ARMAND BOREL

INTRODUCTION
AUX
GROUPES ARITHMÉTIQUES

HERMANN
115, Boulevard Saint-Germain, Paris VI

INTRODUCTION AUX GROUPES ARITHMÉTIQUES

Actualités scientifiques et industrielles 1341

TABLE

INTRODUCTION

Ce livre est basé sur la première partie d'un cours de troisième cycle donné à l'Institut Henri-Poincaré en 1964. Il est axé sur la théorie dite de la « réduction » dans un groupe algébrique réel $G_{\mathbf{R}}$, par rapport à un groupe arithmétique Γ. La démonstration des théorèmes généraux utilise pleinement la théorie des groupes algébriques linéaires. Cependant, comme l'auditeur du cours n'était pas nécessairement supposé familier avec cette dernière, on a tout d'abord discuté directement quelques cas classiques, qui sont du reste en partie à l'origine de la théorie générale, et on a résumé, principalement dans trois paragraphes (§§ 7, 10, 11), au fur et à mesure des besoins, les notions et résultats sur les groupes algébriques linéaires utilisés dans la suite. Ces paragraphes contiennent aussi quelques exemples et démonstrations et fournissent donc, dans une certaine mesure, une introduction à quelques aspects de cette théorie.

Par réduction dans $G_{\mathbf{R}}$, par rapport à Γ, on entend ici, en gros, la recherche de sous-espaces, ouverts ou fermés, qui rencontrent chaque orbite de Γ (opérant par translations à droite), en au moins un, mais pas plus d'un nombre fini, de points, et que nous appellerons ensembles fondamentaux (en fait, on imposera des conditions plus précises, (cf. 5.6, 9.6, 15.13)). Il revient au même de résoudre ce problème dans l'espace $X = K\backslash G_{\mathbf{R}}$ des classes à droite de $G_{\mathbf{R}}$ modulo un sous-groupe compact maximal K. Lorsque G est un groupe classique, on retrouve alors en particulier les problèmes de réduction de formes quadratiques ou hermitiennes.

Ce livre se divise assez naturellement en trois parties. La première (§§ 1 à 6) est consacrée essentiellement à la réduction des formes quadratiques, traitée par des méthodes qui trouvent une généralisation naturelle dans les paragraphes ultérieurs. On considère tout d'abord le cas où $G = \mathbf{GL}(n, \mathbf{R})$, $\Gamma = \mathbf{GL}(n, \mathbf{Z})$, $K = \mathbf{O}(n)$, donc où X est l'espace des formes quadratiques positives non dégénérées sur $\mathbf{R}^n$. On montre que toute orbite de Γ dans G rencontre un ensemble de Siegel (1.4) convenable et on en déduit quelques conséquences, en particulier le critère de Mahler pour la compacité relative d'une partie de l'espace $\mathbf{GL}(n, \mathbf{R})/\mathbf{GL}(n, \mathbf{Z})$ des réseaux de $\mathbf{R}^n$, et la finitude du volume de $\mathbf{SL}(n, \mathbf{R})/\mathbf{SL}(n, \mathbf{Z})$. Le § 2 traduit ces résultats en termes de formes quadratiques, et établit quelques liens avec la réduction de Minkowski. Le § 4 montre qu'un ensemble de Siegel ne rencontre qu'un nombre fini de ses translatés par $x.\Gamma$, pour tout $x \in \mathbf{GL}(n, \mathbf{Q})$, (4.6). Le § 5 est consacré à la réduction des formes quadratiques indéfinies suivant la méthode de Hermite. Le point central en est une propriété de finitude de « réduites entières », qui sera ici déduite d'un lemme plus général démontré au § 6.

La deuxième partie (§§ 7, 8, 9) est consacrée à deux théorèmes généraux sur les groupes arithmétiques, dont la démonstration ne fait encore appel qu'à un ensemble

assez restreint de résultats sur les groupes algébriques, qui sont rappelés ou démontrés au § 7. Ce sont le critère de compacité du quotient $G_{\mathbf{R}}/\Gamma$ (§ 8), et une première construction d'ensembles fondamentaux qui généralise celle de Hermite. En outre, le § 8 montre que l'image d'un groupe arithmétique par une isogénie est aussi un groupe arithmétique, et le § 9 établit un théorème de finitude pour les orbites de Γ dans l'ensemble des points entiers d'une orbite fermée de G, dans l'espace d'une représentation linéaire de G. Cela généralise la finitude des classes de formes quadratiques de déterminant non nul donné (6.4), et des résultats de Jordan sur les classes de formes homogènes de degré $\geqq 3$, (6.5).

La troisième partie (§§ 10 à 17) est consacrée à des ensembles fondamentaux en général plus maniables que ceux du § 9. Leur existence est démontrée de deux manières très différentes, au § 13, où l'on s'appuie sur le § 9, et au § 16, où l'on utilise un principe d'extremum appliqué à un type de fonctions étudiées au § 14, et qui généralisent entre autres le $|cz + d|$ du demi-plan de Poincaré. Ces ensembles sont réunions d'un nombre fini de translatés par des éléments de $G_{\mathbf{Q}}$ d'un ensemble de forme simple, dit de Siegel. Enfin le § 17 décrit, dans un cas particulier, $X\backslash G_{\mathbf{R}}/\Gamma$ comme l'intérieur d'une variété à bord compacte.

Le souci de rendre la première partie autonome, et de ne faire appel à la théorie des groupes algébriques que quand cela s'avère nécessaire, a conduit à quelques redites ou inconséquences. Ainsi le § 4 est un cas particulier du § 15, non utilisé dans ce dernier, et l'existence d'une décomposition de Bruhat est démontrée dans le § 3 pour $\mathbf{GL}(n, k)$, alors qu'elle est admise sans démonstration dans un cas beaucoup plus général à partir du § 12. En conséquence, cet exposé, qui suit, *grosso modo*, l'ordre chronologique, et contient des « rappels » assez étendus, n'est pas le plus économique possible, et la lecture d'un paragraphe ne présuppose pas nécessairement celle de tous les précédents. Faisons encore, en guise de « Leitfaden », quelques remarques sur l'interdépendance des différents paragraphes : le § 1, jusqu'à 1.11, est fondamental pour tout le livre, mais la fin de ce paragraphe, et les §§ 2 à 5, ne sont pas utilisés dans la suite, si ce n'est à titre d'exemples; le lecteur désireux de parvenir aussi rapidement que possible aux théorèmes généraux peut concentrer son attention sur les §§ 1, 8, 12, 14, 15, 16, s'il veut bien admettre une propriété de finitude, démontrée ici en s'appuyant sur le § 13, mais qui peut se voir plus directement en utilisant l'analogue adélique des §§ 1 et 8 (cf. introduction au § 16); enfin, le § 6 intervient essentiellement au § 5 et dans le § 9, lui-même utilisé au § 13, mais pas ailleurs.

Une première rédaction de ce cours, polycopiée et distribuée par l'Institut Henri-Poincaré, due à H. Jacquet, J.-J. Sansuc et J.-P. Jouanolou, m'a été très utile, et j'en remercie vivement les auteurs. Je tiens aussi à remercier J. E. Humphreys, qui a lu le manuscrit, signalé un nombre considérable de fautes « d'impression » et suggéré quelques améliorations d'exposition, ainsi que A. Robert et J. Joel, pour m'avoir aidé à corriger les épreuves.

A. BOREL

Princeton, novembre 1968

NOTATIONS

0.1. $\mathbf{Z}$ est l'anneau des entiers, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ désignent le corps des nombres rationnels, réels, et complexes resp. et $\mathbf{N}$ est l'ensemble des entiers $\geqq 0$. Si A est un anneau à élément unité, A^* désigne le groupe multiplicatif des éléments inversibles de A. Si A est un anneau commutatif, $\mathbf{M}(n, A)$ est l'anneau des matrices carrées d'ordre n, à coefficients dans A, $\mathbf{GL}(n, A)$ ou $\mathbf{GL}_n(A)$ est le groupe des matrices carrées d'ordre n à coefficients dans A, dont le déterminant est une unité de A, et $\mathbf{SL}_n(A)$ ou $\mathbf{SL}(n, A)$ est le sous-groupe des éléments de $\mathbf{GL}_n(A)$ de déterminant un.
$\mathbf{O}(n)$ est le sous-groupe de $\mathbf{GL}(n, \mathbf{R})$ laissant invariante la forme quadratique $\sum x_i^2$ et $\mathbf{SO}(n) = \mathbf{O}(n) \cap \mathbf{SL}(n, \mathbf{R})$. Si p et q sont des entiers $\geqq 0$ et $n = p + q$, alors $\mathbf{O}(p, q)$ est le sous-groupe de $\mathbf{GL}(n, \mathbf{R})$ laissant invariante la forme quadratique

$$(x_1^2 + \ldots + x_p^2) - (x_{p+1}^2 + \ldots + x_{p+q}^2) \qquad \text{et} \qquad \mathbf{SO}(p, q) = \mathbf{O}(p, q) \cap \mathbf{SL}(n, \mathbf{R}).$$

0.2. Soient G un groupe et α un homomorphisme de G dans $\mathbf{C}^*$. La valeur de α en $g \in G$ sera notée $\alpha(g)$ ou aussi g^α. Cette dernière notation sous-entend que l'on écrit additivement la loi de composition naturelle des homomorphismes de G dans $\mathbf{C}^*$.

0.3. Soit G un groupe. Si $g \in G$, on note Int g l'automorphisme intérieur $x \mapsto g.x.g^{-1}$ de G. Si A et H sont des parties de G, alors ^{A}H désigne la réunion des ensembles $a.H.a^{-1}$ $(a \in A)$.
Soient V_i $(1 \leqq i \leqq n)$ des ensembles et $f_i : V_i \to G$ des applications. L'application $f : V_1 \times \ldots \times V_n \to G$ définie par $(v_1, \ldots, v_n) \mapsto f_1(v_1) \cdot \ldots \cdot f_n(v_n)$ est appelée l'application produit des f_i.

0.4. Soient G un groupe et G_i $(1 \leqq i \leqq n)$ des sous-groupes distingués de G. On dit que G est produit presque direct des G_i si l'application produit des inclusions naturelles des G_i dans G est surjective, de noyau fini.

0.5. Une fonction à valeurs dans un espace topologique sera dite bornée si son ensemble de valeurs est relativement compact.
Soient X un espace topologique, f, g des fonctions à valeurs réelles $\geqq 0$ sur X. On écrit :

$$f \prec g$$

s'il existe une constante $c > 0$ telle que $f(x) \leqq c.g(x)$ pour tout $x \in X$ et $f \succ g$ si $g \prec f$, $f \asymp g$ si l'on a simultanément $f \prec g$ et $g \succ f$. La relation $f \asymp g$ signifie donc qu'il existe des constantes $c, d > 0$ telles que :

$$c.f(x) \leqq g(x) \leqq d.f(x) \qquad (x \in X).$$

Si $f \prec g$ (resp. $f \succ g$, resp. $f \asymp g$), on dira quelquefois que f minore essentiellement g (resp. majore essentiellement g, resp. est comparable à g).

Quelques groupes classiques

1. Ensembles de Siegel et réduction dans $\mathbf{GL}(n, \mathbf{R})$

On désignera par G le groupe $\mathbf{GL}(n, \mathbf{R})$ des matrices carrées inversibles de degré n à coefficients réels et par Γ le sous-groupe $\mathbf{GL}(n, \mathbf{Z})$ de G formé des matrices de déterminant ± 1 à coefficients entiers. G est un groupe de Lie réel dont Γ est un sous-groupe discret.
On se propose de donner en première approximation un système de représentants des classes à droite de Γ dans G. Pour cela, rappelons tout d'abord la décomposition d'Iwasawa de $\mathbf{GL}(n, \mathbf{R})$ [8, Chap. VII, § 3, Prop. 7] :

1.1. PROPOSITION. *Soit* A *le groupe des matrices diagonales à coefficients strictement positifs. Si* K *et* N *désignent respectivement le groupe orthogonal et le groupe « trigonal strict supérieur », formé des matrices triangulaires supérieures de valeurs propres égales à un, l'application :*

$$(k, a, n) \mapsto k.a.n$$

est un homéomorphisme de $\mathrm{K} \times \mathrm{A} \times \mathrm{N}$ *sur* $\mathbf{GL}(n, \mathbf{R})$.

Si $g \in \mathrm{G}$, on notera $g = k_g.a_g.n_g$ sa décomposition d'Iwasawa. Ceci dit, posons la :

1.2. DÉFINITION. On appelle *ensemble de Siegel* de $\mathbf{GL}(n, \mathbf{R})$ tout ensemble de la forme : $\mathfrak{S}_{t,u} = \mathrm{K}.\mathrm{A}_t.\mathrm{N}_u$ (t et u réels positifs)

où $\quad \mathrm{A}_t = \{a \in \mathrm{A} \mid a_{ii} \leqslant t.a_{i+1,i+1} \quad (i = 1, \ldots, n-1)\}$

et $\quad \mathrm{N}_u = \{n \in \mathrm{N} \mid |n_{ij}| \leqslant u \quad (1 \leqq i < j \leqq n)\}$.

On sait que N est un sous-groupe fermé de G, homéomorphe à $\mathbf{R}^m$ ($m = n(n-1)/2$) par l'application $\theta : n \mapsto (n_{ij})_{i<j\leqslant n}$; par conséquent, N_u est compact.
On appellera plus généralement ensemble de Siegel une partie de G de la forme $\mathfrak{S}_{t,\omega} = \mathrm{K}.\mathrm{A}_t.\omega$ où ω est un voisinage compact de e dans N.
Soit $\mathfrak{S}$ un ensemble de Siegel. Il résulte immédiatement de la définition que $g.\mathfrak{S} = \mathfrak{S}$ si $g \in \mathrm{K}$ ou $g = c.\mathrm{I}$ ($c > 0$) et que $\mathfrak{S}.h$ est contenu dans un ensemble de Siegel si $h \in \mathrm{A}.\mathrm{N}$.

Une propriété fondamentale des ensembles A_t est le :

1.3. LEMME. *Si ω est relativement compact dans* N, *alors* $\bigcup_{a \in A_t} a\omega a^{-1}$ *est aussi relativement compact dans* N.

En effet, si $n = (n_{ij}) \in \omega$, on a $(a.n.a^{-1})_{ij} = (a_{ii}/a_{jj}).n_{ij}$, d'où :

$$|(a.n.a^{-1})_{ij}| \leqslant t^{j-i}.|n_{ij}| \qquad \text{si } i < j.$$

Notons en passant (nous en aurons besoin dans la suite) que la mesure de Haar sur N est l'image par θ^{-1} de la mesure de Lebesgue de $\mathbf{R}^m$, de sorte que le module de l'automorphisme :

$$\text{int}\,(a) : n \mapsto a.n.a^{-1} \text{ de N}$$

est

$$|\det_{\mathbf{R}^m}(\text{int}\,a)| = \prod_{i<j} \frac{a_{ii}}{a_{jj}}.$$

Nous avons en vue le :

1.4. THÉORÈME. *On a* $G = \mathfrak{S}_{t,u}\Gamma$ *dès que* $t \geqslant 2/\sqrt{3}$, $u \geqslant 1/2$.

Remarquons tout d'abord que l'on a :

$$N = N_{1/2}.N_{\mathbf{Z}} \qquad (N_{\mathbf{Z}} = N \cap \Gamma). \tag{1}$$

En effet, cela revient à dire que, étant donné $u = (u_{ij}) \in N$, on peut trouver $z = (z_{ij}) \in N_{\mathbf{Z}}$ tel que $|(u.z)_{ij}| \leqq 1/2$ $(i < j)$. Or on a :

$$(u.z)_{ij} = z_{ij} + u_{i,i+1}.z_{i+1,j} + \ldots + u_{ij} \qquad (1 \leqq i < j \leqq n)$$

ce qui permet de construire z_{ij} par une récurrence convenable sur (i, j) en commençant par $z_{n-1,n}$.
Le point essentiel est donc la condition portant sur la composante en A. Pour le traiter, on utilisera un principe de minimum. Soit (e_i) $(1 \leqq i \leqq n)$ la base canonique de $\mathbf{R}^n$ et soit Φ la fonction sur G définie par :

$$\Phi(g) = \|g.e_1\|.$$

C'est une fonction continue réelle > 0, qui vérifie visiblement :

$$\Phi(k.a.n) = \|k.a.n(e_1)\| = \|a(e_1)\| = a_1 = \Phi(a) \tag{2}$$

$(k \in K,\ a \in A,\ n \in N)$, où a_1 est le premier coefficient de A.
Pour tout $g \in G$, la fonction $z \mapsto \Phi(g.z)$ $(z \in \Gamma)$ a un minimum > 0 sur Γ. En effet, on a $g.\Gamma.e_1 \subset g(\mathbf{Z}^n - \{0\})$, donc $g.\Gamma.e_1$ est formé d'éléments non nuls d'un réseau de $\mathbf{R}^n$.

1.5. LEMME. *Soit* $g \in G$ *et soit* $g = k.a.n$ *sa décomposition d'Iwasawa. Supposons que* $\Phi(g) \leqq \Phi(g.\gamma)$ $(\gamma \in \Gamma)$. *Alors* $a_{11} \leqq (2/\sqrt{3}).a_{22}$.

Si $u \in N_{\mathbf{Z}}$, alors $\Phi(g.u) = \Phi(g)$ et $a_{g.u} = a_g$. On peut donc, vu (1),

admettre que $|n_{12}| \leqq 1/2$. Soit $z \in \Gamma$ l'élément qui permute e_1 et e_2 et laisse e_i fixe $(3 \leqq i \leqq n)$. On a alors :

$$g.z(e_1) = g(e_2) = k.a.n(e_2) = k.a.(e_2 + n_{12}.e_1) = k(a_{22}.e_2 + a_{11}.n_{12}.e_1),$$

donc

$$\Phi(g.z)^2 = a_{22}^2 + a_{11}^2.n_{12}^2 \leqq a_{11}^2/4 + a_{22}^2.$$

Comme $\Phi(g) = a_{11}$, l'hypothèse entraîne :

$$a_{11}^2 \leqq a_{11}^2/4 + a_{22}^2,$$

d'où le lemme.

Le théorème 1.4 sera conséquence de l'énoncé plus précis suivant :

1.6. THÉORÈME. *Soit* $g \in G$. *Le minimum de* Φ *sur* $g.\Gamma$ *est atteint en un point de* $g.\Gamma \cap \mathfrak{S}_{2/\sqrt{3},\,1/2}$.

On écrit $\mathfrak{S}_0$ pour $\mathfrak{S}_{2/\sqrt{3},\,1/2}$. La démonstration procède par récurrence sur n. Pour $n = 1$, $G = \mathfrak{S}_0$ et il n'y a rien à démontrer.

