^*(2n)$ le sous-groupe de $\mathrm{SL}_{2n}(\mathbb{C})$ formé des matrices qui commutent avec la transformation réelle

$$\psi\colon (z_1,\dots,z_{2n}) \mapsto (\overline{z_{n+1}},\dots,\overline{z_{2n}},-\overline{z_1},\dots,-\overline{z_n}).$$

Remarquons qu'on peut ici prendre la représentation de

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

définie par $\rho(i) = L_{4n}$, $\rho(j) = J_{4n}$.

On vérifie alors que $\Phi_{\mathbb{C}}\big(\mathrm{SU}^*(2n)\big)$ s'identifie au commutant dans $\mathrm{SL}(4n,\mathbb{R})$ des matrices J_{4n} et L_{4n}. Le stabilisateur de I est $U(2n) \cap \mathrm{SU}^*(2n) = \mathrm{Sp}(n)$ (voir [He, pp. 343, 344]).

Proposition 3.1 *Soit G un sous-groupe de $\mathrm{SL}(n,\mathbb{R})$ stable par transposition et défini par des relations de commutation dans $M_n(\mathbb{R})$, alors V_G vérifie la condition C.*

Preuve Par linéarité, l'algèbre de Lie de G et l'espace tangent en I à V_G sont définis par les mêmes relations. Si X est une matrice de $T_I V_G$, on pose

$$Y = \frac{\mathrm{Tr}(X^2)}{n} I - X^2$$

et $c(t) = tX + t^2 Y$. On vérifie que Y appartient à l'espace tangent en I. De plus,

$$\langle \nabla_u(I), Y \rangle = {}^t uYu = 2\frac{\mathrm{Tr}(X^2)}{n}|u|^2 > 0$$

pour tout $u \in S(I)$. On a donc $Y \in \bigcap_{u \in T_1(X)} H_u^+$ et on applique le lemme 2.4. ∎

Le corollaire suivant est alors immédiat :

Corollaire 3.1

$$V_{\mathrm{SL}(n,\mathbb{C})} \simeq \mathrm{SL}(n,\mathbb{C}) / \mathrm{SU}(n)$$

et

$$V_{\mathrm{SU}^*(2n)} \simeq \mathrm{SU}^*(2n) / \mathrm{Sp}(n)$$

vérifient la condition C.

Exemples

(1) Ce lemme permet de retrouver la condition C dans P_n qui est seulement l'orbite du commutant de l'identité. Plus généralement, celle-ci est vérifiée pour les réseaux G-stables lorsque G est un sous-groupe fini de $\mathrm{SL}(n,\mathbb{Z})$ (*cf.* [B-M2] pour le théorème de Voronoï).

(2) Soit V le sous-ensemble de P_n formé par les réseaux qui se décompo sent en somme orthogonale $\Lambda_1 \perp \cdots \perp \Lambda_k$ avec Λ_i de dimension n_i. En choisissant une base de chaque Λ_i, on voit que la matrice de Gram de Λ se décompose en une matrice diagonale par bloc de taille n_i, $1 \le i \le k$. En particulier, on peut trouver une matrice g de $\mathrm{SL}(n,\mathbb{R})$ qui commute avec la matrice diagonale par bloc $D = \mathrm{diag}(I_{n_1}, 2I_{n_2}, \ldots, kI_{n_k})$ et telle que $\mathrm{Gram}(\Lambda) = g.I$. D'un autre coté, l'orbite de I sous l'action du commutant de D est l'ensemble des matrices symétriques G de determinant 1 telles que $G = DGD^{-1}$. On vérifie alors par récurrence sur k que $G.I = V$. La famille de réseaux formées par les réseaux qui se décomposent en somme orthogonale $\Lambda = \Lambda_1 \perp \cdots \perp \Lambda_k$ vérifie la condition C.

