ANDRÉ WEIL

Groupes des formes quadratiques indéfinies et des formes bilinéaires alternées

Séminaire Henri Cartan, tome 10, n° 1 (1957-1958), exp. n° 2, p. 1-14
<http://www.numdam.org/item?id=SHC_1957-1958__10_1_A2_0>

GROUPES DES FORMES QUADRATIQUES INDÉFINIES ET DES FORMES BILINÉAIRES ALTERNÉES

par André WEIL

1. Quelques concepts généraux. Comme précédemment, soient G un groupe semi-simple non compact, K un sous-groupe maximal de G, Γ un sous-groupe discret de G. L'espace homogène G/K est l'espace riemannien symétrique associé à G.

On est amené à considérer les propriétés suivantes de Γ :

(I). $v(G/\Gamma) < + \infty$ (v désigne bien entendu le volume invariant, ou mesure de Haar, sur G ; il est invariant à droite et à gauche, parce que G est semi-simple, et se transporte à G/Γ d'une manière évidente).

(II). Il existe dans G un ouvert U de mesure finie (i.e. $v(U) < + \infty$) tel que $U\Gamma = G$ (autrement dit, l'image de U dans G/Γ est G/Γ), et que $U^{-1}U \cap \Gamma$ soit fini (autrement dit, il n'y a qu'un nombre fini d'éléments $\gamma \in \Gamma$ tels que $U\gamma$ rencontre U).

(III). G/Γ est compact.

Il est clair que (III) $\Longrightarrow$ (II) $\Longrightarrow$ (I). Mais, entre (II) et (III), il y a lieu d'insérer une propriété de plus ; pour l'énoncer, on introduit la notion suivante. Deux groupes Γ, Γ' sont dits commensurables si $\Gamma \cap \Gamma'$ est d'indice fini dans Γ et dans Γ'. On démontre sans peine que c'est là, pour les sous-groupes d'un groupe G donné, une relation d'équivalence. Il s'ensuit que les $x \in G$ tels que $x\Gamma x^{-1}$ soit commensurable à Γ forment un groupe $\tilde{\Gamma}$ (dit "groupe des transformations" de G/Γ), et que, si Γ et Γ' sont commensurables, les "groupes de transformations" $\tilde{\Gamma}$, $\tilde{\Gamma}'$ qui leur sont associés coïncident, ce qui implique en particulier que $\Gamma' \subset \tilde{\Gamma}$. Cela posé, on s'intéresse aussi à la propriété :

(M). Il existe dans G un ouvert U de mesure finie, tel que $KU = U$ (U est "saturé" par rapport à K, ou encore est l'image réciproque, par l'application canonique de G sur G/K, d'un ouvert de G/K), que $U\Gamma = G$, et que $U^{-1}U \cap x\Gamma$ soit fini quel que soit $x \in \tilde{\Gamma}$.

(On observera que, dans le groupe $\tilde{\Gamma}$, toute classe à gauche suivant Γ est contenue dans une réunion finie de classes à droite, et réciproquement, de sorte que, dans la dernière condition de (M), on peut écrire Γx au lieu de $x\Gamma$ sans rien changer).

Il est clair que (III) $\Longrightarrow$ (M) $\Longrightarrow$ (II). Si (II) est satisfaite, SIEGEL dit que Γ est "de première espèce". Si (M) est satisfaite, on propose de dire que Γ est "minkowskien" dans G. Les théorèmes énoncés dans le premier exposé disent essentiellement que, dans le groupe $G_o = PL_+(\mathbb{R},n)$, le groupe $\Gamma_o = PL(\mathbb{Z},n)$ ("groupe modulaire") est minkowskien ; dans ce cas, on vérifie facilement que le groupe des transformations $\tilde{\Gamma}_o$ associé à Γ_o est $PL_+(\mathbb{Q},n)$; on prend pour ensemble U l'un des ouverts $S_o(t)$, $S'_o(u)$ introduits précédemment ; le fait que (M) est vérifié (et non seulement (II)) est précisément le théorème de Siegel. Ce même exemple montre que (M) n'entraîne pas (III) ; en revanche, on ignore, (pour parler plus prudemment, le conférencier ignore) si (I), (II), (M) sont vraiment distinctes. En dehors des groupes fuchsiens, pour lesquels on possède des modes de définition géométriques (par un "polygone fondamental") et, comme dirait l'autre, fonction-théorétiques (revêtement universel de surfaces de Riemann avec ramifications données), il semble bien que tous les groupes connus satisfaisant à (I) soient des groupes à définition arithmétique, et qu'en vertu des travaux de Siegel on puisse affirmer que tous ces groupes sont minkowskiens.

[N.B. On peut donner de tous ces groupes "arithmétiques" une définition unique, comme suit : Soit A une algèbre semi-simple sur $\mathbb{Q}$, munie d'un antiautomorphisme involutif J ; soit $\mathfrak{M}$ un "module" dans A (sous-groupe additif de type fini de A, tel que $\mathfrak{M}\mathbb{Q} = A$). Soit $A_{\mathbb{R}}$ l'extension de A à $\mathbb{R}$, munie de l'antiautomorphisme qui étend J ; soit G le groupe des automorphismes de $A_{\mathbb{R}}$ (munie de J, c'est-à-dire groupe des automorphismes de l'algèbre $A_{\mathbb{R}}$ qui commutent avec J) ; G est semi-simple, et c'est même le groupe semi-simple "classique" le plus général ("classique" signifiant que G n'a aucun facteur qui soit un des groupes simples exceptionnels). On prend pour Γ le plus grand sous-groupe de G qui envoie $\mathfrak{M}$ dans $\mathfrak{M}$].