Soit $x \in G$. On peut trouver $y \in x.\Gamma$ tel que $\Phi(y) \leqq \Phi(x.\gamma)$ $(\gamma \in \Gamma)$, d'où aussi $\Phi(y) \leqq \Phi(y.\gamma)$ $(\gamma \in \Gamma)$. On peut écrire :

$$k_y^{-1}.y = \begin{pmatrix} a_{11} & * \\ 0 & b \end{pmatrix}, \qquad b \in \mathbf{GL}(n-1, \mathbf{R}).$$

Par hypothèse de récurrence, il existe :

$$z' \in \mathbf{GL}(n-1, \mathbf{Z}) \quad \text{tel que} \quad b.z' \in \mathfrak{S}_0^{(n-1)},$$

où l'on note $\mathfrak{S}_0^{(n-1)}$ le domaine de Siegel $\mathfrak{S}_{2/\sqrt{3},\,1/2}$ de $\mathbf{GL}(n-1, \mathbf{R})$. Soit :

$$b.z' = k'.a'.n'$$

la décomposition d'Iwasawa de $b.z'$. Alors :

$$k_y^{-1}.y.z = \begin{pmatrix} a_{11} & * \\ 0 & k'.a'.n' \end{pmatrix} = k''.a''.n'', \qquad z = \begin{pmatrix} 1 & 0 \\ 0 & z' \end{pmatrix}$$

avec

$$k'' = k_y.\begin{pmatrix} 1 & 0 \\ 0 & k' \end{pmatrix} \in K, \qquad a'' = \begin{pmatrix} a_{11} & 0 \\ 0 & a' \end{pmatrix} \in A, \qquad n'' = \begin{pmatrix} 1 & 0 \\ 0 & n' \end{pmatrix} \in N.$$

Par construction, on a $(a'')_{ii} \leqq (2/\sqrt{3})a''_{i+1,\,i+1}$ $(2 \leqq i < n)$. Mais z laisse e_1 fixe, donc $\Phi(y.z) = \Phi(y)$ et par suite :

$$\Phi(y.z) \leqq \Phi(y.z.\gamma) \qquad (\gamma \in \Gamma).$$

Le lemme 1.5 montre alors que $(a'')_{11} \leqq (2/\sqrt{3}).(a'')_{22}$. Par conséquent :

$$y.z \in K.A_{2/\sqrt{3}}.N$$

et, compte tenu de (1),

$$x \in y.\Gamma \subset K.A_{2/\sqrt{3}}.N.\Gamma = \mathfrak{S}_0.\Gamma.$$

1.7. COROLLAIRE (Hermite). *Soit* $g \in G$. *Alors* :

$$\min_{x \in \mathbf{Z}^n - \{0\}} \|g(x)\| \leqq (2/\sqrt{3})^{(n-1)/2}.|\det g|^{1/n}.$$

On peut trouver un élément $g' \in g.\Gamma \cap \mathfrak{S}_{2/\sqrt{3},1/2}$ vérifiant (1.6). Comme Γ est formé d'éléments de déterminant ± 1, on a $|\det g| = |\det g'|$. D'autre part :

$$\min_{x \in \mathbf{Z}^n - \{0\}} ||g(x)|| \leqq \min_{\gamma \in \Gamma} ||g\gamma(e_1)|| = ||g'(e_1)|| = a'_{11},$$

où a' est la composante en A de g'. De $a' \in A_{2/\sqrt{3}}$, on tire

$$(a'_{11})^n \leqq (2/\sqrt{3})^{n(n-1)/2}.a'_{11}.\ldots.a'_{nn} = (2/\sqrt{3})^{n(n-1)/2}\,|\det g|.$$

1.8. *Remarque.* Soit $||\ ||_1$ une norme sur $\mathbf{R}^n$, i.e. une fonction continue, strictement positive en dehors de l'origine, telle que $||r.x||_1 = |r|.||x||_1$ $(r \in \mathbf{R},\ x \in \mathbf{R}^n)$. Il existe deux constantes $d, d' > 0$ telles que :

$$d||x|| \leqq ||x||_1 \leqq d'||x|| \qquad (x \in \mathbf{R}^n).$$

(C'est clair sur la sphère unité, et est alors vrai sur $\mathbf{R}^n$ par homogénéité.) Le corollaire implique donc l'existence d'une constante $C > 0$ telle que :

$$(1) \qquad \min_{x \in \mathbf{Z}^n - \{0\}} ||g(x)||_1 \leqq C.|\det g|^{1/n} \qquad (g \in G).$$

Nous passons maintenant à une application qui jouera un rôle important dans la suite. Soit $\mathscr{R}$ l'ensemble des réseaux de $\mathbf{R}^n$. Il s'identifie à G/Γ, d'où une topologie sur $\mathscr{R}$.

On notera Δ la fonction sur $\mathscr{R}$ qui associe à tout réseau L le volume euclidien du parallélotope sous-tendu par une base de L. Si $L = g(L_0)$ où $L_0 = \mathbf{Z}^n$, on a donc $\Delta(L) = |\det g|$.

1.9. COROLLAIRE (Critère de Mahler). *Soit* $M \subset \mathscr{R}$. *Alors les deux conditions suivantes sont équivalentes :* (a) M *est relativement compact ;* (b) Δ *est borné sur* M *et il existe un voisinage* U *de l'origine dans* $\mathbf{R}^n$ *tel que* $L \cap U = \{0\}$ *quel que soit* $L \in M$.

Soit $\mathfrak{S}$ un ensemble de Siegel envoyé sur $\mathscr{R}$ par l'application $g \mapsto g(L_0)$ (cf. 1.4). Il est clair que (a) équivaut à l'existence de $M' \subset \mathfrak{S}$, relativement compact, tel que $M'(L_0) = M$. D'autre part, $M' \subset \mathfrak{S}$ est relativement compact si, et seulement si, les composantes $a_x (x \in M')$ forment un ensemble relativement compact dans A, donc, si, et seulement si, il existe deux constantes $\alpha, \beta > 0$ telles que

$$(1) \qquad \alpha \leqq (a_g)_{ii} \leqq \beta \qquad (g \in M';\ i = 1, \ldots, n)$$

Il faut donc voir que (1) équivaut à :

(2) $|\det g|$ est borné sur M'; il existe $c > 0$ telle que $||g(x)|| \geqq c$ quels que soient $x \in \mathbf{Z}^n - \{0\}$, $g \in M'$.

(1) $\Rightarrow$ (2). On a $|\det g| = \prod (a_g)_{ii}$, donc $|\det g|$ est borné. Soit $x \in \mathbf{Z}^n - 0$. On peut écrire $x = \sum_1^k m_i.e_i$ avec m_i entier, $m_k \neq 0$.

Alors $||g(x)|| = ||a_g.n_g(x)||$ et la $k^{\text{ième}}$ coordonnée de $a_g.n_g(x)$ est $(a_g)_{k,k}m_k$, donc $||g(x)|| \geqq \alpha$.

(2) $\Rightarrow$ (1). On a $||g(e_1)|| = (a_g)_{11} \geqq c$. Comme les $a_g (g \in M')$ font partie d'un ensemble A_t, cette inégalité entraîne l'existence d'une constante $\alpha > 0$ telle que $(a_g)_{ii} \geqq \alpha$ pour tout i. Comme le produit des $(a_g)_{ii}$ est borné, cela entraîne (1).

1.10. *Ensembles de Siegel et réduction dans* $\mathbf{SL}(n, \mathbf{R})$. La décomposition d'Iwasawa dans $\mathbf{GL}(n, \mathbf{R})$ induit une décomposition dans $\mathbf{SL}(n, \mathbf{R})$:

$$\mathbf{SL}(n, \mathbf{R}) = \mathbf{SO}(n).A^*.N \qquad (A^* = \mathbf{SL}(n, \mathbf{R}) \cap A).$$

On définit les ensembles de Siegel $\mathfrak{S}^*_{t,u}$ dans $\mathbf{SL}(n, \mathbf{R})$ exactement comme dans $\mathbf{GL}(n, \mathbf{R})$. On a donc $\mathfrak{S}^*_{t,u} = \mathbf{SL}(n, \mathbf{R}) \cap \mathfrak{S}_{t,u}$. Les théorèmes 1.4, 1.6 restent valables. Le seul point nouveau est que *le volume invariant du quotient* $\mathbf{SL}(n, \mathbf{R})/\mathbf{SL}(n, \mathbf{Z})$ *est fini*. Vu 1.4, cela résulte du

1.11. LEMME. *Le volume d'un ensemble de Siegel* $\mathfrak{S}^*_{t,u}$ *de* $\mathbf{SL}(n, \mathbf{R})$, *par rapport à une mesure de Haar, est fini.*

Soient $K^* = \mathbf{SO}(n)$ et $B^* = A^*.N$. Soient dk, da, dn des mesures de Haar sur K^*, A^*, N, nécessairement biinvariantes, car ces groupes sont unimodulaires. Montrons que l'homéomorphisme de la décomposition d'Iwasawa transporte une mesure de Haar dg de G en

$$\rho(a).dk.da.dn \qquad (a \in A^*;\ \rho(a) = \prod_{i<j} a_{ii}/a_{jj}). \tag{1}$$

Faisons opérer $k \in K$ (resp. $b \in B^*$) sur $K \times B^*$ et G par translation à gauche par k (resp. à droite par b^{-1}). Alors l'application produit définit un homéomorphisme de $K \times B^*$ sur G commutant à $K \times B^*$. L'image réciproque de dg est une mesure invariante à gauche par K, à droite par B, donc est égale au produit $dk.d_r b$, où $d_r b$ est une mesure de Haar invariante *à droite* sur B^*. Mais B^* est le produit semi-direct des deux sous-groupes unimodulaires A^*, N donc [8, Chap. VII, § 2, n. 9] $d_r b = m(a).da.dn$, où $m(a)$ est le module de a; mais on a déjà vu (cf. 1.3) que ce dernier est égal à $\rho(a)$.

On a alors, puisque K^* et N_u sont compacts :

$$\int_{\mathfrak{S}_{t,u}} dg = C. \int_{A^*_t} \rho(a)\, da,$$

où C est une constante > 0. Mais on peut écrire :

$$\rho(a) = \prod_1^{n-1} b_i^{r_i} \qquad (b_i = a_{ii}/a_{i+1,i+1};\ 1 \leqq i < n)$$

où les r_i sont des entiers > 0. Les b_i forment un système de coordonnées sur A^*. D'autre part, l'application $(y_i)_{1 \leqq i < n} \mapsto (\exp y_i)_{1 \leqq i < n}$ définit un isomorphisme du groupe additif $\mathfrak{a}^*$ des matrices diagonales de trace nulle sur A^*, qui transforme la mesure de Lebesgue en une mesure de Haar. On a donc :

$$\int_{A^*_t} \rho(a)\, da = \prod_{1 \leqq i < n} \left(\int_{-\infty}^{\log t} (\exp r_i y_i).dy_i \right) < \infty.$$

1.12. *Minima successifs.* Nous revenons maintenant à $\mathbf{GL}(n, \mathbf{R})$. Le théorème 1.6 a été démontré à l'aide d'une récurrence et d'une condition de minimum. Nous voulons indiquer ici quelques variantes de ce procédé, qui font appel à k conditions de minimum successives $(1 \leqq k \leqq n)$.

Soient I_n l'ensemble des entiers compris entre 1 et n, et $j \in I_n$. Les éléments $e_{i_1} \wedge \ldots \wedge e_{i_j}$ $(i_1 < \ldots < i_j)$ forment une base de la $j^{\text{ième}}$ puissance extérieure $\wedge^j \mathbf{R}^n$ de $\mathbf{R}^n$. On notera aussi $||\ ||$ la norme euclidienne de $\wedge^j \mathbf{R}^n$ pour laquelle cette base est orthonormale. Soit $\Phi_j : G \to \mathbf{R}$ la fonction définie par :

$$\Phi_j(g) = ||g(e_1) \wedge \ldots \wedge g(e_j)||.$$

C'est une fonction continue > 0, qui vérifie

$$\Phi_j(k.a.n) = \Phi_j(a) = a_{11} \ldots a_{jj}. \tag{1}$$

$$\Phi_j(g.b) = \Phi_j(g).\Phi_j(b) = \Phi_j(g)\,|\Lambda_j(b)|, \tag{2}$$

où Λ_j désigne l'homomorphisme du groupe trigonal supérieur B dans $\mathbf{R}^*$ qui envoie $b = (b_{ij})$ sur $b_{11} \ldots b_{jj}$. Évidemment, la fonction Φ considérée en 1.6 n'est autre que Φ_1.

Soit P_j le sous-groupe formé des éléments $g = (g_{ik})$ de $\mathbf{GL}(n, \mathbf{R})$ qui laissent stable le j-plan sous-tendu par $e_1, \ldots, e_j$, donc qui vérifient $g_{ik} = 0$ si $i \geqq j + 1$ et $k \leqq j$. Il est immédiat que Φ_j est invariante à droite par $\Gamma \cap P_j$. Pour toute partie D de I_n, on pose :

$$\Phi_D = \prod_{j \in D} \Phi_j, \qquad P_D = \bigcap_{j \in D} P_j.$$

On a donc :

$$\Phi_D(g.\gamma) = \Phi_D(g) \qquad (g \in G;\ \gamma \in \Gamma \cap P_D). \tag{3}$$

Soit L_j le réseau de $\wedge^j \mathbf{R}^n$ engendré par la base $(e_{i_1} \wedge \ldots \wedge e_{i_j})$. Il est clair que $\Gamma(L_j) = L_j$, donc, pour $g \in G$ fixé, $g.\Gamma(e_1 \wedge \ldots \wedge e_j)$ est dans l'ensemble des éléments non nuls d'un réseau de $\wedge^j \mathbf{R}^n$. Par suite, étant donné $c > 0$, Φ_j ne prend sur $g.\Gamma$ qu'un nombre fini de valeurs $\leqq c$. Il s'ensuit que Φ_D a un minimum > 0 sur $g.\Gamma$. Cela étant, le lemme 1.5 admet la généralisation suivante.

1.13. LEMME. *On conserve les notations précédentes. Soit* $g \in G$ *tel que :*

$$\Phi_D(g) \leqq \Phi_D(g.\gamma) \qquad (\gamma \in \Gamma \cap P_{D'};\ D' = I_n - D) \tag{1}$$

et soit $g = k.a.n$ *la décomposition d'Iwasawa de g. Alors*

$$a_{jj} \leqq (2/\sqrt{3}).a_{j+1,\,j+1}, \qquad (j \in D). \tag{2}$$

Le groupe $N_{\mathbf{Z}} = N \cap \Gamma$ est contenu dans $\Gamma \cap P_D$, et la multiplication à droite par un élément de $N_{\mathbf{Z}}$ ne change ni la valeur de Φ_D, ni la composante en A d'un élément. Comme $N = N_{1/2}.N_{\mathbf{Z}}$, (1.4(1)), on peut supposer que

$$|n_{ij}| \leqq 1/2 \qquad (1 \leqq i \leqq j \leqq n).$$

Fixons $j \in D$. Soit z_j l'élément de $\Gamma \cap P_{D'}$, qui laisse fixe e_i $(i \neq j, j+1)$ et applique e_j, e_{j+1} sur e_{j+1} et $-e_j$ respectivement. Il est immédiat que $\Phi_i(g) = \Phi_i(g.z_j)$ si $i \neq j$, donc l'hypothèse entraîne :

$$\Phi_j(g) \leqq \Phi_j(g.z_j). \tag{3}$$

On vérifie sans difficulté que l'on peut écrire :

$$n = n'.n'',$$

où $n', n'' \in N$, et n' a tous ses coefficients non diagonaux nuls, à l'exception éventuelle de $n'_{j,j+1} = n_{j,j+1}$, et où $n''_{j,j+1} = 0$, et que l'on a :

$$n^* = z_j.n''.z_j^{-1} \in N, \qquad n^*_{j,j+1} = 0.$$

Mettons a sous la forme

$$a = a'.a'' \qquad (a'_{ii} = 1,\ i \neq j, j+1;\quad a'_{ii} = a_{ii},\ i = j, j+1;\quad a'' \in A).$$

On a :

$$\Phi_j(g) = a_{11} \dots a_{jj} = a_{11} \dots a_{j-1,j-1}.\Phi_j(a'.n')$$
$$\Phi_j(g.z_j) = \Phi_j(a'.a''.n'.z_j.n^*) = \Phi_j(a'.a''.n'.z_j)$$

comme $a''_{ii} = 1$, $(i = j, j+1)$, l'élément a'' commute à $n'.z_j$ et :

$$\Phi_j(g.z_j) = \Phi_j(a'.n'.z_j.a'') = a_{11} \dots a_{j-1,j-1}.\Phi_j(a'.n'.z_j).$$

(3) implique donc :

$$\Phi_j(a'.n') \leqq \Phi_j(a'.n'.z_j).$$

On en déduit alors (2) par une démonstration en tous points semblable à celle du lemme 1.5.

1.14. THÉORÈME. *Soit $D_1, \dots, D_s$ une partition de l'ensemble des entiers compris entre 1 et n, et soit $g \in G$. Alors il existe $h \in g.\Gamma \cap \mathfrak{S}_{2/\sqrt{3},1/2}$ qui vérifie les conditions*

$$\Phi_{D_1}(h) \leqq \Phi_{D_1}(h.\gamma) \qquad (\gamma \in \Gamma)$$
$$\Phi_{D_i}(h) \leqq \Phi_{D_i}(h.\gamma) \qquad (\gamma \in \Gamma \cap P_{D_1 \cup \dots \cup D_{i-1}},\ 1 < i \leqq s). \tag{1}$$

Comme Φ_{D_1} a un minimum sur $g.\Gamma$, on peut trouver $\gamma_1 \in \Gamma$ tel que :

$$\Phi_{D_1}(g.\gamma_1) \leqq \Phi_{D_1}(g.\gamma) \qquad (\gamma \in \Gamma).$$

Soit $h_1 = g.\gamma_1$. Alors :

$$\Phi_{D_1}(h_1) \leqq \Phi_{D_1}(h_1.\gamma) \qquad (\gamma \in \Gamma). \tag{2}$$

On peut ensuite trouver $\gamma_2 \in \Gamma \cap P_{D_1}$ tel que :

$$\Phi_{D_2}(h_1.\gamma_2) \leqq \Phi_{D_2}(h_1.\gamma) \qquad (\gamma \in \Gamma \cap P_{D_2}). \tag{3}$$

Mais Φ_{D_1} est invariante à droite par $\Gamma \cap P_{D_1}$. Par conséquent $h_2 = h_1.\gamma$ vérifiera encore les mêmes conditions (2), (3) que h_1. En procédant ainsi par récurrence, on voit qu'il existe $h \in g\Gamma$ vérifiant (1). Comme $N = N_{1/2}.N_Z$ et les fonctions Φ_D sont invariantes à droite par N_Z, on peut supposer $h \in K.A.N_{1/2}$. Mais on a $h \in K.A_{2/\sqrt{3}}.N$ d'après le lemme 1.13, donc $h \in \mathfrak{S}_{2/\sqrt{3},1/2}$.