3.3 Familles de réseaux orthogonaux

Soit E un espace Euclidien et σ une isométrie de E telle que $\sigma^2 = \mathrm{Id}$, $\sigma \neq \pm\mathrm{Id}$. Un réseau Λ est σ-orthogonal si σ est une isométrie de Λ sur son dual. Quitte à

https://doi.org/10.4153/CJM-2002-015-1 Published online by Cambridge University Press

choisir une base de E, on peut supposer que la matrice de σ est $I_{p,q}$. Les réseaux σ-orthogonaux forment alors une ou deux orbites du groupe $\mathrm{SO}_0(p,q)$ ([B-M3]). On obtient des sous-variétés totalement géodésiques isométriques à l'espace symétrique

$$\mathrm{SO}_0(p,q)/\,\mathrm{SO}(p)\times\mathrm{SO}(q),$$

pour lequel la condition C est connue.

Réseaux orthogonaux complexes Si Λ est un $\mathbb{Z}[i]$-module dans un espace Hermitien E, on note $\Lambda^*_{\mathbb{C}}$ son dual complexe, c'est-à-dire l'ensemble des vecteurs y tels que $H(x,y)\in\mathbb{Z}[i]$ pour tout $x\in\Lambda$. Quitte à choisir une base, on peut supposer que Λ est un $\mathbb{Z}[i]$-module dans $\mathbb{C}^n$. On note $\Lambda_{\mathbb{C}}$ ce $\mathbb{Z}[i]$-module et $\Lambda_{\mathbb{R}}$ le réseau image de $\Lambda_{\mathbb{C}}$ par $\theta_{\mathbb{C}}$. On vérifie facilement que le dual de $\Lambda_{\mathbb{R}}$ est l'image du dual complexe de $\Lambda_{\mathbb{C}}$. Supposons maintenant que $\Lambda_{\mathbb{C}}$ admette un automorphisme Hermitien σ de $\Lambda_{\mathbb{C}}$ sur $\Lambda^*_{\mathbb{C}}$ tel que $\sigma^2=Id$, alors le réseau $\Lambda_{\mathbb{R}}$ est σ-orthogonal.

Soit $\mathcal{E}$ l'espace des réseaux σ-orthogonaux complexes, en procédant comme dans [B-M3], on vérifie que si Λ est un tel réseau et si $g\in\mathrm{SL}(n,\mathbb{C})$,

$$g.\Lambda\in\mathcal{E}\iff {}^t\overline{g}\sigma g\in\sigma.\,\mathrm{Aut}(\Lambda).$$

Par connexité de $\mathrm{SU}(p,q)$, la composante connexe dans $\mathcal{E}$ d'un tel réseau est l'orbite de ce réseau sous l'action de $\mathrm{SU}(p,q)$, et $\mathcal{E}$ est réunion finie de telles orbites. De plus, par transitivité de $\mathrm{SL}(n,\mathbb{R})$, toutes les orbites sont isométriques à l'orbite de l'identité $\mathrm{SU}(p,q).I$. Le stabilisateur de l'identité est $S(U_p\times U_q)$ et on obtient ainsi une réunion d'images isométriques de

$$V_{\mathrm{SU}(p,q)}\simeq\mathrm{SU}(p,q)/S(U_p\times U_q).$$

On a

$$\mathrm{SU}(p,q)=\{g\in\mathrm{SL}_{p+q}(\mathbb{C}),{}^t\overline{g}I_{p,q}g=I_{p,q}\}$$

$$S(U_p\times U_q)=\left\{\begin{pmatrix}g_1&0\\0&g_2\end{pmatrix},g_1\in U(p),g_2\in U(q),\det(g_1)\det(g_2)=1\right\}$$

$$\mathfrak{su}(p,q)=\{g\in M^0_{p+q}(\mathbb{C}),{}^t\overline{g}I_{p,q}+I_{p,q}g=0\}$$

$$\mathrm{Sym}\big(\mathfrak{su}(p,q)\big)=\left\{g=\begin{pmatrix}0&Z\\{}^t\overline{Z}&0\end{pmatrix},Z\in M_{p,q}(\mathbb{C})\right\}.$$

Proposition 3.2 *$V_{\mathrm{SU}(p,q)}\simeq\mathrm{SU}(p,q)/S(U_p\times U_q)$ vérifie la condition C.*