Il est facile de démontrer que, si (II) est satisfaite, Γ est engendré par les éléments de $U \cap U\gamma$, donc de type fini. On peut se demander si le groupe des relations entre ces générateurs de Γ est lui-même de type fini ; on démontre assez simplement qu'il en est ainsi, du moins, si $KU = U$ [travailler dans G/K, et se servir du fait connu que G/K est simplement connexe ; exercice recommandé aux lecteurs].

Enfin, il est immédiat que, si Γ est minkowskien, il en est de même de tout groupe commensurable à Γ ; en revanche, "on" ignore s'il peut arriver que, de deux groupes commensurables, l'un soit "de première espèce" et l'autre ne le soit pas. C'est même là une des raisons pour lesquelles il est recommandé de toujours travailler avec (M), plutôt qu'avec (II), malgré la complication apparente de la dernière partie de la condition (M).

2. Formes indéfinies. Soit, pour commencer, F une forme quadratique indéfinie non-dégénérée dans un vectoriel E de dimension n sur $\mathbb{R}$. Soit G le groupe orthogonal de F (groupe des automorphismes de E qui laissent F invariante). Soit E' le dual de E ; toute forme bilinéaire sur E détermine canoniquement, comme on sait, une application linéaire de E dans E' ; en particulier, la forme bilinéaire $F(x,y)$ associée à F, c'est-à-dire telle que $F(x) = F(x,x)$, déterminera une application linéaire f de E sur E', qui est symétrique (i.e. ${}^tf = f$) et de rang n.

Soit K un sous-groupe compact de G ; il laisse invariante, comme chacun sait, au moins une forme positive non dégénérée Φ ; soit φ l'application de E sur E' associée à Φ. On peut, par le choix d'une base convenable dans E (cf. Bourbaki, Alg., Chap. IX), mettre F, Φ sous la forme $F = \sum_i d_i x_i^2$, $\Phi = \sum_i x_i^2$; la matrice de $\varphi^{-1}f$, pour cette base, sera la matrice diagonale de coefficients $d_1, \dots, d_n$. Tout automorphisme de E qui laisse F et Φ invariantes commute évidemment à $\varphi^{-1}f$, ou autrement dit laisse invariants les sous-espaces E_ν de E formés respectivement des vecteurs propres de $\varphi^{-1}f$ par rapport aux valeurs propres de $\varphi^{-1}f$, valeurs propres qui ne sont autres que les d_i (ou plutôt les éléments distincts parmi ceux-ci). Soit E_+ (resp. E_-) la somme directe de ceux des E_ν qui sont associés à des valeurs propres >0 (resp. <0). Alors K est contenu dans le produit des groupes orthogonaux K_+, K_-, des formes induites respectivement dans E_+ et dans E_- par F ; K_+, K_- sont compacts, puisque F est positive (resp. négative) non dégénérée sur E_+ (resp. E_-). Par suite, pour que K soit sous-groupe compact maximal de G, il faut et il suffit qu'on ait $K = K_+ \times K_-$, ou autrement dit que K soit le groupe des automorphismes de E qui laissent invariantes F et une forme positive non dégénérée Φ telle que $\varphi^{-1}f$ n'ait pas d'autres valeurs propres que ± 1, ou, ce qui revient au même, telle que $(\varphi^{-1}f)^2 = 1$. Il est clair alors que les points de G/K (le riemannien symétrique associé à G) sont en correspondance biunivoque avec les Φ possédant cette propriété ; il revient au même de dire qu'ils sont en correspondance biunivoque avec les couples (E_+, E_-) de sous-espaces complémentaires de E tels que F induise sur E_+ une forme positive non dégénérée, et sur E_- une forme négative non dégénérée. D'ailleurs, s'il en est ainsi, E_+ et E_- sont orthogonaux l'un à l'autre, par rapport à F ; donc ils se déterminent réciproquement. D'ailleurs, si (p,q) est la signature de F , E_+ et E_- ont nécessairement les dimensions p,q . Enfin, en vertu de la loi d'inertie, si E_+ est un sous-espace de E de dimension p sur lequel F induise une forme positive non dégérée, F induit nécessairement sur l'orthogonal E_- de E_+ une forme négative non dégénérée, et réciproquement. Cela permet de représenter, canoniquement, G/K comme partie ouverte d'une grassmanienne (à savoir, soit la grassmanienne des sous-espaces de E de dimension p , soit celle des sous-espaces de E de dimension q) ; ces ouverts peuvent facilement être définis par des inégalités explicites.