§ 2. Réduction des formes quadratiques positives non dégénérées

2.1. Identifions l'ensemble des formes quadratiques positives non dégénérées sur $\mathbf{R}^n$ à l'ensemble $\mathfrak{H} = \mathfrak{H}_n$ des matrices symétriques positives non dégénérées. Le groupe $G = \mathbf{GL}(n, \mathbf{R})$ opère à droite sur $\mathfrak{H}$ par :

$$F \mapsto {}^t g.F.g = F[g],$$

le groupe d'isotropie de la forme identité étant $K = \mathbf{O}(n)$.
G est transitif sur $\mathfrak{H}$ et $\mathfrak{H} = K\backslash G$. La projection $\pi : G \to \mathfrak{H}$ définie par $\pi(g) = {}^t g.g = I[g]$ commute à G, opérant sur lui-même par translations à droite :

$$\pi(g)\,[g'] = \pi(g.g'), \qquad (g, g' \in G).$$

Il est clair que π applique $\mathbf{SL}(n, \mathbf{R})$ sur l'ensemble $\mathfrak{H}^{(1)}$ des éléments de déterminant 1 de $\mathfrak{H}$ et que $\mathfrak{H}^{(1)} = \mathbf{SO}(n)\backslash\mathbf{SL}(n, \mathbf{R})$. On peut aussi identifier $\mathfrak{H}^{(1)}$ à l'ensemble des demi-droites de $\mathfrak{H}$.

Définition. On appelle *ensemble de Siegel* $\mathfrak{S}'_{t,u}$ dans $\mathfrak{H}$ tout ensemble de la forme :

$$\mathfrak{S}'_{t,u} = \{{}^t n.a.n \mid a \in A_t, n \in N_u\}.$$

Si $g = kan \in \mathfrak{S}_{t,u}$, alors :

$${}^t g.g = {}^t n.{}^t a.{}^t k.k.a.n = {}^t n.a^2.n \in \mathfrak{S}'_{t^2,u}.$$

On en déduit aussitôt que :

$$\pi(\mathfrak{S}_{t,u}) = \mathfrak{S}'_{t^2,u} \qquad \text{et} \qquad \pi^{-1}(\mathfrak{S}'_{t^2,u}) = \mathfrak{S}_{t,u}.$$

Comme $\pi(gg') = \pi(g)[g']$, les résultats de 1.4, 1.6, 1.10, 1.13 sont équivalents au :

2.2. Théorème.
(i) (Korkine-Zolotareff). $\mathfrak{H} = \mathfrak{S}'_{t,u}[\Gamma]$, *dès que* $t \geqslant 4/3$ *et* $u \geqslant 1/2$.
(ii) (Hermite). *Si* F *est une forme quadratique positive non dégénérée sur* $\mathbf{R}^n$

$$\min_{x \in \mathbf{Z}^n - \{0\}} F(x) \leqslant (4/3)^{\frac{n-1}{2}} (\det F)^{1/n}$$

(iii) (Minkowski). $\mathfrak{H}^{(1)} = \mathfrak{S}'_{t,u}.\mathbf{SL}(n, \mathbf{Z})$, *si* $t \geqslant 4/3$ *et* $u \geqq 1/2$, *et* $\mathfrak{H}^{(1)}/\mathbf{SL}(n, \mathbf{Z})$ *est de volume invariant fini.*

Un élément de $\mathfrak{S}'_{4/3,\,1/2}$ s'appelle souvent une *forme réduite* au sens de Hermite.

2.3. *Cas particulier :* $n = 2$. Soit $\lambda : \mathbf{SL}(2, \mathbf{R}) \to \mathbf{SL}(2, \mathbf{R})$ l'application qui associe $\begin{pmatrix} d & b \\ c & a \end{pmatrix}$ à $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On vérifie tout de suite que $\lambda(g) = w.{}^t g.w^{-1}$, avec $w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, donc que λ est un anti-automorphisme involutif.
Le groupe $\mathbf{SL}(2, \mathbf{R})$ opère à gauche sur le demi-plan de Poincaré

$$P = \{z \in \mathbf{C} \mid \operatorname{Im} z > 0\}$$

par les transformations conformes $z \mapsto g.z = (az + b)\,(cz + d)^{-1}$. On peut donc le faire opérer à droite en associant à g la transformation :

$$z \mapsto \lambda(g).z = (dz + b)\,(cz + a)^{-1}.$$

Il est immédiat que le groupe d'isotropie du point i est $\mathbf{SO}(2)$ et que

$$(\mathfrak{S}_{t,u}).i = \{z \in \mathrm{P},\ |\mathrm{Re}\, z| \leqq u,\ \mathrm{Im}\, z \geqq t\}.$$

Un tel ensemble contient le domaine fondamental classique du groupe modulaire ($|\mathrm{Re}\, z| \leqq 1/2,\ |z| \geqq 1$) si, et seulement si, $t \geqq 2/\sqrt{3},\ u \geqq 1/2$. Ces constantes sont les meilleures possibles pour $n = 2$. On voit aussi que $\mathfrak{S}_{2/\sqrt{3},\,1/2}$ n'est qu'une approximation d'un domaine fondamental au sens strict, et rencontre certaines orbites de $\mathbf{SL}(2, \mathbf{Z})$ en plus d'un point intérieur.

Une forme quadratique binaire positive non dégénérée $\mathrm{F}(x, y)$ s'écrit d'une seule manière $\mathrm{F}(x, y) = a(x + \tau y)\,(x + \overline{\tau} y)$ avec $\mathrm{Im}\, \tau > 0$, et $\varphi : \mathrm{F} \mapsto \tau$ est une bijection de $\mathfrak{H}_2^{(1)}$ sur P. On laisse au lecteur le soin de vérifier que φ est « λ-équivariante », c'est-à-dire que :

$$\varphi(\mathrm{F}[g]) = \lambda(g)\,(\varphi(\mathrm{F})).$$

On sait que :

$$\mathrm{Im}\, g.z = \mathrm{Im}\, z.\,|(cz + d)|^{-2} \qquad (g \in \mathrm{G};\quad z \in \mathrm{P}).$$

En particulier,

$$\mathrm{Im}\, g(i) = (a^2 + c^2)^{-2} = \Phi(g)^{-2}$$

dans les notations de 1.5. Le lemme 1.6 pour $n = 2$ équivaut donc au fait bien connu que, pour tout $z \in \mathrm{P}$, $\mathrm{Im}\, \gamma(z)$ ($\gamma \in \Gamma$), atteint son maximum en un point de $\mathfrak{S}'_{4/3,\,1/2} \cap \Gamma.z$.

2.4. Nous nous proposons maintenant d'établir quelques relations entre les principes de réduction de Hermite, décrit plus haut, et de Minkowski. Soient V un espace vectoriel réel de dimension finie, L un réseau de V et F une forme quadratique positive non dégénérée sur V. On dira que F est M-réduite par rapport à une base $(u_i)_{1 \leqq i \leqq n}$ de L si elle vérifie la condition suivante :

(M) $\mathrm{F}(u_1) \leqq \mathrm{F}(x)$ $(x \in \mathrm{L} - \{0\})$. Pour $i = 2, \ldots, n$, $\mathrm{F}(u_i) \leqq \mathrm{F}(x)$ si x parcourt l'ensemble des éléments de L qui font partie d'une base de L contenant $u_1, \ldots, u_{i-1}$, et sont distincts de ceux-ci.

On a évidemment :

$$\mathrm{F}(u_1) \leqq \ldots \leqq \mathrm{F}(u_n). \tag{1}$$

[Pour obtenir une forme réduite au sens de Minkowski, il faut encore imposer

$$\mathrm{F}(u_i, u_{i+1}) \geqq 0 \qquad (i = 1, \ldots, n - 1).$$

Donc si F vérifie (M), il existe $\varepsilon_i = \pm 1$ tels que F soit réduite au sens de Minkowski par rapport à $(\varepsilon_i u_i)$. Nous omettrons cette condition qui ne jouera pas de rôle ici.]

Une forme quadratique positive non dégénérée sur $\mathbf{R}^n$ sera dite M-réduite si elle est M-réduite par rapport à la base canonique (e_i), et $\mathfrak{M}$ dénotera l'ensemble des formes M-réduites. Il est immédiat que toute $\mathrm{F} \in \mathfrak{H}$ est M-réduite par rapport

à au moins une base de $\mathbf{Z}^n$. Par conséquent, $\mathfrak{H} = \mathfrak{M}[\mathbf{GL}(n, \mathbf{Z})]$. Nous voulons montrer que $\mathfrak{M}$ est contenu dans un domaine de Siegel. Nous nous appuyerons pour cela sur le lemme suivant, dû à Mahler :

2.5. LEMME. *On conserve les notations de* 2.4 *et on suppose* F M*-réduite par rapport à* (u_i). *Soit* $m_i(\mathrm{F})$ *le plus petit nombre* $a > 0$ *tel que l'on puisse trouver* i *éléments linéairement indépendants* $x_j \in \mathrm{L}$ *tels que* $\mathrm{F}(x_j) \leqq a$, $(1 \leqq j \leqq i;\ i = 1, \ldots, n)$. *Alors :*

$$m_i(\mathrm{F}) \leqq \mathrm{F}(u_i) \leqq (3/2)^{2(i-1)}.m_i(\mathrm{F}) \qquad (1 \leqq i \leqq n). \tag{1}$$

On a évidemment :

$$m_1(\mathrm{F}) \leqq \ldots \leqq m_n(\mathrm{F}), \quad m_1(\mathrm{F}) = \mathrm{F}(u_1), \quad \mathrm{F}(u_i) \geqq m_i(\mathrm{F}) \quad (1 \leqq i \leqq n). \tag{2}$$

Le lemme étant évident pour $i = 1$, on suppose $i > 1$, et (1) vraie pour $j < i$. Il existe n éléments $t_k \in \mathrm{L}$, linéairement indépendants, tels que :

$$\mathrm{F}(t_k) = m_k(\mathrm{F}) \qquad (1 \leqq k \leqq n)$$

et un indice $j \leqq i$ tels que $(t_j, u_1, \ldots, u_{i-1})$ soient linéairement indépendants. Désignons par L′ et M les $\mathbf{Z}$-modules engendrés respectivement par $u_1, \ldots, u_{i-1}$ et $u_1, \ldots, u_{i-1}, t_j$ et soit :

$$\mathrm{M}' = \mathrm{L} \cap (\mathbf{R}u_1 + \ldots + \mathbf{R}u_{i-1} + \mathbf{R}t_j).$$

On a donc $\mathrm{M}' \supset \mathrm{M} \supset \mathrm{L}'$, et M′ est évidemment un facteur direct dans L. Il suffit par conséquent de prouver l'existence d'un élément t' de M′ tel que $(t', u_1, \ldots, u_{i-1})$ soit une base de M′ et que

$$\mathrm{F}(t') \leqq (3/2)^{i-1}.m_i(\mathrm{F}). \tag{3}$$

Le groupe L′ est un facteur direct dans L, donc aussi dans M′ et M. Par suite, M′/L′ est un module libre de rang un, et M/L′ est d'indice fini dans M′/L′. Si t' est un élément de M′ dont la classe modulo L′ est un générateur de M′/L′, on voit que $(t', u_1, \ldots, u_{i-1})$ est une base de M′ et que $t_j \equiv c.t' \mod \mathrm{L}'$, $(c \in \mathbf{Z},\ c \neq 0)$. Cela peut s'écrire :

$$t' = c^{-1}.t_j + c_1.u_1 + \ldots + c_{i-1}.u_{i-1} \qquad (c_j \in \mathbf{Q};\ 1 \leqq j \leqq i - 1).$$

Quitte à ajouter à t' un élément de L′, on peut supposer $|c_j| \leqq 1/2$. On a alors :

$$\mathrm{F}(t')^{1/2} \leqq |c|^{-1}\,\mathrm{F}(t_j)^{1/2} + 1/2(\mathrm{F}(u_1)^{1/2} + \ldots + \mathrm{F}(u_{i-1})^{1/2}).$$

Compte tenu de l'hypothèse de récurrence, on en tire :

$$\mathrm{F}(t')^{1/2} \leqq m_j(\mathrm{F})^{1/2} + 1/2 \left(\sum_{1 \leqq k < i} (3/2)^{k-1} m_k(\mathrm{F}) \right)$$

d'où (3), puisque la suite des $m_k(\mathrm{F})$ est croissante.

2.6. THÉORÈME (Minkowski). *Soit* n *un entier* > 0. *Il existe une constante* C_n *telle que l'on ait :*

$$\mathrm{F}(e_1) \cdot \ldots \cdot \mathrm{F}(e_n) \leqq \mathrm{C}_n.\det \mathrm{F}$$

pour toute forme quadratique positive non dégénérée et M*-réduite sur* $\mathbf{R}^n$.

On reprend les notations précédentes, en particulier pour $\mathfrak{H}$, A, N. Soit $F \in \mathfrak{H}$. Elle est de la forme $F = {}^t(a.n).a.n = {}^tn.a^2.n$. En désignant par a_i les termes diagonaux de a, on a donc :

$$F(x) = \sum_{1 \leqq i \leqq n} a_i^2(x_i + n_{i,i+1}.x_{i+1} + \ldots + n_{i,n}.x_n)^2, \tag{1}$$

et, en particulier :

$$F(e_i) = a_i^2 + a_{i-1}^2.n_{i-1,i}^2 + \ldots + a_1^2.n_{1,i}^2, \tag{2}$$

donc aussi :

$$a_i^2 \leqq F(e_i), \qquad (1 \leqq i \leqq n). \tag{3}$$

Si F parcourt un ensemble de Siegel $\mathfrak{S}'$, on a par conséquent :

$$a_i^2 \asymp F(e_i), \qquad (F \in \mathfrak{S}') \tag{4}$$

(cf. 0.5 pour $\asymp$, $\prec$, $\succ$).

D'après 2.2, il existe $g \in \mathbf{GL}(n, \mathbf{Z})$ telle que $F' = F[g] \in \mathfrak{S}'_0$, où l'on écrit $\mathfrak{S}'_0$ pour $\mathfrak{S}'_{4/3,\,1/2}$. On a :

$$F' = {}^t(a'.n').a'.n' \qquad (a' \in A_{2/\sqrt{3}},\ n' \in N_{1/2}). \tag{5}$$

Il est clair que

$$\prod_i a_i^2 = \det F = \det F' = \prod_i a_i'^2, \tag{6}$$

et que, dans les notations de 2.5,

$$m_i(F) = m_i(F') \qquad (1 \leqq i \leqq n). \tag{7}$$

Vu (4) et (7), on a :

$$m_i(F) \prec a_i'^2, \ (1 \leqq i \leqq n; \quad F \in \mathfrak{H},\ F' \in \mathfrak{S}'_0 \cap F[\mathbf{GL}(n, \mathbf{Z})]). \tag{8}$$

Supposons maintenant que F soit M-réduite. Alors, (3), (8) et 2.5, donnent :

$$a_i^2 \leqq F(e_i) \prec a_i'^2 \qquad (1 \leqq i \leqq n; \quad F \in \mathfrak{M}) \tag{9}$$

et la conclusion résulte alors de (6).

2.7. COROLLAIRE. *L'ensemble $\mathfrak{M}$ des formes* M*-réduites est contenu dans un ensemble de Siegel.*

Les relations $a_i^2 \leqq F(e_i)$ et $\prod a_i^2 \succ \prod F(e_i)$ montrent que l'on a en fait :

$$a_i^2 \asymp F(e_i) \qquad (1 \leqq i \leqq n; \quad F \in \mathfrak{M}). \tag{1}$$

Comme les $F(e_i)$ forment une suite croissante, cela entraîne l'existence d'une constante $t > 0$ telle que $a \in A_t$ pour tout $F \in \mathfrak{M}$. Il reste à montrer que n varie dans un ensemble borné de N.

Fixons $i \geqq 2$. On a :

$$F(e_i) \leqq F(e_i + u_{i-1}.e_{i-1} + \ldots + u_1 e_1)$$

quels que soient les entiers u_i. Fixons k $(1 \leqq k < i)$, et supposons $u_j = 0$ pour $k < j < i$. Alors, dans le membre de droite, vu 2.6 (1), le coefficient de a_j^2 $(k < j < i)$

est égal à $n_{j,i}^2$, et l'on voit aisément que, en choisissant convenablement les u_j ($j \leqq k$), on peut faire en sorte que les coefficients des a_j^2 soient $\leqq 1/4$ pour $j \leqq k$. On obtient donc, vu 2.6 (2) :

$$a_1^2 n_{1,i}^2 + \ldots + a_k^2 n_{k,i}^2 \leqq 1/4(a_1^2 + \ldots + a_k^2).$$

Comme $a \in A_t$, cela entraîne que :

$$a_k^2 \succ a_k^2 . n_{k,i}^2 \qquad (i = 2, \ldots, n; k = 1, 2, \ldots, i-1)$$

et montre que $n_{k,i}^2$ est borné, puisque $a_k \neq 0$.

2.8. On dira qu'un élément $g \in \mathbf{GL}(n, \mathbf{R})$ est M-réduit si ${}^t g.g$ est M-réduite. 2.7 entraîne que l'ensemble $\mathfrak{M}'$ des éléments M-réduits de $\mathbf{GL}(n, \mathbf{R})$ est contenu dans un ensemble de Siegel. Évidemment, $K.\mathfrak{M}' = \mathfrak{M}'$ et $\mathbf{GL}(n, \mathbf{R}) = \mathfrak{M}'.\mathbf{GL}(n, \mathbf{Z})$.

Note bibliographique

Les résultats des §§ 1, 2 ont été tout d'abord formulés dans le cadre des formes quadratiques. Le théorème 2.2 (i) est dû à Korkine-Zolotareff [15], mais en fait, il ne fait qu'expliciter un principe de réduction des formes quadratiques positives dû à Hermite [13] (et qui remonte à Gauss pour $n = 2$) et qui a permis à cet auteur de démontrer notamment 2.2 (ii). Le critère de Mahler est prouvé dans [16]. Des démonstrations ne faisant pas appel à la réduction des formes quadratiques ont été données par Chabauty et, dans un cadre plus général, par Macbeath et Swierczkowski (voir [8, Chap. 8, § 5] ou aussi Cassels, *Geometry of numbers*, Springer édit.).
La finitude du volume de $\mathfrak{H}^{(1)}/\mathbf{SL}(n, \mathbf{Z})$ est démontrée par Minkowski dans [17], où se trouve développée une théorie de la réduction basée sur la notion appelée ici réduite de Minkowski (2.4). Elle contient 2.6, et mène à des résultats plus précis que ceux de 1.4 ou 2.2, mais dont nous n'aurons pas besoin.

§ 3. Décomposition de Bruhat de $\mathbf{GL}(n, k)$

Ce paragraphe donne la démonstration de l'existence d'une « décomposition de Bruhat » dans un cas particulier élémentaire. Pour l'énoncé général, cf. § 11.

3.1. Dans ce paragraphe, sauf mention expresse du contraire, le corps de base k est un corps commutatif quelconque distinct du corps à deux éléments. On désigne par G le groupe $\mathbf{GL}(n, k)$, par D le sous-groupe des matrices diagonales inversibles, par N (resp. N^-) le sous-groupe des matrices unipotentes triangulaires supérieures (resp. inférieures) par $B = DN$ le sous-groupe des matrices triangulaires supérieures inversibles.
Puisque k contient au moins deux éléments inversibles distincts, il est immédiat

que les droites ke_i engendrées par les vecteurs de la base canonique sont les seules droites stables par D. Elles sont donc permutées par les éléments du normalisateur N(D) de D (qui est donc le groupe des matrices monomiales), d'où un morphisme visiblement surjectif de N(D) dans le groupe symétrique de degré n, dont le noyau est D. Le groupe $W = N(D)/D$ est le « groupe de Weyl » de $\mathbf{GL}(n, k)$ relatif à D.