Preuve Le système $\mathcal{S}_1$ s'écrit à travers $\Phi_{\mathbb{C}}$ de la manière suivante :

$$\Re({}^t\overline{z}Y_{\mathbb{C}}z)=0$$

$$Y_{\mathbb{C}}z=0.$$

$Y_{\mathbb{C}}$ doit se décomposer sous la forme $\left(\begin{smallmatrix} 0 & Y \\ {}^t\overline{Y} & 0 \end{smallmatrix}\right)$. De même, si X est une matrice orthogonale aux gradients de T, X se décompose sous la forme $\left(\begin{smallmatrix} 0 & X \\ {}^t\overline{X} & 0 \end{smallmatrix}\right)$ à travers $\Phi_{\mathbb{C}}$ et $T_1(X) = \{u \in T, Xu = 0\}$ s'identifie par $\theta_{\mathbb{C}}$ à l'ensemble $\tilde{T}_1 := \{(z_1, z_2, Xz_2 = {}^t\overline{X}z_1 = 0\}$.

Soit A (respectivement B) le sous-espace vectoriel de $\mathbb{C}^p$ (respectivement $\mathbb{C}^q$) engendré par les z_1 tels que $(z_1, z_2) \in \tilde{T}_1$ (respectivement les z_2 tels que $(z_1, z_2) \in \tilde{T}_1$). A et B sont différents de $\mathbb{C}^p$ et $\mathbb{C}^q$. Il existe $u\colon \mathbb{C}^q \to \mathbb{C}^p$ avec $u(A) \subset B^\perp$, ${}^t\overline{u}(B) \subset A^\perp$ et $u(z_1)$ ou ${}^t\overline{u}(z_2)$ non nul dès que $(z_1, z_2) \in \tilde{T}_1$ (on rappelle que $\tilde{T}_1$ est *fini*). Si Y_1 est la matrice de u dans les bases canoniques, on vérifie que la matrice

$$Y = \begin{pmatrix} 0 & Y_1 \\ {}^t\overline{Y_1} & 0 \end{pmatrix}$$

résout $\mathcal{S}_1$. ■

Réseaux orthogonaux quaternioniques Soit σ une isométrie de carré Id sur un espace quaternionique muni d'une forme sesquilinéaire (E, S). On s'intéresse aux réseaux quaternioniques tels que σ soit une isométrie de Λ sur son dual

$$\Lambda^*_{\mathbb{H}} = \{y \in E, S(x, y) \in \mathbb{Z}[i, j] \text{ pour tout } x \in \Lambda\}.$$

Comme pour les orthogonaux complexes, on vérifie que l'espace des paramètres de tels réseaux s'identifie à une réunion d'images isométriques de

$$\begin{gathered} V_{\mathrm{Sp}(p,q)} \simeq \mathrm{Sp}(p,q)/\mathrm{Sp}(p) \times \mathrm{Sp}(q) \\ \mathrm{Sp}(p,q) = \{g \in \mathrm{Sp}(p+q, \mathbb{C}), {}^t g K_{p,q} \overline{g} = K_{p,q}\} \\ \mathfrak{sp}(p,q) = \{g \in \mathfrak{sp}(p+q, \mathbb{C}), {}^t g K_{p,q} + K_{p,q} \overline{g} = 0\} \\ \mathrm{Sym}\big(\mathfrak{sp}(p,q)\big) = \left\{ \begin{pmatrix} 0 & Z_1 & 0 & Z_2 \\ {}^t\overline{Z_1} & 0 & {}^t Z_2 & 0 \\ 0 & \overline{Z_2} & 0 & -\overline{Z_1} \\ {}^t\overline{Z_2} & 0 & -{}^t Z_1 & 0 \end{pmatrix} \right\}. \end{gathered}$$

Proposition 3.3 $V_{\mathrm{Sp}(p,q)} \simeq \mathrm{Sp}(p,q)/\mathrm{Sp}(p) \times \mathrm{Sp}(q)$ *vérifie la condition C.*

Preuve À travers $T\Phi_{\mathbb{H}}$, on identifie $\mathrm{Sym}\big(\mathfrak{sp}(p,q)\big)$ à

$$\left\{ H \in M_n(\mathbb{H}), H = \begin{pmatrix} 0 & Z_1 + jZ_2 \\ {}^t Z_1 + j{}^t\overline{Z_2} & 0 \end{pmatrix} \right\}$$

et le système $\mathcal{S}_1$ s'écrit

$$\pi\big(-j^t i(h) H h\big) = Hh \neq 0$$

où on a identifié $T_1(X)$ à un sous-ensemble fini de $\mathbb{H}^n$.