Comme précédemment, soit P le cône convexe de toutes les formes positives non dégénérées dans E . A toute forme indéfinie non dégénérée F est associé, d'après ce qui précède, l'ensemble $V(F)$ des $\Phi \in P$ telles que $(\varphi^{-1}f)^2 = 1$. Il est clair que les $\Phi \in V(F)$ ont la propriété $\Phi(x) \geqslant |F(x)|$ quel que soit $x \in E$. Ces dernières inégalités définissent une partie convexe de P (fermée dans P) , dont $V(F)$ est la frontière (comme il résulte immédiatement de la possibilité de réduire simultanément F et une forme quelconque de P à la forme diagonale). On a, pour tout $x \in E$, $|F(x)| = \inf_{\Phi \in V(F)} \Phi(x)$, d'où s'ensuit aisément que F est déterminée, d'une manière unique au signe près, par $V(F)$. Tout cela subsiste d'ailleurs si F est "définie", mais devient sans intérêt, $V(F)$ étant alors réduit à $\{F\}$ ou bien à $\{-F\}$. On a l'habitude de dire par abus de langage, que les $\Phi \in V(F)$ sont les "majorantes" de F (ce sont en réalité les éléments frontières de l'ensemble des majorantes).

Le groupe $\mathcal{L}(E,E)$ opère transitivement dans P , comme on a vu, au moyen de $\Phi \to \Phi \circ X$ (pour l'application φ de E sur E' , canoniquement associée à Φ , cela s'écrit $\varphi \to {}^tX.\varphi.X$; ainsi en particulier si on écrit en matrices, après choix d'une base). Bien entendu, $V(F \circ X)$ est l'ensemble transformé de $V(F)$ par $\Phi \to \Phi \circ X$; en particulier, $V(F)$ est invariant par tout élément X du groupe orthogonal G de F ; la manière dont G opère sur $V(F)$ est celle même qu'on obtient en transportant à $V(F)$, au moyen de la correspondance biunivoque entre G/K et $V(F)$ définie ci-dessus, les opérations de G sur l'espace homogène G/K . Donc, pour étudier les propriétés locales de la bijection $G/K \to V(F)$, il suffit de les étudier au voisinage du point $\Phi = \sum x_i^2$, pour F donnée par $F = x_1^2 + \dots + x_p^2 - x_{p+1}^2 - \dots - x_n^2$. Cela ne fait pas de difficulté ; on en conclut que $V(F)$ est une variété analytique réelle, plongée dans P , et que $G/K \to V(F)$ est un isomorphisme au sens analytique réel (en particulier, c'est une application différentiable de rang égal à la dimension pq de G/K).

HERMITE introduisit les idées exposées ci-dessus (qu'on s'est contenté d'assaisonner de sauce bourbachique) en vue de la théorie arithmétique ("réduction") des formes quadratiques indéfinies. La pyramide convexe M ("domaine fondamental de Minkowski") étant définie dans P comme il a été dit dans l'exposé précédent, on dira que la forme indéfinie F est réduite si $V(F)$ rencontre M ; pour que cela ait un sens, il faut naturellement qu'on soit dans $\underset{\sim}{R}^n$, puisque la définition de M est relative à une base déterminée. On dira qu'une forme est à coefficients entiers s'il est ainsi de la matrice de la forme bilinéaire associée. Il est aisé de voir qu'il n'y a qu'un nombre fini de formes réduites à coefficients entiers de déterminant donné ($\neq 0$). Il revient au même de faire voir que l'ensemble des matrices B symétriques, à coefficients entiers, de déterminant donné $b \neq 0$, telles que $V(B) \cap S'(u) \neq \emptyset$, est fini, pour chaque valeur donnée de u . Cela vient de la propriété des $S'(u)$ contenue dans le lemme trivial suivant :

LEMME. - Il y a une matrice π unimodulaire, à coefficients entiers, telle que, quel que soit $u > 1$, il y ait un $u' > 1$ pour lequel ${}^t\pi . S'(u)^{-1} . \pi$ (ensemble des matrices ${}^t\pi . A^{-1} . \pi$, pour $A \in S'(u)$) , soit contenu dans $S'(u')$.

[On prendra pour π la matrice de la permutation

$$(1 , 2 , \dots , n) \longrightarrow (n , n-1 , \dots , 1) ,$$

ou autrement dit la matrice $(\delta_{i,n+1-j})$; le lemme résulte alors de ceque, dans le groupe triangulaire, $T \longrightarrow T^{-1}$ transforme tout compact en un compact (propriété qui ne caractérise nullement le groupe triangulaire)] .

Cela posé, $V(B) \cap S'(u)$ est l'ensemble des $A \in S'(u)$ tels que $(A^{-1}B)^2 = 1$, i.e. :

$$A = BA^{-1}B = {}^t(\pi^{-1}B).({}^t\pi . A^{-1} . \pi).(\pi^{-1}B).$$

Donc la matrice entière $\pi^{-1}B$, de déterminant b , transforme un point de $S'(u')$ en un point de $S'(u)$; si u et par suite u' sont fixés, il n'y a, d'après le théorème de Siegel, qu'un nombre fini de matrices susceptibles de faire une pareille chose. C.Q.F.D. [N.B. On n'a pas supposé B indéfinie, donc le cas des formes positives est inclus ; ce cas est d'ailleurs facile à liquider directement] .