Pour tout $w \in N(D)/D = W$, choisissons un relèvement $s_w \in N(D)$. (Par exemple, notant σ la permutation de $[1, n]$ associée à w, on peut prendre pour s_w la matrice de permutations telle que $(s_w)_{\sigma(p),\,p} = 1$ et $(s_w)_{q,\,p} = 0$ si $q \neq \sigma(p)$. C'est un élément du groupe K des matrices orthogonales.)

Le groupe W agit sur les fonctions sur D par $w(\alpha)\,(d) = \alpha(w^{-1}(d))$. Il opère en particulier sur les caractères rationnels de D, qui sont les homomorphismes de la forme $t \mapsto t_1^{m_1} \ldots t_n^{m_n}$ $(m_i \in \mathbf{Z})$. On a notamment :

$$w(t_i) = t_{\sigma(i)};\ w(t_i/t_{i+1}) = w(\alpha_i) = t_{\sigma(i)}/t_{\sigma(i+1)},$$

σ désignant la permutation associée à w.

On voit donc que :

$$w(\alpha_i) = \prod_{1 \leqslant j \leqslant n-1} \alpha_j^{n_{ij}(w)},$$

où l'on a $n_{ij}(w) = 1$, pour $\sigma(i) \leqslant j < \sigma(i+1)$ et $n_{ij}(w) = 0$ pour les autres valeurs de j, si $\sigma(i) < \sigma(i+1)$, et $n_{ij}(w) = -1$, pour $\sigma(i+1) \leqslant j < \sigma(i)$ et $n_{ij}(w) = 0$ pour les autres valeurs de j, si $\sigma(i+1) < \sigma(i)$.

3.2. LEMME. *Soit $w \in W$. Supposons qu'il existe un indice λ tel que $n_{i\lambda}(w) \geqslant 0$ pour $i = 1, \ldots, n-1$. Alors tout relèvement s_w est dans le sous-groupe « parabolique » P_λ (sous-groupe des matrices inversibles (q_{ik}) telles que $q_{ik} = 0$ pour les couples tels que $1 \leqslant k \leqslant \lambda$, $\lambda + 1 \leqslant l \leqslant n$).*

En effet, l'hypothèse entraîne aussitôt que si $a < b$, on a :

$$w(t_a/t_b) = \prod_{1 \leqslant j \leqslant n-1} \alpha_j^{n_{a,b,j}(w)}$$

avec des exposants $n_{a,b,j} \geqslant 0$.

Raisonnons par l'absurde; si s_w n'est pas dans P_λ, c'est qu'il existe un indice $a \leqslant \lambda$ tel que $\sigma(a) > \lambda$. Mais comme dans s_w, il y a un élément et un seul par ligne qui soit non nul, il existe aussi $b > \lambda$ tel que $\sigma(b) \leqslant \lambda$.

Alors $w(t_a/t_b) = t_{\sigma(a)}/t_{\sigma(b)} = \alpha_{\sigma(a-1)}^{-1} \cdot \alpha_{\sigma(a-2)}^{-1} \cdot \ldots \cdot \alpha_{\sigma(b)}^{-1}$, ce qui est contradictoire. Le lemme est démontré.

Choisissons maintenant un relèvement s_w de chaque $w \in W$. On a donc :

$$N(D) = \bigcup_{w \in W} s_w D$$

et pour chaque w l'ensemble $G_w = Ns_wB$ ne dépend que de w.

3.3. THÉORÈME. *Les ensembles $G_w (w \in W)$ forment une partition de G.*

Pour démontrer le théorème, il sera commode d'utiliser la notion de drapeau : un drapeau dans un espace vectoriel de dimension n est une suite croissante de sous-espaces :

$$V_1 \subset V_2 \subset \ldots \subset V_n,$$

telle que $\dim V_i = i$. En particulier dans k^n le drapeau canonique F_0 est le drapeau tel que V_i soit engendré par les i premiers vecteurs de la base canonique.
Le groupe G opère transitivement dans l'ensemble $\mathscr{F}$ des drapeaux et B est le groupe d'isotropie du drapeau F_0 de sorte que $\mathscr{F}$ s'identifie canoniquement à l'espace homogène G/B.
Cela dit le théorème peut encore s'énoncer ainsi : pour tout drapeau F, il existe au moins un $w \in W$ et un $n \in N$, tel que $F = ns_w(F_0)$; de plus, w est déterminé de manière unique par F. D'autre part, pour démontrer le théorème, il suffit d'envisager les cas où on a choisi pour s_w une matrice de permutation. Dans cette démonstration, on note aussi w la permutation de $[1, n]$ associée à $w \in W$.
Si $F = (V_1, V_2, \ldots, V_n)$ peut s'écrire $ns_w(F_0)$, c'est que le sous-espace V_i est engendré par les vecteurs $v_1, v_2, \ldots, v_i$ où :

$$v_i = e_{w(i)} + \sum_{1 \leqslant k \leqslant w(i)} n_{kw(i)} e_k.$$

On voit donc que pour tout $i \geqslant 1$, $w(i)$ est le plus grand indice distinct de $w(1), \ldots, w(i-1)$ tel qu'il existe dans $V_i \cap \complement V_{i-1}$ un vecteur v_i dont la $w(i)^{\text{ème}}$ coordonnée soit non nulle, donc w est déterminé par F (on a posé $V_0 = (0)$).
Réciproquement, étant donné F, on peut trouver une suite de vecteurs (v_i), et une permutation w vérifiant la condition précédente, v_i s'écrivant sous la forme :

$$v_i = e_{w(i)} + \sum_{1 \leqslant k \leqslant w(i)} n_{kw(i)} e_k.$$

On a alors $F = ns_w(F_0)$, où $n \in N$ a les coefficients $n_{kw(i)}$.
Nous allons maintenant écrire les ensembles G_w sous une forme différente. Ceci exige la démonstration de quelques lemmes.

3.4. LEMME. *Pour toute matrice carrée g d'ordre n soit $\Delta_i(g)$ le déterminant de la matrice $(g_{kl})_{1 \leqslant k, l \leqslant i}$. L'application produit définit une bijection φ de $N^- \times B$ (resp. $N^- \times N$) sur l'ensemble des $g \in G$ tels que $\Delta_i(g) \neq 0$ (resp. $\Delta_i(g) = 1$) pour $i = 1, 2, \ldots, n-1$. Les coefficients de $\varphi^{-1}(g)$ sont des polynômes, à coefficients entiers en les coefficients de g et les inverses des $\Delta_i(g)$.*

Comme $\Delta_i(n^-.b) = b_{11} \ldots b_{ii}$ si $n^- \in N^-$ et $b \in B$, il est clair que l'image de $N^- \times B$ (resp. $N^- \times N$) est contenue dans l'ensemble des g, tels que $\Delta_i(g) \neq 0$ (resp. $\Delta_i(g) = 1$). Il suffit d'autre part, de démontrer l'assertion relative à $N^- \times B$. Elle est évidente pour $n = 1$. Nous pouvons la supposer vraie pour $n-1$ ($n > 1$) et raisonner par récurrence.
Soient $n^- \in N^-$ et $b \in B$. Écrivons-les sous la forme :

$$n^- = \begin{pmatrix} n' & 0 \\ n'' & 1 \end{pmatrix} \qquad b = \begin{pmatrix} b' & b'' \\ 0 & b_{n,n} \end{pmatrix}$$

où n' et b' sont carrés d'ordre $n-1$, n'' une matrice à 1 ligne et $(n-1)$ colonnes et b'' une matrice à 1 colonne et $(n-1)$ lignes.
Alors,

$$n^- b = \begin{pmatrix} n'b' & n'b'' \\ n''b' & b_{n,n} + n''b'' \end{pmatrix}.$$

Soit g une matrice telle que $\Delta_i(g) \neq 0$ pour tout i. Écrivons-la sous la forme :

$$g = \begin{pmatrix} g' & q \\ p & g_{n,n} \end{pmatrix} \quad \text{où } g' \text{ est carrée d'ordre } n-1.$$

Avec les notations précédentes, la relation $g = n^- . b$ équivaut à :

$$g' = n'b', \qquad p = n''b', \qquad q = n'b'', \qquad g_{n,n} = b_{n,n} + n''b''.$$

D'après l'hypothèse de récurrence, il existe n' triangulaire unipotente inférieure d'ordre $n-1$ et b' triangulaire supérieure, uniques, telles que $g' = n'.b'$. Comme n' et b' sont inversibles, les relations $p = n''.b'$, $q = n'.b''$ déterminent uniquement n'' et b''. Alors $b_{n,n}$ est déterminé par la dernière relation. L'existence et l'unicité de n^- et b sont ainsi prouvées.
La dernière assertion résulte aussitôt des considérations précédentes.
Pour tout couple d'indices (i,j), $(i \neq j)$, désignons par N_{ij} le sous-groupe des matrices n de N telles que tous les éléments non diagonaux autres que n_{ij} soient nuls.

3.5. LEMME. (i) *Le produit définit une bijection de* $\prod_{1 \leqslant i \leqslant n-1} \left(\prod_{i+1 \leqslant j \leqslant n} N_{ij} \right)$ *sur* N.
(ii) *Pour n'importe quel ordre sur l'ensemble des couples* (i,j) *où* $i < j$, *le produit définit une surjection du produit* $\prod N_{ij}$ *où les facteurs sont pris dans l'ordre des couples* (i,j), *sur* N.

Prouvons (i) par récurrence sur n (il n'y a rien à démontrer pour $n = 1$). Soit n une matrice de N. Écrivons :

$$n = \begin{pmatrix} 1 & a \\ 0 & n' \end{pmatrix}$$

où n' est une matrice unipotente d'ordre $(n-1)$. On a alors :

$$n = \begin{pmatrix} 1 & 0 \\ 0 & n' \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & I_{n-1} \end{pmatrix}.$$

En d'autres termes, si l'on identifie le groupe N' des matrices triangulaires unipotentes supérieures d'ordre $n-1$ au sous-groupe de N formé des matrices de N vérifiant $n_{12} = n_{13} = \ldots n_{1n} = 0$, et si l'on désigne par A les matrices de N dont tous les éléments autres que les éléments diagonaux et ceux de la première ligne sont nuls, le produit définit une bijection de $N' \times A$ sur N.
Mais par hypothèse de récurrence le produit définit une bijection de

$$\prod_{2 \leqslant i \leqslant n-1} \left(\prod_{i+1 \leqslant j \leqslant n} N_{ij} \right) \text{ sur } N'.$$

D'autre part, tout élément a de A s'écrit de manière unique comme produit d'éléments appartenant aux $N_{1j} (2 \leqslant j \leqslant n)$. De manière précise $a = \prod \bar{a}_j$ où $\bar{a}_j$ est l'élément de N_{1j} tel que le coefficient d'indices $(1,j)$ soit a_{1j}.
Il en résulte que tout élément de N peut s'écrire de manière unique comme produit d'éléments appartenant aux N_{ij} pris dans l'ordre lexicographique.
L'assertion (ii) résulte aussitôt de (i) et des deux remarques suivantes :

(a) N_{ij} et $N_{i'j'}$ se centralisent l'un l'autre sauf si $i' = j$ ou $j' = i$.

(b) Si $i' = j$, on a :

$$N_{ij} N_{i',j'} \subset N_{i',j'} N_{ij} N_{ij'}.$$

Remarque. On peut prouver que pour tout ordre sur l'ensemble des couples (i,j) le produit définit une bijection de $\prod N_{ij}$, les facteurs étant pris dans l'ordre croissant des couples (i,j), sur N.
Pour tout $w \in W$, l'ensemble $s_w^{-1} N s_w$ ne dépend que de w; nous le noterons N_w.

3.6. LEMME. *Soient* $N'_w = s_w(N_w \cap N^-)\, s_w^{-1}$, $N''_w = s_w(N_w \cap N)\, s_w^{-1}$. *Le produit définit une bijection de* $N'_w \times N''_w$ *sur* N.

En effet, d'après 3.5 (i) :

$$N_w = \prod_{1 \leqslant i \leqslant n-1} \Big(\prod_{i+1 \leqslant j \leqslant n} N_{w^{-1}(i),\, w^{-1}(j)} \Big).$$

Mais d'après (ii), on peut aussi écrire :

$$N_w = \prod_{\substack{(i,j) \in L \\ i > j}} N_{(ij)} \cdot \prod_{\substack{(i,j) \in L \\ i > j}} N_{(ij)},$$

L désignant l'ensemble des couples $(w^{-1}(i), w^{-1}(j))$, $(1 \leqslant i < j \leqslant n)$.
Puisque $N \cap N^- = \{1\}$, on a $N_w = (N_w \cap N^-)\,(N_w \cap N)$ et tout élément de N_w s'écrit de manière unique comme produit d'un élément de N^- et de N.
Le lemme en résulte aussitôt.

3.7. PROPOSITION. *Pour tout* w, $G_w = N.s_w.B = N'_w.s_w.B$. *La décomposition d'un élément de* G_w *sous la forme* $x.s_w.y$ $(x \in N'_w,\ y \in B)$ *est unique.*

On a $N'_w.s_w.B \subset N.s_w.B$. En sens inverse $N.s_w.B = N'_w.N''_w.s_w.B$. Mais $N''_w.s_w \subset s_w N$, par conséquent $N.s_w.B \subset N'_w.s_w.N.B \subset N'_w.s_w.B$. La première assertion est donc démontrée.
Si $xs_w y = x' s_w y'$ $(x, x' \in N'_w,\ y, y' \in B)$, on a encore $s_w^{-1}.x.s_w.y = s_w^{-1}.x'.s_w y'$. Comme y et y' sont dans B, $s_w^{-1}.x.s_w$ et $s_w^{-1}.x'.s_w$ dans N^-, la deuxième assertion résulte de 3.4.
En définitive, nous avons obtenu une partition de G en ensembles $G_w = N'_w.s_w.D.N$.
Si $g \in G_w$, il s'écrit de manière unique :

$$g = u_g.s_w.t_g.v_g$$

où $u_g \in N'_w$, $t_g \in D$, $v_g \in N$. Seul l'élément t_g dépend du choix de s_w; u_g et v_g ne dépendent que de g. C'est la décomposition de Bruhat.
Dans le reste de ce paragraphe, nous supposons $k = \mathbf{R}$. Alors $D = (D \cap K).A$ et $N(D) = (K \cap N(D)).A$.

3.8. PROPOSITION. *Supposons choisis les* s_w *dans* K. *Soit* $g \in G_w$. *Écrivons :*

$$g = u_g.s_w.t_g.v_g \quad (u_g \in N'_w,\ t_g \in D,\ v_g \in N).$$

Alors $a_g = a(s_w^{-1} u_g s_w)\, a(t_g)$.

On peut écrire :

$$g = u_g . s_w . t_g . v_g = s_w . s_w^{-1} . u_g . s_w . t_g . v_g .$$

Posons $c = s_w^{-1} . u_g . s_w$. Il vient :

$$g = s_w . k_c . a_c . n_c . t_g . v_g = s_w . k_c . a_c . t_g . t_g^{-1} . n_c . t_g . v_g .$$

Or $s_w . k_c \in \mathrm{K}$, $v_g \in \mathrm{N}$, $t_g^{-1} . n_c . t_g \in \mathrm{N}$.
On a donc :

$$a_g = a_c\, a(t_g).$$

Signalons pour terminer une conséquence facile de 1.4.

3.9. LEMME. *Pour qu'un ensemble* $\omega \subset \mathrm{N}^-$ *soit relativement compact dans* N^- *il faut et il suffit que* $a(\omega)$ *soit relativement compact dans* A.

La condition est évidemment nécessaire.
Inversement si elle est satisfaite, l'égalité :

$$x . n_x^{-1} = k_x a_x \qquad (x \in \mathrm{N}^-),$$

montre que $x . n_x^{-1}$ parcourt un ensemble relativement compact dans G. Mais le produit définit un homéomorphisme de $\mathrm{N}^- \times \mathrm{N}$ sur un sous-espace fermé de G (1.4). Donc, ω est lui-même relativement compact dans N^-.

§ 4. La propriété de Siegel dans $\mathbf{GL}_n$

Le but de ce paragraphe est la démonstration d'un théorème de Siegel qui affirme notamment que si $b \in \mathbf{GL}(n, \mathbf{Q})$ et $\mathfrak{S}$ est un ensemble de Siegel de $\mathbf{GL}(n, \mathbf{R})$, alors l'ensemble des $\gamma \in \mathbf{GL}(n, \mathbf{Z})$ tels que $\mathfrak{S}\gamma \cap \mathfrak{S}b \neq \emptyset$ est fini (cf. 4.6).
Nous le déduirons ici d'un théorème de Harish-Chandra.

4.1. Nous démontrerons tout d'abord quelques propriétés des fonctions Φ_i introduites au § 1. Rappelons que :

$$\Phi_i(g) = \|g(e_1 \wedge e_2 \wedge \ldots \wedge e_i)\| \qquad (g \in \mathrm{G};\ i = 1, \ldots, n)$$

et

$$\Lambda_i(b) = b_{11} \ldots b_{ii} \qquad (b \in \mathrm{B} = \mathrm{DN})$$

d'où :

$$\Phi_i(g) = \Phi_i(a_g) = \Lambda_i(a_g) = a_{11} a_{22} \ldots a_{ii}$$
$$\Phi_i(gb) = \Phi_i(g)\, \Phi_i(b) = \Phi_i(g)\, |\Lambda_i(b)| \qquad (g \in \mathrm{G};\ b \in \mathrm{B}).$$

En particulier, cela montre qu'un sous-ensemble $\mathrm{C} \subset \mathrm{A}$ est relativement compact si, et seulement si, il existe des constantes $\alpha, \beta > 0$ telles que :

$$(1) \qquad \alpha \leqslant \Phi_i(c) \leqslant \beta \qquad (c \in \mathrm{C};\ i = 1, \ldots, n).$$

Enfin, si l'on utilise la décomposition de Bruhat :

$$g = k_g . a_g . n_g = u_g . s_w . t_g . v_g$$

on a (3.8) :

$$a_g = a(s_w^{-1} u_g s_w) . a(t_g)$$

donc

$$\Phi_i(g) = \Phi_i(a_g) = \Phi_i(s_w^{-1} . u_g . s_w)\, \Phi_i(t_g). \tag{2}$$

4.2. LEMME. (i) *Pour tout* $n \in \mathrm{N}^-$, *on a* $\Phi_i(n) \geqslant 1$ $(i = 1, 2, \ldots, n)$; (ii) *Pour tout* $g \in \mathrm{G}$, *on a* $\Phi_i(a_g) \geqslant \Phi_i(t_g)$.

En effet $n(e_1 \wedge e_2 \wedge \ldots \wedge e_i) = e_1 \wedge e_2 \wedge \ldots \wedge e_i + a$ où a est une combinaison linéaire des éléments de la base canonique de $\wedge^i \mathbf{R}^n$ autres que $e_1 \wedge e_2 \wedge \ldots \wedge e_i$, donc :

$$\Phi_i(n) = ||n(e_1 \wedge e_2 \wedge \ldots \wedge e_i)|| \geqslant 1.$$

(ii) résulte alors de (2) et du fait que $s_w^{-1} . u_g . s_w$ est dans N^-.