On décompose les vecteurs de $\mathbb{H}^n$ en (h_1, h_2) et soit A (respectivement B) le sous-espace engendré par les h_1 tels que $(h_1, h_2) \in T_1(X)$ (respectivement les h_2 tels que $(h_1, h_2) \in T_1(X)$) et soit N un supplémentaire de B dans $\mathbb{H}^n$. On munit $\mathbb{H}^n$ de la forme ${}^t i(h)h'$. Il existe une application linéaire u de B dans $A^\perp$ telle que $u(h_2) \neq 0$ si $h_2 \neq 0$. D'autre part, $\bigcup_{h_1 \neq 0} h_1^\perp$ est une réunion finie d'hyperplans, donc il existe une application v de N dans $\mathbb{H}^p$ telle que $v(N) \not\subset \bigcup_{h_1 \neq 0} h_1^\perp$. On pose

$$\phi = \begin{cases} u & \text{sur } B \\ v & \text{sur } N. \end{cases}$$

Soit Y la matrice de ϕ, on pose

$$H = \begin{pmatrix} 0 & Y \\ {}^t i(Y) & 0 \end{pmatrix}$$

et on vérifie que H résout $\mathcal{S}_1$. ■

3.4 Réseaux autoduaux

Soit $(E, \langle ., . \rangle)$ un espace complexe (respectivement quaternionique) muni d'une forme bilinéaire symétrique non dégénérée. Quitte à prendre une base orthogonale, on peut supposer que $E = \mathbb{C}^n$ (respectivement $E = \mathbb{H}^n$), $\langle x, y \rangle = {}^t xy$ (respectivement $({}^t z_1 - j{}^t\overline{z_2})(z_1' + jz_2')$). Si Λ est un réseau de E, on note Λ^0 son dual par rapport à la forme $\langle ., . \rangle$ et à l'anneau $\mathbb{Z}[i]$ (respectivement $\mathbb{Z}[i, j, k]$). On s'intéresse aux réseaux tels que $\Lambda = \Lambda^0$. Comme précédemment, on peut vérifier que l'on obtient des images isométriques de

$$V_{\mathrm{SO}(n,\mathbb{C})} \simeq \mathrm{SO}(n, \mathbb{C}) / \mathrm{SO}(n)$$

(respectivement $V_{\mathrm{SO}^*(2n)} \simeq \mathrm{SO}^*(2n)/U(n)$).

$$\mathrm{SO}(n, \mathbb{C}) = \{g \in \mathrm{SL}(n, \mathbb{C}), {}^t gg = I\}$$

$$\mathfrak{so}(n, \mathbb{C}) = \{g \in M_n^0(\mathbb{C}), {}^t g + g = 0\}$$

$$\mathrm{Sym}\big(\mathfrak{so}(n, \mathbb{C})\big) = \{iY, Y \in M_n(\mathbb{C}), {}^t Y + Y = 0\}$$

Proposition 3.4 *$V_{\mathrm{SO}(n,\mathbb{C})} \simeq \mathrm{SO}(n, \mathbb{C}) / \mathrm{SO}(n)$ vérifie la condition C.*

Preuve L'espace tangent en I est $\left\{ \left(\begin{smallmatrix} 0 & -Y \\ Y & 0 \end{smallmatrix}\right), Y + {}^t Y = 0 \right\}$. On décompose $u \in \mathbb{R}^{2n}$ en (a, b), alors $T_1(X) = \{(a, b), Xa = Xb = 0\}$.