Ce qui précède sert principalement à démontrer que, dans le groupe orthogonal G d'une forme quadratique indéfinie F , non dégénérée, à coefficients entiers, le "groupe des unités [arithmétiques] " de F , intersection de G avec le groupe des matrices de déterminant ± 1 sur $\underset{\sim}{Z}$, est minkowskien. Pour cela, soit B la matrice de F ; d'après ce qui précède, les matrices B_i équivalentes à B (i.e., transformées de B par des matrices sur $\underset{\sim}{Z}$ de déterminant ± 1)), telles que $V(B_i)$ rencontre $S(t)$, sont en nombre fini (pour un choix, fixé une fois pour toutes, de $t > 1$). Pour chacune, soit M_i une matrice sur $\underset{\sim}{Z}$, de déterminant ± 1, transformant B dans B_i, i.e. telle que $B_i = {}^tM_i.B.M_i$. Alors $A \longrightarrow {}^tM_i^{-1}.A.M_i^{-1}$ est une bijection de $V(B_i)$ sur $V(B)$; soit U_i l'ouvert de $V(B)$, image par cette bijection de $S(t) \cap V(B_i)$; soit U la réunion des U_i. On montre que U (plus exactement, l'image réciproque dans G de l'ouvert de G/K, image de U par la bijection définie précédemment entre G/K et $V(B)$) a les propriétés énoncées dans (M). Quant à la première, tout revient évidemment à démontrer que, quelle que soit la forme indéfinie F, l'ouvert $S(t) \cap V(F)$ est de mesure finie au sens de l'unique mesure invariante (par rapport au groupe G) définie dans $V(F)$; cela se fait par des majorations explicites. Pour montrer que U contient un système complet de représentants par rapport au sous-groupe (c'est la deuxième propriété à vérifier), soit $A \in V(B)$; on peut transformer A en un point ${}^tM.A.M$ de $S(t)$ au moyen d'un M de déterminant ± 1 sur $\underset{\sim}{Z}$; celui-ci est alors dans $V(B')$ avec $B' = {}^tM.B.M$, ce qui implique, par définition des B_i, que B' est l'un des B_i, donc que M_iM^{-1} est une "unité" de B, et aussi que le transformé ${}^t(M.M_i^{-1}).A.(M.M_i^{-1})$ par $M.M_i^{-1}$ est dans U_i, donc dans U ; autrement dit, A est dans le transformé de U par $M_i.M^{-1}$. Quant au dernier point à vérifier, il résulte du théorème de Siegel par l'A.Q.T.

Comme dans la réduction des formes positives, on peut se proposer de calculer (et non pas seulement de majorer) le volume de G/Γ, l'unité de volume étant explicitement choisie. Là, on ne s'en tire pas à si bon marché. Le lecteur est prié de se reporter à Siegel.

En revanche, on peut, dans ce qui précède, remplacer $S(t)$ par la pyramide de Minkowski ; on obtient alors un "pavage" de G/K par un "domaine fondamental" et ses transformés par le groupe des unités de B, ce pavage offrant aux amateurs de jouissances esthétiques à peu près les mêmes agréments que celui de Minkowski dans le cône P des formes positives. A noter toutefois qu'à cause des B_i en nombre fini, le domaine fondamental se compose, non pas d'un, mais de plusieurs morceaux, dont chacun est une espèce de polyèdre convexe ; en attribuant à chacun de ces morceaux une couleur différente, on obtient, pour l'ensemble du pavage, des résultats fort pittoresques (cf. H. WEYL). Autant qu'"on" peut savoir, cela ne sert strictement à rien.

Enfin, ce qui précède permet de décider dans quel cas G/Γ est compact ; il faut et il suffit pour cela, visiblement, que $S(t) \cap V(B')$, ou, ce qui revient au même, $S'(u) \cap V(B')$ soit d'adhérence compacte dans le cône P pour toute B' équivalente à B. Or c'est l'ensemble des $A \in S'(u)$ tels que $B'^{-1}AB'^{-1}A = 1_n$; pour qu'il soit compact, il faut et il suffit que l'adhérence du cône de sommet 0 qu'il engendre n'ait aucun point commun, autre que 0, avec la frontière du cône P (i.e., ne contienne aucune forme dégénérée $\neq 0$). Mais ce cône est l'ensemble des $A \in S'(u)$ tels que $B'^{-1}AB'^{-1}A = \lambda . 1_n$, avec $\lambda \geqslant 0$; si A appartient à l'adhérence de ce cône et est dégénérée, on aura $B'^{-1}AB'^{-1}A = 0$. Ecrivant que A est dans l'adhérence de $S'(u)$ et est $\neq 0$, on trouve que A est de la forme $\begin{pmatrix} 0 & 0 \\ 0 & C \end{pmatrix}$, avec C non dégénérée ; de $B'^{-1}AB'^{-1}A = 0$, on conclut alors que B'^{-1} est de la forme $\begin{pmatrix} * & * \\ * & 0 \end{pmatrix}$, donc a au moins un coefficient diagonal 0. Par suite, B'^{-1}, donc aussi $B' = {}^tB'.B'^{-1}.B'$, donc aussi B, "représentent" 0 (ce qui veut dire que, si F est la forme de matrice B, $F(x) = 0$ a une solution rationnelle $\neq 0$). La réciproque s'ensuit de même. Autrement dit, pour que G/Γ soit compact, il faut et il suffit que B ne représente pas 0 (ce qui peut arriver pour $n = 3$ et pour $n = 4$; en revanche, un théorème classique de Meyer affirme que toute forme indéfinie à $n \geqslant 5$ variables, à coefficients entiers, "représente" 0).