4.3. LEMME. *Pour tout indice* $i (1 \leqslant i \leqslant n)$, *il existe une constante* $d_i > 0$ *telle que* $||g(v)|| \geqslant d_i . ||v||. \Phi_i(g)$ *lorsque* g *parcourt* $\mathfrak{S}$ *et* v *parcourt* $\wedge^i(\mathbf{R}^n)$.

On peut se borner à démontrer la relation pour $||v|| = 1$. Écrivons $\mathrm{G} = \mathrm{KAN}$ et $\mathfrak{S} = \mathrm{KA}_t\omega$, où ω est donc un ensemble relativement compact dans N et A_t l'ensemble des matrices diagonales à coefficients > 0 vérifiant $a_{ii} \leqslant t . a_{i+1,i+1}$.
Soient $v \in \wedge^i(\mathbf{R}^n)$ de norme 1 et $g \in \mathrm{G}$:

$$||g(v)|| = ||k_g . a_g . n_g(v)|| = ||a_g . n_g(v)||.$$

On peut écrire :

$$n_g(v) = \sum \beta_j(n_g) f_j$$

où les f_j parcourent la base canonique de $\wedge^i(\mathbf{R}^n)$.
D'autre part, si $f_j = e_{l_1} \wedge e_{l_2} \wedge \ldots \wedge e_{l_i}$ $(l_1 < l_2 < \ldots < l_i)$ alors :

$$a_g(f_j) = a_{l_1 l_1} . a_{l_2 l_2} \cdot \ldots \cdot a_{l_i l_i} . f_j = \Lambda_i(a_g) \frac{a_{l_1 l_1}}{a_{11}} \cdot \ldots \cdot \frac{a_{l_i l_i}}{a_{ii}} f_j$$

$$a_g(f_j) = \Lambda_i(a_g)\, \alpha_1^{m_{1,j}} \alpha_2^{m_{2,j}} \cdot \ldots \cdot \alpha_{n-1}^{m_{n-1,j}} . f_j$$

où $\alpha_i = a_i / a_{i+1}$ $(i = 1, 2, \ldots, n-1)$ et les $m_{i,j}$ $(i = 1, \ldots, n-1)$ sont des entiers négatifs.
En combinant ces deux résultats, on obtient :

$$a_g . n_g(v) = \Lambda_i(a_g) . \sum \beta_j(n_g)\, \alpha_1^{m_{1,j}} \cdot \ldots \cdot \alpha_{m-1}^{m_{n-1,j}} . f_j.$$

Si maintenant g est dans $\mathfrak{S}$, on a $0 < \alpha_i \leqslant t$ par hypothèse. Il existe donc une constante $\delta > 0$, telle que :

$$||a_g . n_g(v)||^2 \geqslant \delta . \Lambda_i(a_g)^2 . (\sum \beta_j(n_g)^2).$$

Mais $||v|| = 1$ et n_g parcourt un compact. On a donc :

$$||n_g(v)|| \geqslant \delta' > 0$$

d'où l'existence d'une constante $d > 0$ telle que :

$$||a_g . n_g(v)|| \geqslant d . \Lambda_i(a_g), \qquad (g \in \mathfrak{S},\ ||v|| = 1),$$

ce qui peut s'écrire :

$$||g(v)|| \geqslant d.\Phi_i(g).$$

Le lemme est donc démontré.

4.4. THÉORÈME (Harish-Chandra). *Soient* $\mathfrak{S} \subset \mathbf{GL}(n, \mathbf{R})$ *un domaine de Siegel,* s_w *un choix de représentants dans* $N(D) \cap K$ *des éléments de* W, *et* M *un sous-ensemble de* G *vérifiant :*

(i) $M = M^{-1}$;

(ii) *Pour tout* i $(1 \leqslant i \leqslant n)$, *il existe une constante* $C_i > 0$ *telle que* $\Phi_i(t_m) \geqslant C_i$ *pour tout* $m \in M$ (t_m *étant relatif aux* s_w, cf. (3.7)).

Alors l'ensemble $M_{\mathfrak{S}}$ *des* $m \in M$ *tels que* $\mathfrak{S}m$ *rencontre* $\mathfrak{S}$ *est relativement compact dans* G.

Prouvons d'abord que lorsque g parcourt $M_{\mathfrak{S}}$, son composant a_g dans la décomposition d'Iwasawa $(g = k_g.a_g.n_g)$ et ses composants u_g et t_g dans celle de Bruhat $(g = u_g.s_w.t_g.v_g)$ décrivent des ensembles relativement compacts.
Soient $m \in M_{\mathfrak{S}}$, et $x, y \in \mathfrak{S}$ tels que $x = m.y$. Appliquons (4.3) successivement au vecteur v et au vecteur $m(e_1 \wedge e_2 \wedge \ldots \wedge e_i)$. Nous obtenons :

$$||(xm).v|| \geqslant d.||v||.\Phi_i(xm),$$

puis :

$$\Phi_i(xm) \geqslant d.\Phi_i(x).\Phi_i(m),$$

soit :

$$||(xm).v|| \geqslant d^2.||v||.\Phi_i(m).\Phi_i(x).$$

En particulier, prenons $v = (m^{-1}).(e_1 \wedge e_2 \wedge \ldots \wedge e_i)$, il vient :

$$\Phi_i(x) \geqslant d^2.\Phi_i(m^{-1}).\Phi_i(m).\Phi_i(x),$$

d'où

$$\Phi_i(m).\Phi_i(m^{-1}) \leqslant d^{-2}. \tag{1}$$

Par ailleurs, d'après 4.2 (ii) et l'hypothèse (ii) :

$$\Phi_i(m) = \Phi_i(a_m) \geqslant \Phi_i(t_m) \geqslant C_i > 0. \tag{2}$$

Comme $M = M^{-1}$, (1) et (2) montrent que $\Phi_i(m)$ et $\Phi_i(t_m)$ sont aussi bornés *supérieurement* sur $M_{\mathfrak{S}}$. Il existe donc des constantes $\alpha, \beta > 0$ telles que :

$$\alpha \leqslant \Phi_i(a_m) \leqslant \beta, \qquad \alpha \leqslant \Phi_i(t_m) \leqslant \beta \qquad (m \in M_{\mathfrak{S}}).$$

Cela prouve que $a(M_{\mathfrak{S}})$ et $t(M_{\mathfrak{S}})$ sont relativement compacts (cf. 4.1 (1)). D'autre part (3.8) :

$$a_m = a(s_w^{-1}.u_m.s_w)\, a(t_m)$$

donc $a(s_w^{-1}.u_m.s_w)$ reste dans un ensemble relativement compact lorsque m varie dans $M_{\mathfrak{S}} \cap G_w$. Comme $s_w^{-1}.u_m.s_w \in N^-$, il en est alors de même (3.9) de $s_w^{-1}u_m s_w$, ce qui démontre notre assertion.
Nous pouvons maintenant démontrer le théorème par récurrence sur la dimension n. Il est immédiat pour $n = 1$. Supposons donc $n > 1$ et le théorème vrai pour $n - 1$. Tout revient à montrer que la trace de $M_{\mathfrak{S}}$ sur chacun des ensembles G_w (qui

sont en nombre fini) est relativement compact. Fixons $w \in W$. Nous distinguons deux cas :

(i) *L'élément s_w n'est dans aucun des sous-groupes paraboliques* P_λ $(\lambda = 1, 2, \ldots, n-1)$.

Un ensemble de Siegel est invariant par translation à gauche par une matrice $c.I$ $(c > 0)$; donc, si m vérifie une relation $x.m = y$ $(x, y \in \mathfrak{S})$, on voit, en multipliant par $|\det x|^{-1}.I$, qu'il vérifie aussi une égalité de ce type avec $|\det x| = 1$. Par suite, pour établir (i), il suffit de prouver que l'ensemble X des $x \in \mathfrak{S}$ tels que $|\det x| = 1$ et $x.m \in \mathfrak{S}$ pour m convenable dans $M_{\mathfrak{S}} \cap G_w$, et l'ensemble Y des $y \in \mathfrak{S}$ tels que $y = x.m$ pour $x \in X$ et $m \in M_{\mathfrak{S}} \cap G_w$, sont tous deux relativement compacts. Soient donc $x \in X$, $y \in Y$, $m \in M_{\mathfrak{S}} \cap G_w$ tels que $xm = y$. On a :

$$k_y.a_y.n_y = k_x.a_x.n_x.u_m.s_w.t_m.v_m = k_x.s_w.k_c.a_c.n_c.(s_w^{-1}.a_x.s_w).t_m.v_m$$

où

$$c = s_w^{-1}.a_x.n_x.u_m.a_x^{-1}.s_w.$$

Comme $k_x.s_w.k_c$ est un élément de K, on a (3.8) :

$$a_y = a_c.(s_w^{-1}.a_x.s_w).a(t_m).$$

D'après ce qu'on vient de voir, u_m décrit un ensemble relativement compact. Comme n_x est dans un compact fixe $a_x n_x u_m a_x^{-1}$ reste borné vu la propriété fondamentale (1.3) des ensembles de Siegel. Il en est de même de c et de a_c. La démonstration sera achevée si nous prouvons que a_x décrit un ensemble relativement compact, car $a(t_m)$ restant borné, comme on l'a vu, il en sera alors de même de a_y.
Comme $\det a_x = 1$, cela revient à prouver que :

$$\alpha_\lambda(a_x) \geqslant c_\lambda > 0 \qquad (\lambda = 1, 2, \ldots, n-1).$$

Comme les coefficients de a_c et $a(t_m)$ sont bornés supérieurement et inférieurement et que $\alpha_i(a_y)$ est borné supérieurement, on voit que pour $i = 1, 2, \ldots, n$, les $w(\alpha_i)$ (a_x) restent bornés supérieurement.
Pour λ donné $(1 \leqslant \lambda \leqslant n-1)$, il existe (3.2) au moins un indice i, $(1 \leqslant i \leqslant n)$ tel que :

$$w(\alpha_i)\ (a_x) = \prod_{1 \leqslant j \leqslant n-1} \alpha_j(a_x)^{n_{ij}} \quad \text{avec} \quad n_{i\lambda} < 0.$$

Mais les $\alpha_j(a_x)$ sont bornés supérieurement. On voit que $\alpha_\lambda(a_x)$ ne peut être arbitrairement petit, ce qu'il fallait démontrer.

(ii) *L'élément s_w est dans l'un des groupes* P_λ, $(1 \leqslant \lambda \leqslant n-1)$.

Si $s_w \in P_\lambda$, on vérifie aussitôt que $G_w \subset P_\lambda$. Tout revient donc à prouver l'assertion suivante :

Pour tout λ $(1 \leqslant \lambda \leqslant n-1)$, $M_{\mathfrak{S}} \cap P_\lambda$ *est relativement compact.*

Remarquons d'abord que si x et y sont dans $\mathfrak{S}$, et $m \in M_{\mathfrak{S}} \cap P_\lambda$ tel que $xm = y$, on peut supposer, quitte à modifier x, que $k_x = e$, donc $x \in A.N \subset P_\lambda$. On a alors $y \in P_\lambda$, ce qui montre que $M_{\mathfrak{S}} \cap P_\lambda$ est exactement l'ensemble des $m \in M$ tels que $\mathfrak{S} \cap P_\lambda$ rencontre $(\mathfrak{S} \cap P_\lambda)\, m$.

Le groupe P_λ est le produit semi-direct $P_\lambda = S.R$ où S est le produit direct :

$$S = \mathbf{GL}(\lambda, \mathbf{R}) \times \mathbf{GL}(n - \lambda, \mathbf{R})$$

et R le sous-groupe distingué unipotent des matrices de la forme :

$$\begin{pmatrix} I_\lambda & * \\ 0 & I_{n-\lambda} \end{pmatrix}.$$

Soient Π, Π_0, Π_1, Π_2 les projections de P_λ sur S, R, $\mathbf{GL}(\lambda, \mathbf{R})$, $\mathbf{GL}(n - \lambda, \mathbf{R})$ respectivement. Il s'agit de prouver que $\Pi_i(M_{\mathfrak{S}} \cap P_\lambda)$ est relativement compact $(i = 0, 1, 2)$. On a $\mathbf{O}(n) \cap P_\lambda = \mathbf{O}(\lambda).\mathbf{O}(n - \lambda)$, (produit direct). Il en résulte que Π_1 (resp. Π_2) transforme la décomposition d'Iwasawa d'un élément g de P_λ en la décomposition d'Iwasawa de $\Pi_1(g)$ (resp. $\Pi_2(g)$) dans le groupe $\mathbf{GL}(\lambda, \mathbf{R})$ (resp. $\mathbf{GL}(n - \lambda, \mathbf{R})$). De manière précise, si $x = k_x.a_x.n_x$ est dans P_λ, on a :

$$\Pi(x) = k_x.a_x.\Pi(n_x), \qquad \Pi_0(x) = \Pi_0(n_x)$$

et $\Pi_1(k_x)$, $\Pi_1(a_x)$, $\Pi_1(n_x)$ (resp. $\Pi_2(k_x)$, $\Pi_2(a_x)$, $\Pi_2(n_x)$)

sont les composants de $\Pi_1(x)$ (resp. $\Pi_2(x)$) dans la décomposition d'Iwasawa. En particulier $\Pi_i(\mathfrak{S}) \subset \mathfrak{S}_i$ $(i = 1, 2)$ où $\mathfrak{S}_i$ est un domaine de Siegel. Si l'on pose $M_i = \Pi_i(M \cap P_\lambda)$, on voit que $\Pi_i(M_{\mathfrak{S}} \cap P_\lambda) \subset M_{\mathfrak{S}_i}$.

Il est clair que M_i satisfait à la première hypothèse du théorème.

Il est immédiat que Π_1 (resp. Π_2) transforme la décomposition de Bruhat d'un élément g de P_λ en la décomposition de Bruhat de $\Pi_1(g)$ (resp. $\Pi_2(g)$) dans $\mathbf{GL}(\lambda, \mathbf{R})$ (resp. $\mathbf{GL}(n - \lambda, \mathbf{R})$); on déduit aussitôt que M_i satisfait aussi à la seconde hypothèse. Par l'hypothèse de récurrence, $(M_i)_{\mathfrak{S}_i}$ est relativement compact $(i = 1, 2)$.

Il reste à prouver que $\Pi_0(M_{\mathfrak{S}} \cap P_\lambda)$ est relativement compact. Or si $m \in M_{\mathfrak{S}} \cap P_\lambda$, l existe x et y dans $P_\lambda \cap \mathfrak{S}$ tels que $x.m = y$, ce qui peut s'écrire :

$$k_x.a_x.n_x.m = k_y.a_y.n_y$$

d'où :

$$k_x.a_x.\Pi(n_x).\Pi_0(n_x).\Pi(m).\Pi_0(m) = k_y.a_y.\Pi(n_y).\Pi_0(n_y).$$

Le premier membre s'écrit aussi :

$$k_x.a_x.\Pi(n_x).\Pi(m).(\Pi(m)^{-1}.\Pi_0(n_x).\Pi(m)).\Pi_0(m).$$

Comme $k_x.a_x.\Pi(n_x).\Pi(m)$ est dans S et $(\Pi(m)^{-1}.\Pi_0(n_x).\Pi(m)).\Pi_0(m)$ dans R. on a :

$$\Pi_0(n_y) = \Pi(m)^{-1}.\Pi_0(n_x).\Pi(m).\Pi_0(m).$$

$\Pi_0(n_x)$ et $\Pi_0(n_y)$ sont bornés puisque x et y sont dans un ensemble de Siegel. On vient de prouver que $\Pi(m)$ est borné. Il en est donc de même de $\Pi_0(m)$ et le théorème est démontré.

4.5. COROLLAIRE. *Soient $\mathfrak{S}'$ un domaine de Siegel dans l'espace des matrices symétriques positives non dégénérées et M un sous-ensemble de G vérifiant les hypothèses du théorème. Alors l'ensemble des $m \in M$ tels que $\mathfrak{S}'[m]$ rencontre $\mathfrak{S}'$ est relativement compact.*

4.6. THÉORÈME (Siegel). *Soient* $\mathfrak{S}$ *un domaine de Siegel dans* $\mathbf{GL}(n, \mathbf{R})$, M *un ensemble de matrices inversibles à coefficients entiers dont les déterminants vérifient* $|\det m| \leqslant c$, $m \in \mathrm{M}$. *Alors* $\mathrm{M}_{\mathfrak{S}}$ *est fini.*

Comme $\mathbf{M}(n, \mathbf{Z})$ est fermé et discret dans $\mathbf{M}(n, \mathbf{C})$, l'ensemble $\mathrm{M}_{\mathfrak{S}}$ est lui-même fermé et discret. Il suffit donc de montrer que $\mathrm{L} = \mathrm{M} \cup \mathrm{M}^{-1}$ satisfait à l'hypothèse (ii) du théorème 4.4. Cela résulte aussitôt du lemme suivant :

4.7. LEMME. *Soit* L *un sous-ensemble de* $\mathbf{GL}(n, \mathbf{Q})$ *dont les éléments ont des coefficients à dénominateurs bornés supérieurement en valeur absolue.*
Alors il existe une constante $c > 0$ *telle que* $\Phi_i(t_x) \geqslant c$ *pour tout* $x \in \mathrm{L}$ *et tout* $i = 1, 2, \ldots, n$.

Soit $x \in \mathrm{G}_w \cap \mathrm{L}$. Tout revient à prouver que les produits $|t_{11} \ldots t_{ii}|$ des coefficients diagonaux de t_x ont des dénominateurs bornés supérieurement.
Or $s_w^{-1}.x = c_x.t_x.v_x$ où $c_x = s_w^{-1}.u_x.s_w \in \mathrm{N}^-$. En particulier lorsque $x \in \mathrm{G}_w \cap \mathrm{L}$, les dénominateurs des coefficients de $c_x.t_x.v_x$ restent bornés supérieurement. Les éléments $\det((c_x.t_x.v_x)_{jk})_{1 \leqslant j,\, k \leqslant i} = t_{11} \ldots t_{ii}$ ont donc la même propriété.

4.8. COROLLAIRE. *Le groupe* $\Gamma = \mathbf{GL}(n, \mathbf{Z})$ *est de type fini et les sous-groupes finis de* $\mathbf{GL}(n, \mathbf{Z})$ *forment un nombre fini de classes de conjugaison pour les automorphismes intérieurs de* Γ.

On a $\mathfrak{H} = \mathfrak{S}'[\Gamma]$, où $\mathfrak{S}'$ est un domaine ouvert de Siegel convenable (cf. § 2). Il est alors immédiat que Γ est engendré par l'ensemble $\Gamma_{\mathfrak{S}'}$ des γ de Γ tels que $\mathfrak{S}'[\gamma]$ rencontre $\mathfrak{S}'$, et cet ensemble est fini d'après le théorème 4.5. Soit maintenant L un sous-groupe fini de Γ; il a un point fixe F dans $\mathfrak{H}$. On peut écrire $\mathrm{F} = c[\gamma]$, où c est dans $\mathfrak{S}'$ et γ dans Γ. Alors $\gamma.\mathrm{L}.\gamma^{-1} \subset \Gamma_{\mathfrak{S}'}$. La conclusion résulte donc de ce que $\Gamma_{\mathfrak{S}'}$ est fini.