Soit α l'endomorphisme représenté par X dans la base canonique de $\mathbb{R}^n$, alors $\ker \alpha^\perp$ est stable par α. Soit e_i une base de $\mathbb{R}^n$ dans laquelle X s'écrit $\left(\begin{smallmatrix} X_1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ avec X_1 inversible. Soit β un endomorphisme de $\ker X$ sur $(\ker X)^\perp$ tel que $\beta(a_i) \neq 0$, $\beta(b_i) \neq 0$ dès que a_i et b_i sont non nuls, Y_1 la matrice de β dans la base e_i. On pose

$$Y = \begin{pmatrix} 0 & Y_1 \\ -{}^t Y_1 & 0 \end{pmatrix}$$

et $\tilde{\beta}$ l'endomorphisme représenté par y dans la base e_i. Si Y_2 est la matrice de $\tilde{\beta}$ dans la base canonique, on vérifie que

$$\begin{pmatrix} 0 & -Y_2 \\ Y_2 & 0 \end{pmatrix}$$

résout $\mathcal{S}_1$ dans $\Phi_{\mathbb{C}}\Big(\operatorname{Sym}\big(\mathfrak{so}(n,\mathbb{C})\big)\Big)$. ∎

Proposition 3.5 *$V_{\mathrm{SO}^*(2n)} \simeq \mathrm{SO}^*(2n)/U(n)$ vérifie la condition C.*

$$\mathrm{SO}^*(2n) = \{g \in \mathrm{SO}(2n,\mathbb{C}), {}^t\overline{g} J_{2n} g = J_{2n}\}$$
$$\mathfrak{so}^*(2n) = \{g \in M_{2n}(\mathbb{C}), {}^t g + g = 0, {}^t\overline{g} J_{2n} + J_{2n} g = 0\}$$
$$\operatorname{Sym}\big(\mathfrak{so}^*(2n)\big) = \left\{ i \begin{pmatrix} Y_1 & Y_2 \\ Y_2 & -Y_1 \end{pmatrix}, Y_1, Y_2 \textit{ réelles}, \begin{matrix} Y_1 + {}^tY_1 = 0, \\ Y_2 + {}^tY_2 = 0, \end{matrix} \right\}$$

Preuve Soit $X \in T_I V_{\mathrm{SO}^*(2n)}$, X s'écrit

$$\begin{pmatrix} 0 & -\tilde{X} \\ \tilde{X} & 0 \end{pmatrix}$$

et $\tilde{X}$ est de la forme

$$\begin{pmatrix} X_1 & X_2 \\ X_2 & -X_1 \end{pmatrix} = T\Phi_{\mathbb{C}}(\tilde{X}_{\mathbb{C}} = X_2 + iX_1).$$

$T_1(X)$ s'identifie à un sous-ensemble fini de $\mathbb{C}^n$.

La condition C pour $\mathrm{SO}^*(2n)$ se ramène alors au problème suivant : soit X une matrice complexe antisymétrique, z_i une famille finie de vecteurs non nuls de $\operatorname{Ker} X$, il existe Y antisymétrique telle que $Yz_i \neq 0$ et ${}^t z_i Y z_i = 0$. X étant antisymétrique, elle s'écrit

$${}^tG \begin{pmatrix} X_1 & 0 \\ 0 & 0 \end{pmatrix} G$$

avec $G \in \mathrm{SL}_n(\mathbb{C})$ et X_1 inversible. $G^{-1}z_i$ est donc de la forme $(0, \alpha_i)$. On choisit alors Y_0 telle que $Y_0\alpha_i \neq 0$ et on pose

$$\tilde{Y} = \begin{pmatrix} 0 & Y_0 \\ -{}^tY_0 & 0 \end{pmatrix}.$$

On vérifie que $Y = {}^tG^{-1}\tilde{Y}G^{-1}$ résout le système associé. ∎

https://doi.org/10.4153/CJM-2002-015-1 Published online by Cambridge University Press

3.5 Réseaux symplectiques

Pour terminer, on regarde les réseaux réels (respectivement complexes) σ-isoduaux pour une isométrie (respectivement une isométrie complexe) σ de carré $-\mathrm{Id}$. L'ensemble de ces réseaux est l'orbite de l'identité sous l'action de $\mathrm{Sp}(n,\mathbb{R})$ (respectivement $\mathrm{Sp}(n,\mathbb{C})$).