3. Formes alternées ; groupe de Siegel. C'est le couplet suivant de la chanson ; il se chante sur le même air.

Soit F bilinéaire alternée non dégénérée sur E ; cela exige, bien entendu, que E soit de dimension paire $2n$. Soit f l'application de E sur E' définie par F. Soit G le groupe des automorphismes de F ; soit K un sous-groupe compact de G ; il laisse invariante une Φ positive non dégénérée, à laquelle appartient une application φ de E sur E'. L'adjoint, par rapport à Φ, de l'automorphisme $\iota = \varphi^{-1}f$ de E, est $-\iota$; il s'ensuit que ι est "semi-simple" (du point de vue matriciel, cela veut dire que ι peut être réduit à la forme diagonale, sinon sur $\mathbb{R}$, en tout cas sur $\mathbb{C}$), à valeurs propres toutes purement imaginaires. Si ι a au moins deux valeurs propres distinctes et non imaginaires conjuguées l'une de l'autre, E se décompose en somme directe de sous-espaces dont chacun est invariant par tout automorphisme de E qui commute avec ι ; on en conclut, à peu près comme au n°2, qu'alors K ne peut être maximal. Pour que K soit maximal, il faut et il suffit que ι n'ait que deux valeurs propres distinctes, imaginaires conjuguées l'une de l'autre ; en multipliant Φ par un facteur scalaire > 0, on peut supposer que ces valeurs propres sont $\pm i$, ce qui revient à dire que $\iota^2 = -1$. En ce cas, ι détermine une structure complexe sur E (on définira dans E la multiplication scalaire par les complexes au moyen de $(\alpha + i\beta)x = \alpha x + \beta\iota x)$; pour celle-ci, il est immédiat que la forme bilinéaire à valeurs complexes $H = \Phi + iF$ est hermitienne positive non dégénérée (N.B. Ici, et dans ce qui suit, on note indifféremment par Φ, par abus de langage, soit la forme quadratique introduite ci-dessus, soit la forme bilinéaire associée). Comme les éléments de K commutent avec ι, ce sont des automorphismes de E muni de sa structure complexe ; il est clair alors que K est le groupe unitaire déterminé par la forme hermitienne H. Il contient donc toujours un centre non discret, formé des multiples $e^{it}.1$ de l'automorphisme identique (cela, au sens de la structure complexe). Dans le cas des formes quadratiques indéfinies de signature (p,q), le centre du sous-groupe compact maximal est non discret si $p = 2$ ou $q = 2$, et dans ce cas seulement. On démontre que l'existence d'un tel centre est nécessaire et suffisante pour qu'il y ait sur G/K une structure complexe invariante par G ; on va le vérifier dans le cas présent.

[N.B. La suffisance de la condition se justifie en général comme suit : K opère dans G/K, avec un point fixe qui est le point de G/K qui correspond à K lui-même ; il opère donc sur l'espace des vecteurs tangents à G/K en ce point ; dans cet espace, chacun des deux éléments d'ordre 4 du centre de K définit un automorphisme de carré -1, et permet donc de définir une structure complexe, invariante par K. On peut en faire autant en chaque point ; on a ainsi une structure presque complexe ; reste à montrer qu'elle est intégrable. On peut le voir par exemple (d'après EHRESMANN) en remarquant qu'en général, pour une structure presque complexe, le "défaut d'intégrabilité" s'exprime par un "tenseur mixte", celui qui donne les coefficients des $\overline{\omega}_\beta \overline{\omega}_\gamma$ dans l'expression des différentielles $d\omega_\alpha$ des formes ω_α de type (1,0) ; en exprimant que ce tenseur est invariant par le centre de K, on trouve qu'il s'annule].

En définitive, on voit que G/K a été mis en correspondance biunivoque avec l'ensemble des structures complexes sur E pour lesquelles F est la partie imaginaire d'une forme hermitienne positive non dégénérée $H = \Phi + iF$, et aussi avec l'ensemble $V(F)$ des parties réelles Φ de telles formes ; comme au n°2, $V(F)$ est une sous-variété du cône P des formes positives non dégénérées sur E, et $G/K \to V(F)$ est une bijection analytique réelle de G/K sur $V(F)$.

Si on est dans $\underset{\sim}{R}^{2n}$, et qu'on suppose F donnée par une matrice à coefficients entiers, on démontre, exactement comme au n°2, que le groupe des "unités arithméques" de F est minkowskien dans le groupe des automorphismes de F. Dans un exposé ultérieur, on définira, d'une manière plus ou moins explicite, un ouvert U de G/K satisfaisant à la condition (M) ; ce sera fait, du moins, pour le "groupe de Siegel" (ou "groupe modulaire d'ordre n ") proprement dit, qui est celui des unités si F est donnée dans $\mathbb{R}^{2n}$ par une matrice alternée de déterminant 1. Si "on" a du vice, "on" définira même, dans ce dernier cas, un "domaine fondamental" qui, avec ses transformés, fournit un beau pavage de l'espace G/K .