4.9. Nous terminons ce paragraphe par une proposition de Harish-Chandra qui intervient dans la discussion de fonctions automorphes.
Par norme $||x||$ de $x \in \mathbf{R}^n$ on entend la norme euclidienne de x. Pour $g \in \mathbf{GL}(n, \mathbf{R})$, on appelle norme de g et on note $||g||$, la trace de ${}^t g.g$, autrement dit la somme des carrés des coefficients de g. On a donc :

$$||g|| = \sum_{1 \leqq i \leqq n} ||g.e_i||^2.$$

On voit facilement que si $c \in \mathbf{GL}(n, \mathbf{R})$, alors :

$$||g|| \asymp ||g.c|| \asymp ||c.g|| \qquad (g \in \mathbf{GL}(n, \mathbf{R})). \tag{1}$$

Cela entraîne que si H est un sous-groupe de $\mathbf{GL}(n, \mathbf{R})$ et H' un sous-groupe d'indice fini de H, alors,

$$\inf_{u \in \mathrm{H}} ||g.u|| \asymp \inf_{u \in \mathrm{H}'} ||g.u|| \qquad (g \in \mathbf{GL}(n, \mathbf{R})). \tag{2}$$

Par conséquent, si L est un sous-groupe de $\mathbf{GL}(n, \mathbf{R})$ commensurable à H, i.e. tel que $\mathrm{L} \cap \mathrm{H}$ soit d'indice fini dans L et H, on a :

$$\inf_{u \in \mathrm{L}} ||g.u|| \asymp \inf_{u \in \mathrm{H}} ||g.u|| \qquad (g \in \mathbf{GL}(n, \mathbf{R})).$$

4.10. PROPOSITION. *Soit* $\mathfrak{S}$ *un ensemble de Siegel de* $\mathbf{GL}(n, \mathbf{R})$, *et soit* $\Gamma = \mathbf{GL}(n, \mathbf{Z})$. *Alors :*

$$||g|| \asymp \operatorname*{Inf}_{u \in \Gamma} ||g.u|| \qquad (g \in \mathfrak{S}).$$

Évidemment le membre de gauche est plus grand que le membre de droite. Il suffit de montrer que $||g|| \prec \operatorname*{Inf}_{u \in \Gamma} ||g.u||$ $(g \in \mathfrak{S})$. Quitte à agrandir $\mathfrak{S}$, on peut, vu 2.7, supposer que $\mathfrak{S}$ contient l'ensemble $\mathfrak{M}$ des éléments M-réduits de $\mathbf{GL}(n, \mathbf{R})$, au sens de 2.8. Soit C l'ensemble des $c \in \mathbf{GL}(n, \mathbf{Z})$, tels que $\mathfrak{S}.c \cap \mathfrak{S} \neq \emptyset$. Il est fini d'après 4.6.

Vu (4.9), il existe des constantes $a, b > 0$, telles que :

$$a. \operatorname*{Inf}_{\gamma \in \Gamma} ||g.\gamma|| \leqq \operatorname*{Inf}_{\gamma \in \Gamma} ||g.c.\gamma|| \leqq b. \operatorname*{Inf}_{\gamma \in \Gamma} ||g.\gamma||, \qquad (g \in \mathbf{GL}(n, \mathbf{R});\ c \in \mathrm{C}),$$

et d'autre part, $||g|| \asymp ||g.c||$ $(g \in \mathbf{GL}(n, \mathbf{R}),\ c \in \mathrm{C})$.

Soit maintenant $g \in \mathfrak{S}$. Il existe $\gamma \in \Gamma$ tel que $g = g'.\gamma$ $(g' \in \mathfrak{M})$. Comme $\mathfrak{M} \subset \mathfrak{S}$, on a alors $\gamma \in \mathrm{C}$. Il résulte donc des deux relations précédentes que l'on est ramené à prouver :

$$||g|| \prec \operatorname*{Inf}_{\gamma \in \Gamma} ||g.\gamma|| \qquad (g \in \mathfrak{M}).$$

Désignons par F_g la forme quadratique de matrice ${}^t g.g$. On a les relations suivantes, où $m_n(\mathrm{F}_g)$ est le nombre introduit dans 2.6 :

$$||g.\gamma|| = \sum_{1 \leqq i \leqq n} ||g.\gamma(e_i)||^2 = \sum_i \mathrm{F}_g(\gamma.e_i) \geqq m_n(\mathrm{F}_g[\gamma]) = m_n(\mathrm{F}_g),$$

la dernière égalité résultant de la définition de $m_n(\mathrm{F})$. D'après 2.6, il existe une constante $d > 0$, *indépendante de* $g \in \mathfrak{M}$, telle que :

$$m_n(\mathrm{F}_g) \geqq d.\mathrm{F}_g(e_n) = d.||g.e_n||^2 \qquad (g \in \mathfrak{M})$$

d'où, puisque les $||g.e_i||$ forment une suite croissante :

$$||g.\gamma|| \geqq \frac{d}{n} . \sum_i ||g.e_i||^2 = \frac{d}{n} . ||g|| \qquad (g \in \mathfrak{M}).$$

Note bibliographique

Le théorème 4.6 est démontré dans [29]. Il semble du reste que Hermite savait que sa théorie de la réduction fournissait des ensembles de réduites qui ne rencontrent qu'un nombre fini de leurs translatés par Γ. C'est tout au moins ce qui ressort d'une remarque [13, p. 230] qu'il fait à propos de la réduction des formes indéfinies, dont il déduit notamment que le groupe des unités d'une telle forme est à engendrement fini.

Le théorème 4.4 est en fait un cas particulier d'un théorème (non publié) de Harish-Chandra, qui sera énoncé et démontré au § 15. La démonstration donnée ici est modelée sur celle du cas général. 4.10 équivaut essentiellement au Satz 4, p. 34, de C. L. Siegel, *Zur Reduktionstheorie quadratischer Formen*, Publ. M. S. Japan 5, 1959.

§ 5. Réduction des formes quadratiques indéfinies

5.1. Avant de traiter la réduction des formes quadratiques indéfinies, nous allons étudier la notion de majorante de Hermite d'une forme quadratique, qui permet de faire le lien avec la réduction des formes quadratiques positives du § 2.
V désigne un espace vectoriel réel de groupe linéaire G et $\mathfrak{H}$ l'ensemble des formes quadratiques positives non dégénérées sur V ; $\mathfrak{H}$ est muni d'un ordre partiel, défini par $F \leqslant F'$ si, quel que soit $v \in V$, on a $F(v) \leqslant F'(v)$. G opère à droite sur l'ensemble des formes quadratiques par :

$$F \mapsto F[X], \qquad \text{où} \qquad F[X]\,(v) = F[Xv],$$

ce qui se traduit dans une base de V par :

$$F[X]_0 = {}^tX_0 . F_0 . X_0,$$

si l'on note X_0 (resp. F_0), la matrice d'un élément X de G (resp. d'une forme quadratique F) par rapport à la base choisie. O(F) désigne enfin le groupe d'isotropie de la forme quadratique F :

$$O(F) = \{X \in G \mid F[X] = F\}.$$

Définition. 1) $C \in \mathfrak{H}$ majore la forme quadratique F si $|F(v)| \leqslant C(v)$, pour tout $v \in V$;

2) $C \in \mathfrak{H}$ est une majorante d'Hermite (ou minimale) de F, si elle est minimale dans l'ensemble ordonné des majorantes de F.

L'ensemble des majorantes minimales de F est noté $\mathfrak{H}(F)$: si $F \in \mathfrak{H}$ (resp. $-F \in \mathfrak{H}$), cet ensemble est réduit à F (resp. $-F$). Comme $X \in G$ transforme l'ensemble des majorantes de F en celui des majorantes de F[X], on a :

$$\mathfrak{H}(F[X]) = \mathfrak{H}(F)[X],$$

et par suite O(F) opère dans $\mathfrak{H}(F)$: nous allons voir que $\mathfrak{H}(F)$ est ainsi un espace homogène topologique isomorphe à celui des classes à droite de O(F) suivant un sous-groupe compact maximal.

5.2. PROPOSITION. *Si* $C \in \mathfrak{H}$ *et si* F *est une forme quadratique non dégénérée de signature* (a, b), *il y a équivalence entre les assertions suivantes :*

(i) $C \in \mathfrak{H}(F)$.
(ii) *Il existe une décomposition de* V *en somme* $V_1 \oplus V_2$, *orthogonale pour* F *et* C, *telle que* $F = C$ *sur* V_1 *et* $F = -C$ *sur* V_2.
(iii) *Il existe une base de* V *par rapport à laquelle* $F_0 = I_{a,b}$ *et* $C_0 = I$.
(iv) *Dans toute base de* V, *on a* $(F_0 . C_0^{-1})^2 = I$.

($I_{a,b}$ désigne la matrice diagonale dont les a premiers coefficients diagonaux sont égaux à 1 et les b derniers à -1.)

D'après les hypothèses, on peut trouver une base de V dans laquelle :

$$F = \sum_{i=1}^{a} x_i^2 - \sum_{i=a+1}^{a+b} x_i^2,$$

$$C = \sum_{i=1}^{a+b} \alpha_i x_i^2, \qquad (\alpha_i > 0;\ 1 \leqslant i \leqslant a+b),$$

C majore alors F si, et seulement si, $\alpha_i \geqslant 1$, $(1 \leqslant i \leqslant a+b)$. Par suite :

$$C \in \mathfrak{H}(F) \Leftrightarrow \alpha_i = 1 \qquad (1 \leqslant i \leqslant a+b).$$

Les équivalences (i) $\Leftrightarrow$ (ii) $\Leftrightarrow$ (iii) en résultent aussitôt. Toujours dans cette base, la relation $(F_0 . C_0^{-1})^2 = I$ s'écrit $\alpha_i^2 = 1$ pour tout i et par suite (iv) $\Rightarrow$ (iii). Enfin un calcul matriciel immédiat montre que si la relation de (iv) est vérifiée dans une base de V, elle l'est également dans toute autre base, ce qui prouve l'implication (iii) $\Rightarrow$ (iv).

5.3. COROLLAIRE. *Sous les hypothèses de la proposition, l'application :*

$$C \mapsto V(C)$$

où $C \in \mathfrak{H}(F)$ *et où* $V(C)$ *désigne l'unique sous-espace de dimension a de* V *sur lequel* $F = C$ *est une bijection de* $\mathfrak{H}(F)$ *sur l'ensemble des sous-espaces de dimension a sur lesquels* F *est positive non dégénérée.*

L'existence d'un espace $V(C)$ au moins vient de (iii), et son unicité de ce qu'il est le sous-espace propre pour la valeur propre 1 de l'opérateur auto-adjoint associé à F par C. Enfin, si V_1 est un sous-espace de dimension a sur lequel F est positive non dégénérée, son orthogonal V_2 pour F est un supplémentaire de V_1 et l'on a $V_1 = V(C)$ avec $C = F$ sur V_1 et $C = -F$ sur V_2.

5.4. PROPOSITION. $O(F)$ *opère transitivement sur* $\mathfrak{H}(F)$. *Le groupe d'isotropie d'un point* C *de* $\mathfrak{H}(F)$ *est un sous-groupe compact maximal* $K \simeq \mathbf{O}(a) \times \mathbf{O}(b)$, *et* $\mathfrak{H}(F)$ *est homéomorphe à* $K\backslash O(F)$.

Le groupe $O(F)$ est transitif, car si C et C′ appartiennent à $\mathfrak{H}(F)$, les deux décompositions de V associées par (ii) sont orthogonales pour F et il existe un élément de $O(F)$ qui transforme l'une en l'autre, donc C en C′. Le groupe d'isotropie dans $O(F)$ de $C \in \mathfrak{H}(F)$ est $O(F) \cap O(C)$, qui s'identifie dans la base de (iii) à $O(I_{a,b}) \cap \mathbf{O}(n)$, égal, comme le montre un calcul immédiat, au sous-groupe compact $\mathbf{O}(a) \times \mathbf{O}(b)$ de $\mathbf{O}(n)$. Comme un sous-groupe compact de $O(F)$ laisse un point $D \in \mathfrak{H}$ fixe [8, Chap. VII, § 3, n° 1, Prop. 1], il suffit, pour prouver que K est maximal, de vérifier que l'inclusion $K \subset O(F) \cap O(D)$ implique l'égalité; or, on voit aisément que l'algèbre de Lie de $O(I_{a,b}) \cap O(\mathrm{diag}\{\alpha_i\})$, où $\alpha_i > 0$ pour tout i, est contenue dans celle de $\mathbf{O}(a) \times \mathbf{O}(b)$. On sait enfin que $\mathbf{GL}(n, \mathbf{R})$ opère proprement à droite dans $\mathfrak{H}$, il en est donc de même de $O(F)$, dont une orbite est précisément $\mathfrak{H}(F)$: il en résulte que $\mathfrak{H}(F)$ est homéomorphe à $K\backslash O(F)$.

5.5. Soient F une forme quadratique rationnelle indéfinie sur $\mathbf{R}^n$, non dégénérée, (a, b) la signature de F, G le groupe de Lie réel $O(F)$ et $\Gamma = G \cap \mathbf{GL}(n, \mathbf{Z})$. Les

éléments de Γ sont appelés les « unités » de F. Ce sont donc des éléments de $O(F)$ qui laissent le réseau $\mathbf{Z}^n$ invariant (on pourrait naturellement substituer à $\mathbf{R}^n$ les points réels d'un espace vectoriel V sur $\mathbf{Q}$ et à $\mathbf{Z}^n$ un réseau L de ce dernier). G opérant à droite proprement dans $\mathfrak{H}(F)$, il en est de même du sous-groupe fermé Γ et le problème de la réduction consiste à trouver un ensemble intéressant de représentants des orbites de Γ.
On choisit pour toute la suite un ensemble de Siegel $\mathfrak{S}'$ de $\mathfrak{H}$ contenant $\mathfrak{S}'_{4/3,\,1/2}$, si bien que $\mathfrak{H}$ est égal à $\mathfrak{S}'.[\mathbf{GL}(n, \mathbf{Z})]$, vu (2.2).

Définition. F est réduite (ou plus précisément $\mathfrak{S}'$-réduite) si :

$$\mathfrak{H}(F) \cap \mathfrak{S}' \neq \emptyset.$$

5.6. DÉFINITION. $\Omega \subset \mathfrak{H}(F)$ est un ensemble fondamental pour Γ s'il vérifie les conditions :

(F 1) $\quad \Omega[\Gamma] = \mathfrak{H}(F)$;

(F 2) $\quad \forall b \in O(F)_{\mathbf{Q}}$, $\{\gamma \in \Gamma \mid \Omega\,[b] \cap \Omega[\gamma] \neq \emptyset\}$ est fini : c'est la propriété de Siegel.

Le lemme de finitude suivant, cas particulier d'un résultat qui sera démontré au § 6, et le théorème de Siegel 4.6, vont permettre de prouver l'existence d'un ensemble fondamental.

5.7. LEMME. *L'ensemble des formes quadratiques entières réduites de déterminant non nul donné est fini.*

5.8. THÉORÈME. *Il existe* $s_1, \ldots, s_m \in \mathbf{GL}(n, \mathbf{Z})$ *tels que :*

$$\Omega = \Big(\bigcup_{i=1}^{m} \mathfrak{S}'[s_i]\Big) \cap \mathfrak{H}(F)$$

soit un ensemble fondamental.

En vertu de l'égalité $\mathfrak{H}(qF) = |q|.\mathfrak{H}(F)$, si $q \in \mathbf{Q}$ et si Ω est fondamental relativement à F, $|q|\,\Omega$ l'est relativement à qF; comme de plus $\mathfrak{S}'$ est stable par homothétie positive, il suffit de prouver le théorème pour F entière.
Or, si F est entière, toutes les formes de l'orbite de F par $\mathbf{GL}(n, \mathbf{Z})$ ayant même déterminant, il n'y a parmi elles qu'un nombre fini de formes réduites, disons $F[s_1^{-1}], \ldots, F[s_m^{-1}]$, d'après le lemme de finitude. Nous allons montrer que :

$$\Omega = \Big(\bigcup_{i=1}^{m} \mathfrak{S}'[s_i]\Big) \cap \mathfrak{H}(F)$$

satisfait à (F 1) et (F 2).

(F 1) : Soit $C \in \mathfrak{H}(F)$; d'après la réduction des formes définies (§ 2), il existe $s \in \mathbf{GL}(n, \mathbf{Z})$ tel que $C[s] \in \mathfrak{S}'$. Mais alors $\mathfrak{H}(F[s]) = \mathfrak{H}(F)[s]$ rencontre $\mathfrak{S}'$ en $C[s]$, ce qui signifie que $F[s]$ est réduite, donc égale à $F[s_i^{-1}]$ pour un certain i. Ainsi $ss_i \in \Gamma$ et $C[ss_i] \in \mathfrak{S}'[s_i] \cap \mathfrak{H}(F)$: l'orbite de C rencontre bien Ω.

(F 2) : Étant donné $b \in O(F)_{\mathbf{Q}}$, supposons $\gamma \in \Gamma$ tel que $\Omega[b] \cap \Omega[\gamma] \neq \emptyset$. D'après la définition de Ω, il existe deux indices i et j tels que $\mathfrak{S}'[s_i\, b] \cap \mathfrak{S}'[s_j \gamma] \neq \emptyset$.

Or la propriété de Siegel est connue pour $\mathfrak{S}'$ (cf. § 4), ce qui permet de conclure en vertu de la finitude de l'ensemble $\{s_i\}$.
Ajoutons qu'on peut prouver la finitude du volume d'un tel ensemble fondamental. Nous allons montrer comment se traduit la notion de forme réduite, lorsqu'on revient au groupe $\mathbf{GL}(n, \mathbf{R})$ ou $\mathbf{SL}(n, \mathbf{R})$. Les ensembles de Siegel associés à $\mathfrak{S}'$ sont : $\mathfrak{S}$ dans $\mathbf{GL}(n, \mathbf{R})$, image réciproque de $\mathfrak{S}'$ par l'application $X \mapsto {}^tXX = I[X]$ et $\mathfrak{S}^1$ dans $\mathbf{SL}(n, \mathbf{R})$, égal à $\mathfrak{S} \cap \mathbf{SL}(n, \mathbf{R})$.

5.9. PROPOSITION. *Soit* F *une forme quadratique non dégénérée de signature* (a, b). *Les conditions suivantes sont équivalentes :*

(i) F *est réduite*;
(ii) $F \in I_{a,b}[\mathfrak{S}]$;
(iii) $F \in \alpha I_{a,b}[\mathfrak{S}^1]$, $(\alpha = |\det F|^{1/n})$.