$$\mathrm{Sp}(n,\mathbb{C}) = \{g \in \mathrm{Gl}_{2n}(\mathbb{C}), {}^t g J_{2n} g = j_{2n}\}$$

$$\mathfrak{sp}(n,\mathbb{C}) = \{g \in M_n(\mathbb{C}), {}^t g J_{2n} + J_{2n} g = 0\}$$

$$\mathrm{Sym}\big(\mathfrak{sp}(n,\mathbb{C})\big) = \left\{ \begin{pmatrix} Z_1 & Z_2 \\ \overline{Z_2} & -\overline{Z_1} \end{pmatrix}, {}^t\overline{Z_1} = Z_1, {}^t Z_2 = Z_2 \right\}$$

Proposition 3.6 *$V_{\mathrm{Sp}(n,\mathbb{C})} \simeq \mathrm{Sp}(n,\mathbb{C})/\mathrm{Sp}(n)$ vérifie la condition C.*

Preuve Les éléments de $\mathrm{Sym}\big(\mathfrak{sp}(n,\mathbb{C})\big)$ sont de la forme $T\Phi_{\mathbb{H}}(Z_1 + jZ_2)$ avec ${}^t Z_1 = Z_1, {}^t\overline{Z_2} = Z_2$. On identifie $T_1(X)$ à un sous-ensemble de $\mathbb{H}^n$ et on définit A comme le sous-espace de $\mathbb{H}^n$ engendré par les éléments de $T_1(X)$. Quitte à changer de base, on peut supposer que X est de la forme

$$\begin{pmatrix} X_1 & 0 \\ 0 & 0 \end{pmatrix}.$$

On choisit alors $Y_0 = Z_1 + jZ_2$ telle que $Yh \neq 0$ pour $h \in T_1(X)$ et on pose

$$Y = \begin{pmatrix} 0 & Z_1 + jZ_2 \\ {}^t Z_1 + j^t\overline{Z_2} & 0 \end{pmatrix}. \qquad \blacksquare$$

Références

[Ba] C. Bavard, *Systole et invariant d'Hermite.* J. Reine Angew. Math. **482**(1997), 93–120.

[B-M1] A. M. Bergé and J. Martinet, *Sur un problème de dualité lié aux sphères en géométrie des nombres.* J. Number Theory **32**(1989), 14–42.

[B-M2] ———, *Réseaux extrêmes pour un groupe d'automorphismes.* Astérisque **198–200**(1991), 41–66.

[B-M3] ———, *Densité dans des familles de réseaux, application aux réseaux isoduaux.* Enseign. Math. **41**(1995), 335–365.

[Co] R. Coulangeon, *Réseaux k-extrêmes.* Proc. London. Math. Soc. (3) **73**(1996), 555–574.

[Eb] P. Eberlein, *Structure of manifolds of non positive curvature.* Lecture Notes in Math. **1156**(1984), 86–153.

[He] S. Helgason, *Differential geometry and symmetric spaces.* Pure and Applied Mathematics **12**, Academic Press, 1962.

[Ra] R. A. Rankin, *On positive definite quadratic forms.* J. London Math. Soc. **28**(1953), 309–314.

[Sch] P. Schmutz, *Riemann surfaces with shortest geodesic of maximal length.* Geom. Funct. Anal. (6) **3**(1993), 564–631.

[Vo] G. Voronoï, *Nouvelles applications des paramètres continus à la théorie des formes quadratiques, premier mémoire, Sur quelques propriétés des formes quadratiques positives parfaites.* J. Reine Angew. Math. **133**(1908), 97-178.
[Wo] S. Wolpert, *Geodesic length functions and the Nielsen problem.* J. Differential Geom. **25**(1987), 275–296.

Mathématiques Pures de Bordeaux
U. M. R. 5467 C. N. R. S.
Université Bordeaux-I
351, avenue de la Libération
F-33405 TALENCE Cedex
France