[N.B. Il est connu que, par un choix convenable de $2n$ générateurs pour le sous-groupe $\mathbb{Z}^{2n}$ des vecteurs à coordonnées entières dans $\mathbb{R}^{2n}$, toute forme alternée à coefficients entiers peut s'écrire $\sum_i d_i(x_i y_{n+i} - x_{n+i}\, y_i)$, où les d_i sont des entiers, les "diviseurs élémentaires", dont chacun est multiple du précédent. Il n'y a donc pas besoin de la théorie de la réduction, dans ce cas, pour montrer qu'il n'y a, pour un déterminant donné, qu'un nombre fini de formes non équivalentes deux à deux. De plus, toutes ces formes sont équivalentes sur $\mathbb{Q}$. Or il est facile de voir que les groupes d'unités arithmétiques de deux formes équivalentes sur $\mathbb{Q}$ sont toujours commensurables ; cela est vrai aussi, bien entendu, pour les formes quadratiques ; mais ici on peut en conclure que les groupes de toutes les formes alternées à coefficients entiers sont commensurables au groupe de Siegel] .

On va s'occuper maintenant de structure complexe. Pour cela, on introduit le "complexifié" de E , qu'on notera E_c (pour raison typographique, au lieu de la notation canonique $E_{\mathbb{C}}$; c'est, comme on sait, $E \otimes \mathbb{C}$ muni de sa structure vectorielle sir $\mathbb{C}$; on considère E comme plongé dedans de la manière évidente). Tout automorphisme ι de E , de carré -1 , se prolonge à E_c en un automorphisme analogue, qui détermine une décomposition de E_c en somme directe des sous-espaces V_i , V_{-i} formés des vecteurs propres relatifs aux valeurs propres i resp. $-i$ de ι ; V_i , V_{-i} sont sous-espaces de E_c sur $\mathbb{C}$, donc sont espaces vectoriels sur $\mathbb{C}$, de dimension n ; on d'ailleurs $V_{-i} = \overline{V}_i$, où, suivant l'usage, la barre dénote l'imaginaire conjugué (défini dans E_c de la manière évidente). Si iE désigne l'ensemble des vecteurs "imaginaires purs" de E_c (image de E par $x \rightarrow ix$), $E_c = E \oplus iE$ est une somme directe ; si $\mathcal{R}$ ("partie réelle") est le projecteur de E_c sur E qu'elle détermine, il est immédiat que $\mathcal{R}$ induit sur V_i un isomorphisme de la structure complexe de V_i sur la structure complexe de E qui est déterminée par ι , c'est-à-dire sur celle de E_ι . Donc ι est complètement déterminé par la donnée de V_i . Réciproquement, soit V_i un sous-espace de E_c de dimension n sur $\mathbb{C}$; pour que $\mathcal{R}$ induise sur V_i une bijection de V_i sur E, il faut et il suffit qu'on ait l'une des relations équivalentes $V_i \cap iE = \{0\}$, $V_i \cap E = \{0\}$, $V_i \cap \overline{V}_i = \{0\}$; lorsqu'il en est ainsi, V_i permet donc de définir sur E, par transport de structure au moyen de $\mathcal{R}$, une structure complexe, donc un automorphisme ι de E de carré -1 ; si alors on étend ι à E_c, V_i sera l'espace des vecteurs propres de ι relatifs à la valeur propre i.

Soit $\mathcal{G}$ la grassmannienne complexe des sous-espaces de E_c de dimension n sur $\mathbb{C}$; dans $\mathcal{G}$, soit $\mathcal{J}$ l'ensemble des sous-espaces dont l'intersection avec E se réduit à $\{0\}$; c'est un ouvert dans $\mathcal{G}$; d'après ce qui précède, il s'identifie avec l'ensemble des structures complexes sur E.

Si on s'est donné comme précédemment, sur $E \times E$, une forme bilinéaire alternée non dégénérée F, celle-ci peut s'étendre à une forme F_c sur $E_c \times E_c$; de même pour l'extension Φ_c d'une forme symétrique Φ. Si on a, sur $E \times E$, $\Phi(x,y)=F(-\iota x,y)$ (ce qui équivaut à la relation $\iota = \varphi^{-1} f$ écrite au début de ce numéro, la relation analogue sera vraie pour les extensions de F, Φ, ι, à E_c ; en particulier, sur V_i, F_c et Φ_c induiront une forme alternée F' et une forme symétrique Φ' telles que l'on ait $\Phi' = -iF'$, ce qui exige évidemment $F' = 0$. Autrement dit, V_i est alors un <u>espace isotrope maximal</u> de F_c ("isotrope" signifie justement que F_c induit 0 sur V_i ; on trouve alors, par exemple par le choix d'une base convenable, que V_i, étant de dimension n, est isotrope <u>maximal</u> parce que F_c est non dégénérée). Ces espaces forment une sous-variété (analytique complexe) $\mathcal{V}$ de la grassmannienne $\mathcal{G}$; on vérifie sans difficulté que le groupe des automorphismes de E_c qui laissent F_c invariante (le "complexifié" du groupe G) opère transitivement sur $\mathcal{V}$. Réciproquement, soit $V_i \in \mathcal{J} \cap \mathcal{V}$; puisqu'on a $E_c = V_i \oplus V_{-i}$, on peut, quel que soit $z \in E_c$, écrire $z = u + v$, $u \in V_i$, $v \in V_{-i}$, et on a alors $\iota z = iu - iv$; si de même on a $z' = u' + v'$, avec $u' \in V_i$, $v' \in V_{-i}$, on aura $F_c(u,u') = 0$ et $F_c(v,v') = 0$ parce que V_i et par suite $V_{-i} = \overline{V}_i$ sont isotropes pour F_c ; cela permet de calculer $F_c(-\iota z,z')$ et de voir que cette forme bilinéaire est symétrique. Il faut exprimer de plus que Φ est positive non dégénérée sur E, ce qui équivaut à $F(-\iota x,x) > 0$ quel que soit $x \neq 0$ dans E. Or, l'isomorphisme de E_ι sur V_i, inverse de l'isomorphisme de V_i sur E_ι induit sur V_i par $\mathcal{R}$, s'écrit $x \to z = x - i.\iota x$ (vérification immédiate) ; en tenant compte de ce que V_i, $V_{-i} = \overline{V}_i$ sont isotropes pour F_c, l'inégalité précédente s'écrit encore $iF_c(z,\overline{z}) < 0$ quel que soit $z \neq 0$ dans V_i. Il est clair que les V_i satisfaisant à cette condition forment un ouvert dans $\mathcal{V}$; ce qui précède implique que cet ouvert n'est pas vide (puisque tout point du riemannien symétrique G/K détermine justement un point de Ω). Il est clair aussi que $V_i \in \Omega$ implique $V_i \in \mathfrak{J}$; sinon, en effet, il y aurait un $z \neq 0$ dans $V_i \cap E$, et on aurait $z = \overline{z}$, $iF(z,z) < 0$, ce qui est idiot. De ce qui précède résulte donc que G/K s'identifie à Ω, qui est une variété (analytique complexe) plongée dans $\mathfrak{J}$. D'où la structure complexe de G/K. Le groupe G des automorphismes de F (i.e. des automorphismes de E qui laissent F invariante) opère sur $\mathfrak{V}$ et sur Ω d'une manière évidente, y laisse invariante la structure analytique complexe, et sa manière d'opérer sur Ω est celle qui résulte, par transport de structure, de son opération sur G/K. Satisfaction générale.