(i) $\Rightarrow$ (ii), car il existe $C \in \mathfrak{H}(F) \cap \mathfrak{S}'$ et, d'après 5.2 (iii), $X \in \mathbf{GL}(n, \mathbf{R})$, tels que $I_{a,b}[X] = F$ et $I[X] = C$, i.e. $X \in \mathfrak{S}$.
(ii) $\Rightarrow$ (i), car si $F = I_{a,b}[X]$ avec $I[X] \in \mathfrak{S}'$, on a :

$$I[X] \in \mathfrak{H}(I_{a,b})[X] \cap \mathfrak{S}' = \mathfrak{H}(F) \cap \mathfrak{S}'.$$

Quant à la dernière équivalence, elle résulte d'un calcul évident.
Cette dernière proposition permet de reformuler le lemme de finitude ainsi :

5.10. LEMME. *Si* $\mathfrak{S}$ *est un ensemble de Siegel de* $\mathbf{SL}(n, \mathbf{R})$, *l'ensemble*

$$\mathbf{M}(n, \mathbf{Z}) \cap \alpha . I_{a,b}[\mathfrak{S}], \qquad (\alpha \in \mathbf{R}\,;\ \alpha > 0),$$

est fini.

C'est sous cette forme qu'il va être démontré dans le paragraphe 6.

6. Un lemme de finitude

6.1. DÉFINITION. Un sous-groupe G de $\mathbf{GL}(n, \mathbf{R})$ est dit auto-adjoint (ou plus précisément I-auto-adjoint) si :

$$X \in G \Rightarrow {}^tX \in G.$$

6.2. LEMME. G *étant égal à* $\mathbf{GL}(n, \mathbf{R})$ *ou à* $\mathbf{SL}(n, \mathbf{R})$, *on considère un ensemble de Siegel* $\mathfrak{S}$ *de* G, *une représentation du groupe opposé dans un espace vectoriel réel* V *muni d'un réseau* L *et un vecteur* v *de* V. *On suppose que :*

(i) *l'orbite* $v.G$ *de* v *est fermée dans* V,
(ii) *le groupe d'isotropie* G_v *de* v *est auto-adjoint,*
(iii) A *étant le groupe des matrices diagonales de* G *à coefficients diagonaux* > 0, *les opérateurs de* A *sont simultanément diagonalisables ; la décomposition de* V *associée :* $V = \oplus_\mu V_\mu$, *où* $V_\mu = \{w \in V \mid w.a = \mu(a)\, w$ *pour tout* $a \in A\}$ *est le sous-espace de poids* μ, *est telle que* $V_\mu \cap L$ *soit un réseau de* V_μ *pour tout* μ.
Alors, l'ensemble $v.\mathfrak{S} \cap L$ *est fini.*

Dans cette démonstration, on note $x = k_x a_x n_x$ la décomposition d'Iwasawa d'un élément x de G et on pose :

$$y_x = x.a_x^{-1} \qquad \text{et} \qquad z_x = x.a_x^{-2}.$$

Prouvons quelques majorations préliminaires :
On peut normer V de telle sorte que la somme $\oplus V_\mu$ soit orthogonale ; on note alors E_μ le projecteur de V sur V_μ. L'hypothèse (iii) permet d'affirmer que le sous-groupe $\sum_\mu V_\mu \cap L$ de L est un réseau de V ; il est donc d'indice fini dans L et comme sa projection sur V_μ en est le réseau $V_\mu \cap L$, la projection $E_\mu(L)$ de L est un réseau de V_μ. Cela prouve l'existence d'un nombre réel $c > 0$, tel que pour tout μ :

$$w \in L \qquad \text{et} \qquad E_\mu(w) \neq 0 \Rightarrow ||E_\mu(w)|| \geqslant c.$$

D'autre part, l'ensemble $\{a_x n_x a_x^{-1}\}_{x \in \mathfrak{S}}$ est relativement compact (1.3) ; or $y_x = k_x.a_x.n_x.a_x^{-1}$, si bien que l'ensemble $\{v.y_x\}_{x \in \mathfrak{S}}$ est borné ; il existe donc une constante c', telle que l'on ait $||v.y_x|| \leqslant c'$ quel que soit $x \in \mathfrak{S}$.
En combinant ces deux majorations, on va montrer que l'ensemble :

$$\{||v.z_x||\}_{x \in \mathfrak{S},\, v.x \in L}$$

est borné. Comme $y_x = x.a_x^{-1}$, $z_x = x.a_x^{-2}$, on a :

$$E_\mu(v.y_x) = \mu(a_x^{-1}).E_\mu(v.x), \qquad E_\mu(v.z_x) = \mu(a_x^{-2}).E_\mu(v.x).$$

Étant donné $x \in G$ et μ, on a, ou bien $E_\mu(v.x) = 0$, donc aussi $E_\mu(v.z_x) = 0$, ou bien $E_\mu(v.x) \neq 0$, auquel cas on tire de ce qui précède :

$$||E_\mu(v.z_x)|| = ||E_\mu(v.y_x)||^2.||E_\mu(v.x)||^{-1} \leqslant c'^2.c^{-1}, \qquad (v.x \in L;\ x \in \mathfrak{S}).$$

L'hypothèse (i) sert à prouver que la bijection $G_v \backslash G \to v.G$ est un homéomorphisme : en effet G opère continûment et transitivement dans $v.G$, qui est un espace de Baire, en tant que fermé de V [8, Chap. VII, App. 1, Lemme 2]. On peut donc remonter à G la majoration trouvée ci-dessus : il existe un compact M de G, tel que l'on ait :

$$\{z_x\}_{x \in \mathfrak{S},\, v.x \in L} \subset G_v.M.$$

Or $z_x = k_x a_x n_x a_x^{-2} = k_x a_x^{-1} a_x^2 n_x a_x^{-2}$; si $x \in \mathfrak{S}$, alors $a_x^2 \in A_t$, et (1.3) l'ensemble $\{a_x^2.n_x.a_x^{-2}\}_{x \in \mathfrak{S}}$ est relativement compact. Ainsi il existe un autre compact M' tel que l'on ait :

$$\{k_x.a_x^{-1}\}_{x \in \mathfrak{S},\, v.x \in L} \subset G_v.M'.$$

D'après l'hypothèse (ii), l'automorphisme $\theta : x \mapsto {}^t x^{-1}$ de G laisse fixe G_v, d'où : $\theta(k_x.a_x^{-1}) = k_x a_x = x n_x^{-1} \in G_v.\theta(M')$.
Finalement, il existe un compact M'' de G tel que l'ensemble $\{x\}_{x \in \mathfrak{S},\, v.x \in L}$ soit inclus dans $G_v M''$, ce qui prouve la finitude de l'ensemble

$$\{v.x\}_{x \in \mathfrak{S},\, v.x \in L},$$

qui est contenu à la fois dans un compact et dans un réseau de V.

6.3. *Application à* 5.10.

Il est immédiat que la conclusion du lemme ci-dessus, dans le cas particulier où l'on prend :

$$V = \mathbf{M}(n, \mathbf{R}), \qquad L = \mathbf{M}(n, \mathbf{Z}), \qquad v = \alpha.I_{a,b},$$

et $G = \mathbf{SL}(n, \mathbf{R})$ opérant à droite dans V de la manière habituelle, n'est autre que celle de 5.10. Il reste donc à voir qu'un tel choix des données satisfait bien aux hypothèses (i), (ii) et (iii) du lemme :

(i) $v.G = \{\alpha.I_{a,b}[g]\}_{g \in \mathbf{SL}(n,\mathbf{R})}$ est l'ensemble des matrices symétriques de signature (a, b) et de déterminant $\alpha^n(-1)^b$; c'est donc un fermé de V.

(ii) $G_v = O(I_{a,b}) \cap \mathbf{SL}(n, \mathbf{R})$; il est auto-adjoint, comme en général O(F) lorsque la matrice symétrique F est égale à son inverse.

(iii) Une base du réseau est $\{E_{ij}\}_{1 \leqslant i,\, j \leqslant n}$, où E_{ij} désigne la matrice dont le seul coefficient non nul est celui de ligne i et colonne j, égal à 1. Or E_{ij} est un vecteur propre pour tout élément a de A, car $E_{ij}[a] = a_{ii}a_{jj}E_{ij}$.

Faisons quelques remarques finales à propos de l'hypothèse (iii) du lemme :

1) Si $G = \mathbf{SL}(n, \mathbf{R})$, on peut diagonaliser simultanément les opérateurs de A.

2) Si la représentation du groupe est définie sur $\mathbf{Q}$, on peut diagonaliser les opérateurs de A simultanément sur $\mathbf{Q}$.

Ainsi pour une représentation : $G \to \mathbf{GL}_m$ définie sur $\mathbf{Q}$, la dernière hypothèse est toujours vérifiée lorsque L est un réseau de $\mathbf{Q}^m$.

6.4. *Remarque.* Reprenons les hypothèses de 6.2 et supposons de plus le réseau L stable par $G_{\mathbf{Z}} = G \cap \mathbf{GL}(n, \mathbf{Z})$. Alors $V \cap L$ est formé d'un nombre *fini* d'orbites de $G_{\mathbf{Z}}$. En effet, on a (§ 1) $G = \mathfrak{S}.G_{\mathbf{Z}}$ pour $\mathfrak{S}$ convenable, donc si $x \in L \cap V$, alors $x:G_{\mathbf{Z}}$ fait partie de l'ensemble $L \cap v.\mathfrak{S}$, qui est fini d'après 6.2.

Plaçons-nous de nouveau dans le cas particulier de 6.3. Une orbite de $\mathbf{GL}(n, \mathbf{Z})$ (resp. $\mathbf{SL}(n, \mathbf{Z})$) dans l'espace des formes quadratiques non dégénérées est une *classe* (resp. *classe propre*) de formes quadratiques. On voit donc que les formes quadratiques entières de déterminant non nul donné se répartissent en un nombre fini de classes (resp. de classes propres).

6.5. *Formes homogènes.* Nous voulons encore signaler une généralisation du résultat précédent à des formes de degré $\geqq 3$, qui remonte à Jordan.

Soit $F_{m,n}$ l'espace des formes homogènes de degré m sur $\mathbf{C}^n$. Il est défini sur $\mathbf{Q}$, la $\mathbf{Q}$-structure étant donnée par les formes à coefficients rationnels. On a une représentation naturelle $\pi_{m,n}$ de $\mathbf{GL}(n, \mathbf{C})$ dans $F_{m,n}$, qui est évidemment définie sur $\mathbf{Q}$. Soient $m, n \geqq 3$ et F un élément de $F_{m,n}$ de discriminant non nul. D'après Jordan [14], le groupe d'isotropie de F dans $\mathbf{SL}(n, \mathbf{C})$ est *fini*. Il s'ensuit que l'orbite $X = \pi_{m,n}(\mathbf{SL}(n, \mathbf{C})).F$ de F est *fermée*. En effet, d'après un principe élémentaire de théorie des groupes algébriques [1], cette orbite est un ouvert de Zariski de son adhérence, et son adhérence est formée d'orbites de dimension strictement plus petite que dim X, qui est ici égale à celle de $\mathbf{SL}(n, \mathbf{C})$ d'après le théorème de Jordan. Mais $\mathbf{SL}(n, \mathbf{C})$ laisse le discriminant invariant, donc un F' dans l'adhérence de X a aussi un discriminant non nul, et son orbite a, par conséquent, même dimension que X.

La première partie de 6.4 s'applique alors à X et montre que les formes à coefficients entiers qui sont transformées de F par $\mathbf{SL}(n, \mathbf{R})$ forment un nombre fini d'orbites de $\mathbf{SL}(n, \mathbf{Z})$, résultat démontré par Jordan et Poincaré. En fait, le théorème de Jordan est plus fort et donne la finitude des orbites de $\mathbf{SL}(n, \mathbf{Z}(i))$, où $\mathbf{Z}(i)$ désigne l'anneau des entiers de Gauss, dans l'ensemble des éléments de X dont les coefficients appartiennent à $\mathbf{Z}(i)$. On pourrait évidemment en donner une démonstration analogue, mais il faudrait pour cela développer le § 1 pour $\mathbf{SL}(n, \mathbf{C})$ et $\mathbf{SL}(n, \mathbf{Z}(i))$. Ce résultat est aussi englobé dans un théorème de [5], sur lequel nous reviendrons en 9.11.

Remarque. Soit F_0 l'hypersurface de l'espace projectif $\mathbf{P}(n - 1, \mathbf{C})$ définie par l'annulation de F. La forme F est de discriminant non nul si, et seulement si, F_0 est lisse. Le théorème de Jordan cité plus haut équivaut au fait que le groupe des transformations projectives laissant F_0 stable est fini. Au moins, si $n \geqq 5$, on peut plus généralement montrer que le groupe Aut F_0 des automorphismes (i.e. homéomorphismes biholomorphes ou, ce qui revient au même d'après le théorème de Chow, birréguliers) de F_0 est fini. On sait que ce groupe est un groupe de Lie complexe. D'après Kodaira-Spencer (*Annals of Math.* (2), **67** (1958), 328-466, lemme 14.2, p. 406), il est discret. Par conséquent, pour tout plongement projectif de F_0, le groupe des transformations projectives laissant F_0 stable, qui est évidemment algébrique, est fini. Or, si $n \geqq 5$, le théorème de Lefschetz entraîne que F_0 est simplement connexe, de deuxième nombre de Betti égal à un. Le groupe Aut F_0 possède donc un sous-groupe H d'indice $\leqq 2$ qui opère trivialement sur le deuxième groupe de cohomologie entière $H^2(F_0; \mathbf{Z}) \simeq \mathbf{Z}$ de F_0. Le groupe H laisse alors stable toute polarisation de F_0, et opère par transformations projectives dans le plongement défini par un système linéaire ample, donc H est fini. Ce dernier raisonnement montre aussi que la composante connexe de Aut F_0 est formée de transformations projectives dans un plongement convenable. Pour $n \geqq 5$, il suffit donc d'utiliser le théorème de Jordan.

Note bibliographique

La construction d'ensembles fondamentaux décrite en 5.8 est due à Hermite [13, p. 122-135]. Le point essentiel en est la finitude du nombre de réduites entières de déterminant non nul donné (5.7); cependant la démonstration fournie par Hermite est incomplète, car elle suppose implicitement que la forme F ne représente pas zéro rationnellement (i.e. $F(x) \neq 0$ si $x \neq 0$ est à coordonnées rationnelles), restriction sérieuse, puisque A. Meyer démontrait plus tard qu'elle entraînait que le nombre de variables est $\leqq 4$.

Des démonstrations de ce lemme ont été ensuite données par Stouff [31], Mordell [18], Siegel [29]. D'un autre côté, antérieurement à Stouff, C. Jordan [14] et H. Poincaré [24] ont prouvé le lemme de Hermite, et ont établi les analogues pour des formes de degré > 2 dont il a été question en (6.5).

Le lemme 6.2 lui-même est démontré sous une forme plus générale dans [5, lemme 5.3], mais le cas considéré ici suffit pour les applications que nous avons en vue.

Groupes algébriques

7. Rappels sur les groupes algébriques. Groupes arithmétiques

A. *Généralités.*

7.1. On fixe pour toute la suite un corps algébriquement clos Ω (il s'agira en pratique de $\mathbf{C}$). Rappelons que le plongement de $\mathbf{GL}(n, \Omega)$ dans Ω^{n^2+1} défini par

$$g \mapsto (g_{ij}, \text{dét } (g_{ij})^{-1})$$

lui donne une structure de variété algébrique affine, dont l'anneau des fonctions régulières est $\Omega[X_{ij}, X_0]/(X_0 \text{ dét } (X_{ij}) - 1) = \Omega[X_{ij}, (\text{dét } (X_{ij}))^{-1}]$.

DÉFINITION. *On appelle groupe algébrique de matrices un sous-groupe* G *de* $\mathbf{GL}(n, \Omega)$ *qui en est un sous-ensemble algébrique, i.e. l'ensemble des zéros d'un idéal de fonctions polynômes. On dit que* G *est défini sur le sous-corps* k *de* Ω, *ou que* G *est un* k*-groupe, si l'idéal de tous les polynômes nuls sur* G *admet un système de générateurs appartenant au sous-anneau :*

$$k[X_{ij}, (\text{dét } (X_{ij}))^{-1}].$$

Si B est un sous-anneau de Ω, on pose $G_B = G \cap \mathbf{GL}(n, B)$.

On peut considérer plus généralement un sous-groupe G de GL(V), V désignant un Ω-espace vectoriel de dimension finie. Si, par le choix d'une base dans V, il s'identifie à un groupe algébrique de matrices, un tel groupe G est appelé groupe algébrique (plus précisément linéaire). L'anneau des fonctions régulières sur G est noté $\Omega[G]$.

Si V a une k-structure, k désignant un sous-corps de Ω, i.e. s'il provient par extension des scalaires d'un k-espace vectoriel V_k, on dit que G est défini sur k s'il en est ainsi pour le groupe de matrices associé à G grâce à une base de V_k. On note alors $k[G]$ le sous-anneau de $\Omega[G]$ formé des fonctions régulières définies sur k. En outre l'algèbre de Lie $\mathfrak{g}$ de G a une k-structure : $\mathfrak{g} = \Omega \otimes_k \mathfrak{g}_k$ où $\mathfrak{g}_k$ désigne $\mathfrak{gl}(V_k) \cap \mathfrak{g}$.

7.2. DÉFINITION. *Un morphisme de groupes algébriques est un morphisme de groupes :*

$$\varphi : G \to G'$$

dont le comorphisme φ^0 *transforme une fonction régulière sur* G′ *en une fonction régulière sur* G. *Si* G *et* G′ *sont définis sur le sous-corps* k *de* Ω, *on dit que le morphisme* Ω *est défini (ou rationnel) sur* k *ou est un* k*-morphisme, si :*

$$\varphi^0(k[G']) \subset k[G].$$

Une représentation algébrique d'un groupe algébrique G dans un Ω-espace vectoriel W est un morphisme algébrique de G dans GL(W). Une telle représentation permet de faire opérer G à droite sur $\Omega[W]$ par :

$$\varphi \mapsto \varphi.g,$$

fonction définie par $(\varphi.g)(w) = \varphi(g.w)$. G opère de la même manière sur $\Omega[X]$ pour toute sous-variété affine X de W stable par G : si W et X sont définis sur k, comme l'action de G préserve la filtration de $\Omega[W]$, toute fonction $\varphi \in k[X]$ appartient à un sous-espace vectoriel de $\Omega[X]$, qui est invariant par G, de dimension finie et défini sur k. Dans le cas particulier où $X = G \subset GL(V)$ et où $W = \mathrm{End}(V)$, on retrouve l'action de G sur $\Omega[G]$ par translations à gauche.

DÉFINITION. *On appelle caractère du groupe algébrique* G *un morphisme algébrique de* G *dans* $\mathbf{GL}(1)$.

Le groupe commutatif des caractères est noté X(G). Si G est défini sur k, le sous-groupe $X(G)_k$ est le sous-groupe des caractères définis sur k.

7.3. Soit $G \subset \mathbf{GL}(n, \Omega)$ un k-groupe. Les parties semi-simple g_s et unipotente g_u d'un élément $g \in G$ appartiennent à G. Cette décomposition de Jordan est préservée par tout morphisme. Si k est parfait, et $g \in G_k$, alors $g_s, g_u \in G_k$. Supposons k de caractéristique zéro. Alors l'application exponentielle définit une bijection de l'ensemble des éléments nilpotents de $\mathfrak{g}_k$ sur l'ensemble des éléments unipotents de G_k, qui est une application polynomiale dont l'inverse, définie par le logarithme, est aussi polynomiale. En particulier, G_k est formé d'éléments semi-simples si, et seulement si, $\mathfrak{g}_k$ ne contient pas d'élément nilpotent $\neq 0$.
Signalons aussi l'analogue infinitésimal de la première assertion de ce paragraphe : les parties semi-simple x_s et nilpotente x_n de $x \in \mathfrak{g}$ font partie de $\mathfrak{g}$. Cette décomposition est préservée par la différentielle de tout morphisme de groupes algébriques.