Profitant de l'absence de DIEUDONNÉ, on va traduire ça en matrices, pour faire le joint avec SIEGEL et pour se mettre en état de calculer quand on ne peut pas faire autrement (ça arrive encore quelquefois). On prend une base $(e_1, \ldots, e_{2n})$ de E sur $\mathbb{R}$ pour laquelle la matrice de F soit $\begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix}$; soient E', E'' les sous-espaces engendrés sur $\mathbb{R}$, respectivement, par $(e_1, \ldots, e_n)$ et $(e_{n+1}, \ldots, e_{2n})$; ce sont des sous-espaces de E isotropes maximaux pour F. Si $V_i \in \Omega$, et que ι, Φ, etc., aient le même sens que ci-dessus, Φ sera positive non dégénérée sur E, donc sur E', et on pourra choisir dans E' n vecteurs orthonormaux pour Φ ; ils le seront alors aussi, dans E_ι, pour la forme hermitienne $H = \Phi + iF$ (puisque E' est isotrope pour F) ; ils formeront donc une base de E_ι sur $\mathbb{C}$, ce qui entraîne que E' et $\iota E'$ sont supplémentaires dans E. Alors V_i est transversal au "complexifié" E'_c de E' ; en effet, E'_c est l'ensemble des $x' + iy'$, avec $x' \in E'$, $y' \in E'$; si un tel point est dans V_i, on a $y' = -\iota x' \in E' \cap \iota E'$, donc $x' = y' = 0$. De même V_i est transversal à E''_c.

Choisissons dans V_i n vecteurs formant une base de V_i (sur $\mathbb{C}$) ; écrivons-les comme "colonnes" (matrices à $2n$ lignes et 1 colonne) au moyen de $(e_1, \ldots, e_{2n})$ pris comme base de E_c sur $\mathbb{C}$; cela donne une matrice à $2n$ lignes et n colonnes (sur $\mathbb{C}$), qu'on peut écrire $\begin{pmatrix} U \\ V \end{pmatrix}$, où U, V sont deux matrices à n lignes et n colonnes ; si on change les vecteurs de base choisis dans V_i, cela revient à multiplier U, V <u>à droite</u> par une même matrice carrée inversible. Puisque V_i est transversal à E''_c, la matrice U est de rang n, c'est-à-dire inversible.

Ecrivons que V_i est isotrope pour F ; cela s'exprime par la formule

$$({}^tU \quad {}^tV) \cdot \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix} \cdot \begin{pmatrix} U \\ V \end{pmatrix} = 0 ,$$

ou autrement dit ${}^tU.V = {}^tV.U$. De même, écrivons que $iF_c(z,\bar{z}) < 0$ pour tout $z \neq 0$ dans V_i ; cela signifie $(1/i)({}^t\bar{U}.V - {}^t\bar{V}.U) \gg 0$ (le premier membre est visiblement une matrice hermitienne).

Posons $Z = VU^{-1}$, matrice qui est indépendante de la base choisie dans V_i. La première des relations ci-dessus s'écrit ${}^tZ = Z$; Z est symétrique. La seconde s'écrit (en multipliant à droite par U^{-1}, à gauche par ${}^t\bar{U}^{-1}$, ce qui ne modifie pas le fait que le premier membre est hermitien positif non dégénérée) $(1/i)(Z - {}^t\bar{Z}) \gg 0$; autrement dit, si on écrit $Z = X + iY$ avec X, Y symétriques réels, Y doit être positive non dégénérée.

On a ainsi obtenu une bijection de Ω, donc en définitive de G/K, sur l'espace de Siegel $\mathfrak{S}$, formé des matrices symétriques $Z = X + iY$ sur $\underset{\sim}{C}$ telles que $Y \gg 0$; $\mathfrak{S}$ peut être considéré comme un ouvert de $\underset{\sim}{C}^N$, avec $N = n(n+1)/2$, muni de la structure complexe induite par celle de $\underset{\sim}{C}^N$.

L'opération de G sur $\mathfrak{S}$ s'écrit immédiatement. En effet, avec les notations ci-dessus, un élément de G s'écrira sous forme d'une matrice carrée $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$, où A, B, C, D sont des matrices à n lignes et n colonnes sur $\underset{\sim}{R}$; cette matrice doit satisfaire à la condition

$$\begin{pmatrix} {}^tA & {}^tC \\ {}^tB & {}^tD \end{pmatrix} \cdot \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix} \cdot \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix}$$

qui exprime qu'elle laisse F invariante. Cette matrice opère sur V_i, définie par les matrices U, V, au moyen de la formule

$$\begin{pmatrix} U \\ V \end{pmatrix} \to \begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot \begin{pmatrix} U \\ V \end{pmatrix}$$

ou autrement dit :

$$(U,V) \to (AU + BV \ , \ CU + DV) \quad ;$$

elle opère donc sur Z par la formule

$$Z \to (C + DZ).(A + BZ)^{-1} .$$

Enfin, on peut donner de l'opération sur $\mathfrak{S}$ du groupe modulaire (sous-groupe de G formé des matrices à coefficients entiers) une interprétation intéressante, et même importante. En effet, F étant donnée dans E, les points de $\mathfrak{S}$ sont, d'après ce qu'on a vu, en correspondance biunivoque avec les structures complexes E_U qu'on peut mettre sur E, pour lesquelles F est partie imaginaire d'une forme hermitienne $H \gg 0$. Supposons donné en même temps dans E un lattice Λ tel que F soit à valeurs entières sur $\Lambda \times \Lambda$; E/Λ est alors un tore de dimension (réelle) $2n$, sur lequel F détermine une classe de cohomologie entière de dimension (réelle) 2. Toute structure complexe sur E détermine sur E/Λ une structure de tore complexe (de dimension complexe n) ; pour que celui-ci soit une variété abélienne, il faut et il suffit qu'il existe dans E une forme hermitienne $\gg 0$ dont la partie imaginaire soit à valeurs entières sur $\Lambda \times \Lambda$; et, lorsqu'il en est ainsi, il y a sur E/Λ un "diviseur positif" appartenant à la classe de cohomologie déterminée par cette partie imaginaire ; muni de cette classe, E/Λ s'appelle alors une variété abélienne polarisée. On voit donc qu'à tout point de $\mathfrak{S}$ correspond sur E/Λ une structure de variété abélienne polarisée par F ; pour qu'à deux points corresponde la même structure, il faut et il suffit qu'ils se déduisent l'un de l'autre par un automorphisme de E qui laisse invariants la forme F et le lattice Λ, donc un élément du groupe discret Γ des automorphismes de F qui sont à coefficients entiers lorsqu'on prend pour base un système de générateurs de Λ. Autrement dit, les points de $\mathfrak{S}/\Gamma$ (quotient de $\mathfrak{S}$ par la relation d'équivalence définie dans $\mathfrak{S}$ par le groupe discret Γ) sont en correspondance biunivoque avec les structures de variété abélienne polarisée par F qu'on peut définir sur E/Λ. Lorsque F est de déterminant 1 sur Λ (c'est-à-dire à tous ses diviseurs élémentaires sur Λ égaux à 1), le groupe Γ qu'on obtient est le groupe modulaire de Siegel proprement dit ; les variétés abéliennes correspondantes sont dites "variétés abéliennes polarisées de la famille principale" (toute jacobienne est une telle variété).

BIBLIOGRAPHIE

MINKOWSKI (Hermann). - Geometrie der Zahlen. - Leipzig und Berlin, B.G. Teubner, 1910 ; New York, Chelsea, 1953.

MINKOWSKI (Hermann). - Diskontinuitätsbereich für arithmetische Äquivalenz, J. für reine und angew. Math., t. 129, 1905, p. 220-274 ; Gesammelte Abhandlungen, Band 2, Berlin, B.G. Teubner, 1911, p. 53-100.

SIEGEL (Carl Ludwig). - Einführung in die Theorie der Modulfunktionen n-ten Grades, Math. Annalen, t. 116, 1939, p. 617-657.

SIEGEL (Carl Ludwig). - Einheiten quadratischer Formen, Abh. math. Sem. Hamburg Univ., t. 13, 1940, p. 209-239.

SIEGEL (Carl Ludwig). - Discontinuous groups, Annals of Math., t. 44, 1943, p. 674-689.

SIEGEL (Carl Ludwig). - Symplectic geometry, Amer. J. Math., t. 65, 1943, p. 1-86.

WEYL (Hermann). - Theory of reduction for arithmetical equivalence, I., Trans. Amer. math. Soc., t. 48, 1940, p. 126-164 ; II., Trans. Amer. math. Soc., t. 51, 1942, p. 203-231.

WEYL (Hermann). - Fundamental domains for lattice groups in division algebras, Comment. Math. Helvet., t. 17, 1944/45, p. 283-306 ; et Selecta Hermann Weyl, Basel und Stuttgart, Birkhäuser, 1956, p. 521-553.