7.4. La composante connexe de l'élément neutre d'un groupe algébrique en topologie de Zariski est irréductible et d'indice fini. Dans le cas où $\Omega = \mathbf{C}$, donc où G a aussi une structure de groupe de Lie complexe, elle s'identifie à la composante neutre de G en topologie ordinaire.
Si $\Omega = \mathbf{C}$, alors $G_{\mathbf{R}}$ est un groupe de Lie réel à un nombre fini de composantes connexes (en topologie ordinaire), mais il n'est pas toujours connexe si G est un $\mathbf{R}$-groupe connexe. On notera G^0 la composante neutre de G, et si $\Omega = \mathbf{C}$ on notera aussi $G^0_{\mathbf{R}}$ la composante neutre de $G_{\mathbf{R}}$ en topologie ordinaire.
Un morphisme surjectif $f : G \to G'$ de $\mathbf{R}$-groupes, défini sur $\mathbf{R}$, induit un homomorphisme $G_{\mathbf{R}} \to G'_{\mathbf{R}}$ de groupes de Lie réels qui n'est pas nécessairement surjectif. Cependant, il applique $G^0_{\mathbf{R}}$ sur $G'^0_{\mathbf{R}}$, donc $f(G_{\mathbf{R}})$ est un sous-groupe ouvert et fermé d'indice fini de $G'_{\mathbf{R}}$. Si H et H' sont des $\mathbf{R}$-sous-groupes de G et G' tels que $f(H) \subset H'$, alors l'application $G_{\mathbf{R}}/H_{\mathbf{R}} \to G'_{\mathbf{R}}/H'_{\mathbf{R}}$ induite par f a une image ouverte et fermée, et $G'_{\mathbf{R}}/H'_{\mathbf{R}}$ est réunion d'un nombre fini d'orbites de $G_{\mathbf{R}}$, qui sont chacune ouverte et fermée.

La finitude du nombre de composantes connexes de $G_{\mathbf{R}}$ peut s'envisager comme cas particulier de la proposition suivante [6, § 6.4] :
Soit ρ une représentation définie sur $\mathbf{R}$ du $\mathbf{R}$-groupe G dans l'espace vectoriel V et soit $v \in V_{\mathbf{R}}$. Alors l'ensemble $(G.v)_{\mathbf{R}}$ des points réels de l'orbite $G.v$ de v est la réunion d'un nombre fini d'orbites de $G^0_{\mathbf{R}}$.

B. *Groupes réductifs.*

7.5. On rappelle qu'un tore est un groupe connexe, commutatif et formé d'éléments semi-simples, ce qui revient à dire qu'il est diagonalisable connexe, i.e. isomorphe à $(\Omega^*)^m$ pour un certain entier m. Un groupe de radical réduit à $\{e\}$ est dit semi-simple (le radical est le plus grand sous-groupe distingué fermé, résoluble et connexe).

DÉFINITION. *Un groupe algébrique* G *est dit réductif si sa composante neutre* G^0 *est égale au produit presque direct* $S.H$ *d'un tore* S *central par un groupe semi-simple* H.

Cette propriété équivaut en caractéristique 0 à la complète réductibilité des représentations de G.
Dans ce qui suit on se limite d'ailleurs à la caractéristique 0.

7.6. PROPOSITION. *Soient* G *un groupe réductif opérant sur un espace vectoriel* W *et* X *une sous-variété irréductible de* W *stable par* G. *Soit* I *l'anneau* $\Omega[X]^G$ *des fonctions régulières sur* X *invariantes par* G :

(i) *il existe un projecteur* $\natural : \Omega[X] \to I$, *qui est* I*-linéaire et qui laisse stable tout sous-espace invariant par* G ;
(ii) I *sépare les ensembles algébriques fermés de* X *stables par* G ;
(iii) I *est une* Ω*-algèbre de type fini.*

(i) Soit N la somme des sous-espaces minimaux de $\Omega[X]$ sur lesquels G n'opère pas trivialement. La complète réductibilité de l'action de G sur $\Omega[X]$ montre que $\Omega[X]$ est égal à $I \oplus N$. L'application bécarre $\natural$ est définie comme le projecteur sur I associé à cette décomposition. Il reste à voir qu'elle est I-linéaire ; or :

$$I \cap IN = \{0\},$$

ce qui entraîne d'après la complète réductibilité l'inclusion $IN \subset N$ et donc l'égalité; par suite si $\varphi \in I$ et $\psi \in \Omega[X]$, on a : $(\varphi.\psi)^\natural = \varphi.\psi^\natural + (\varphi.\psi_N)^\natural = \varphi.\psi^\natural$. Soit enfin E un sous-espace de $\Omega[X]$ stable par G; on a $E = (E \cap I) \oplus (E \cap N)$ vu la complète réductibilité, de sorte que $E^\natural \subset E$.
(ii) Soient A et B deux ensembles algébriques de X stables par G et d'idéaux I(A) et I(B). On les suppose disjoints et par suite *(Nullstellensatz)* $I(A) + I(B) = \Omega[X]$. Ainsi il existe $\alpha \in I(A)$ et $\beta \in I(B)$ tels que $\alpha + \beta = 1$, d'où $\alpha^\natural + \beta^\natural = 1$. Or la stabilité de A et de B par G entraîne celle de I(A) et de I(B) ; par suite (cf. (i)) $\alpha^\natural \in I(A)$ et $\beta^\natural \in I(B)$, et $\alpha^\natural$ est nul sur A, égal à un sur B.
(iii) $\Omega[X]$ s'identifie au quotient de $\Omega[W]$ par l'idéal de X et la projection $\pi : \Omega[W] \to \Omega[X]$ commute à G. La complète réductibilité entraîne l'égalité :

$$\pi(\Omega[W]^G) = I.$$

Il suffit donc de démontrer (iii) lorsque $X = W$. En ce cas les fonctions de I nulles à l'origine engendrent un idéal ayant un ensemble générateur fini $f_1, \ldots, f_s$. Comme les composantes homogènes d'un polynôme invariant sont aussi invariantes, on peut supposer les f_i homogènes, et il suffit de faire voir que tout élément homogène $f \in I$ de degré > 0 est un polynôme en les f_i. On peut écrire $f = \sum_1^s a_i . f_i$, avec $a_i \in \Omega[W]$ homogène de degré $d^0 a_i$ égal à $d^0 f - d^0 f_i$, donc aussi, vu (i), avec $a_i \in I$ homogène de degré $d^0 f - d^0 f_i$. La conclusion s'ensuit alors par récurrence sur le degré.

7.7. PROPOSITION. *Soient* G *un groupe algébrique connexe,* H *un sous-groupe réductif de* G *et* k *un corps de définition pour* G *et* H. *Il existe alors un espace vectoriel de dimension finie* W *défini sur* k, *une représentation à droite de* G *dans* W *rationnelle sur* k *et un point* $w \in W_k$, *tels que l'orbite* X *de* w *soit fermée et que son groupe d'isotropie soit* H.

Cela signifie en particulier que l'ensemble des classes à droite $H\backslash G$ de G suivant H a une structure de variété affine définie sur k.

La démonstration utilise les conclusions de 7.6 dans la situation particulière suivante: le groupe réductif H opère à gauche sur la variété $G \subset GL(V)$, qu'on peut regarder fermée dans $W = \mathrm{End}\,(V \oplus \Omega)$ suivant le plongement usuel (cf. (7.1)).

Ainsi l'algèbre $I = \Omega[G]^H$ des fonctions constantes sur les classes à droite Hx de G suivant H admet un ensemble générateur fini $w_1, \ldots, w_s$, qu'on peut prendre dans $k[G]$ (7.6 (iii)). Ceux-ci appartiennent donc à des sous-espaces W_i de $\Omega[G]$, qui sont définis sur k, stables par G et de dimension finie (cf. A).

Nous allons montrer que l'espace vectoriel $W = \bigoplus_{i=1}^s W_i$, muni de la représentation à droite de G définie par :

$$(v_1, \ldots, v_s) \mapsto (v_1 . g, \ldots, v_s . g)$$

et du point $w = (w_1, \ldots, w_s) \in W_k$, résout le problème posé dans l'énoncé.

Il faut pour cela prouver d'abord que le groupe d'isotropie G_w de w est H; on a $G_w \supset H$, car $w_i \in I$ entraîne $w_i . g = w_i$ et $w . g = w$ pour $g \in H$; inversement, $G_w \subset H$, car si $g \in G_w$, on a $w_i . g = w_i$, donc $w_i(g) = w_i(e)$ pour tout i; or $\{w_i\}$ engendre I, ce qui entraîne $f(g) = f(e)$ pour tout $f \in I$ et par suite $g \in H$, car I sépare les ensembles algébriques fermés de G stables par H, et en particulier les classes à droite de G suivant H, vu 7.6 (ii).

Il reste à montrer que l'orbite X de w est fermée, i.e. égale à $\overline{X}$. Au morphisme $\varphi : G \to W$ défini par $g \mapsto w . g$ correspond le comorphisme

$$\varphi^0 : A = \Omega[\overline{X}] \to \Omega[G].$$

En fait $\varphi^0(A)$ est dans I, car l'inclusion $G_w \supset H$ implique :

$$[(\varphi^0 f) . h](g) = f(w . h . g) = f(wg) = (\varphi^0 f)(g).$$

L'application φ^0 est injective, car si $\varphi^0 f$ est nulle, c'est que f est nulle sur X, donc sur $\overline{X}$. Son image enfin est I; pour le voir, il suffit de montrer que chaque généra-

teur w_i de I appartient à $\varphi^0(B)$. Or si $\{z_1, \ldots, z_n\}$ est une base de W_i et $\{a_1, \ldots, a_n\}$ la base duale, celle-ci définit des fonctions sur W :

$$u_j : (v_1, \ldots, v_s) \mapsto a_j(v_i)$$

telles que $(\varphi^0 u_j)(g) = a_j(w_i.g)$. Il en résulte :

$$w_i(g) = (w_i.g)(e) = \sum_j a_j(w_i.g)\, z_j(e) = \sum_j z_j(e)(\varphi^0 u_j)(g).$$

Ainsi φ^0 est un isomorphisme de A sur I.

Établir l'égalité $X = \overline{X}$ revient à prouver pour tout $x \in \overline{X}$ l'existence d'un zéro $y \in X$ de l'idéal maximal I_x de x ou encore celle d'un zéro $g \in G$ de $\varphi^0(I_x)$. Il suffit pour cela de savoir que $\varphi^0(\mathfrak{m})\,\Omega[G]$ est un idéal propre de $\Omega[G]$ pour tout idéal propre $\mathfrak{m}$ de A : or s'il n'en était pas ainsi, il existerait $m_1, \ldots, m_t \in \mathfrak{m}$ et $f_1, \ldots, f_t \in \Omega[G]$ tels que $\sum \varphi^0(m_i) f_i = 1$, ce qui entraînerait d'après 7.6 (i) et l'inclusion $\varphi^0(A) \subset I$:

$$\sum (\varphi^0 m_i).f_i^{\sharp} = 1.$$

Mais φ^0 est inversible, d'où $\sum m_i f_i' = 1$ avec $f_i' \in A$, ce qui contredit le fait que $\mathfrak{m}$ est propre dans A. Q.E.D.

Remarque. 7.7. montre que l'espace quotient G/H peut être muni d'une structure de variété algébrique, (en fait affine). On voit facilement que c'est une structure quotient au sens de 7.10.

On prouve plus généralement, pour k quelconque, que si H est un k-sous-groupe de G, alors le quotient de G par H « existe » et est défini sur k, et est une variété quasi projective. Cela peut se faire aussi en utilisant une représentation linéaire convenable de G (cf. [1, § 6]).

7.8. PROPOSITION. *Soient* G *un groupe algébrique,* H *un sous-groupe fermé, k un corps de définition commun à* G *et* H. *Alors il existe un espace vectoriel de dimension finie* W, *défini sur k, un morphisme* $G \to GL(W)$ *défini sur k, et un point* $w \in W_k$ *tels que* H *soit l'ensemble des éléments de* G *qui laissent stable la droite* $[w]$ *engendrée par* w.

Soit $J \subset \Omega[G]$ l'idéal des fonctions nulles sur H. Il est défini sur k et possède un système générateur fini. Il existe donc (cf. A) un sous-espace V de dimension finie de $\Omega[G]$, défini sur k, stable par translations à gauche, tel que $V \cap J$ engendre J. On prend alors $W = \wedge^d V$, $(d = \dim V \cap J)$, $[w]$ la droite correspondant à $V \cap J$, et pour ρ la représentation induite dans W par la représentation donnée de G dans V.

7.9. COROLLAIRE. *Si* $X(H)_k = \{1\}$, *alors il existe un morphisme* $G \to GL(W)$ *défini sur k et un point* $w \in W_k$ *dont le groupe d'isotropie est* H.

En effet, l'hypothèse $X(H)_k = \{1\}$ montre que la représentation de H dans $[w]$ est triviale.

7.10. *Remarques.* (1) Il y a une réciproque (*due à Y. Matsushima*, Nagoya M. J., **16** (1950), 205-218) à 7.6 :

« *Si* G *est réductif,* H *un sous-groupe fermé de* G *et* G/H *une variété affine, alors* H *est réductif.* »

Pour d'autres démonstrations, voir [5, § 3.5] ou A. Bialynicki-Birula (*Amer. J. M.*, **85** (1963), 577-582). Dans les deux cas, on se borne à la caractéristique zéro. En fait, il semble qu'en utilisant la cohomologie de Grothendieck, on puisse étendre la démonstration de [5] aux caractéristiques $p > 0$.

(2) La démonstration de 7.7, convenablement modifiée et complétée, donne plus généralement :

« *Soit* X *une variété affine sur laquelle un groupe réductif* H *opère de manière à ce que toutes les orbites soient fermées. Alors le quotient* X/H « *existe* » *et est une variété affine.* »

L'expression « le quotient existe et est affine » signifie ici que l'on peut trouver une variété affine V, un morphisme $\pi : X \to V$, dont les fibres sont les orbites de H, tels que si $f : X \to W$ est un morphisme de X dans une variété algébrique W, qui est constant sur les orbites de H, alors il existe un morphisme $g : V \to W$ tel que $f = g \circ \pi$.

En caractéristique non nulle, cet énoncé et la démonstration ci-dessous valent encore si H est un tore, ce qui équivaut à dire que H a toutes ses représentations rationnelles complètement réductibles [27]. Il ne sera pas utilisé dans la suite, et nous nous bornons à en indiquer brièvement la démonstration, en supposant connues quelques notions élémentaires sur les variétés affines.

Soit $I = \Omega[X]^H$. C'est une algèbre de type fini (7.6). Soit $\{f_1, \ldots, f_d\}$ un système générateur de I. On a donc $I \cong \Omega[T_1, \ldots, T_d]/J$, où J est le noyau de l'homomorphisme $\Omega[T_1, \ldots, T_d] \to \Omega[X]$ défini par $T_i \mapsto f_i$ $(1 \leqq i \leqq d)$. Soit $V \subset \Omega^d$ la variété affine d'idéal J. Alors $\pi : x \mapsto (f_1(x), \ldots, f_d(x))$ définit un morphisme de X dans V. Nous voulons montrer que (V, π) vérifie les conditions imposées plus haut. Le fait que les invariants séparent les ensembles fermés disjoints stables par H (7.6), et l'hypothèse entraînent que les fibres de π sont les orbites de H. Montrons que π est surjectif. Soit $v \in V$ et soit A l'idéal des éléments de $\Omega[V] \cong I$ s'annulant en v. Montrons que $B = A.\Omega[X]$ est un idéal propre de $\Omega[X]$. Si ce n'était pas le cas, on pourrait trouver des éléments $a_j \in A$, $c_j \in \Omega[X]$ $(1 \leqq i \leqq n)$, tels que $\sum a_j.c_j = 1$, d'où :

$$(\sum a_j.c_j)^\natural = \sum a_j.c_j^\natural = 1,$$

et $1 \in A$, ce qui est absurde. Ainsi $B \neq \Omega[X]$ et il existe $x \in X$ qui annule B. On a alors $\pi(x) = v$.

La condition de factorisation formulée plus haut peut aussi s'exprimer ainsi : soient $p, q \in \Omega[X]$ et $a \in X$ tels que $f = p/q$ soit invariante par H, et que $q(a) \neq 0$. Alors il existe $p', q' \in I$ tels que $f = p'/q'$ et $q'(a) \neq 0$. [Ici, p/q, p'/q' sont vus comme des éléments de l'anneau total des fractions de $\Omega[X]$, sur lequel H opère de façon évidente. À $f = p/q$, on associe une fonction régulière sur l'ouvert U des points où $q \neq 0$, dont la valeur en u est égale à $p(u)/q(u)$.]

Soit E un sous-espace de dimension finie de $\Omega[X]$ contenant q et stable par H (7.2). On a une décomposition unique $E = E^\natural + E'$ où $E' = \ker \natural \cap E$. Évidemment, $f.E = f.E^\natural + f.E'$, d'où, vu l'unicité de cette décomposition, $f.E^\natural = (f.E)^\natural$, et en particulier :

$$p^\natural = (f.q)^\natural = f.q^\natural,$$

ce qui montre que $f = p^\natural/q^\natural$. Notre assertion est donc établie si $q^\natural(a) \neq 0$. Quels que soient $s \in \Omega[X]$ et $h \in H$, on peut évidemment écrire $f = s.(p.h)/s.(q.h)$. On a alors aussi :

$$f = (s.(p.h))^\natural/(s.(q.h))^\natural$$

et il suffit, pour terminer la démonstration, de faire voir que l'on peut choisir s et h de manière à ce que $(s.(q.h))^\natural(a) \neq 0$.

Soit F le sous-espace de $\Omega[X]$ engendré par les transformés $q.h$ de q $(h \in H)$ et soit J l'idéal de $\Omega[X]$ engendré par les fonctions $f_i - f_i(a)$ et par F $(1 \leqq i \leqq d)$. Montrons que $1 \in J$. Supposons que ce ne soit pas le cas. On peut alors trouver un zéro $b \in X$ de J. On a donc $f_i(b) = f_i(a)$, $(1 \leqq i \leqq d)$, d'où $r(b) = r(a)$ $(r \in I)$, ce qui entraîne l'existence de $h \in H$, tel que $b = h.a$. On en déduit :

$$q(a) = (q.h^{-1})(h.a) = q.h^{-1}(b) = 0$$

ce qui est absurde. Ainsi, $1 \in J$. On peut donc trouver :

$$c_i, d_j \in \Omega[X], \quad h_j \in H \qquad (1 \leqq i \leqq d;\ 1 \leqq j \leqq n)$$

tels que :

$$\sum_i c_i(f_i - f_i(a)) + \sum_j d_j.(q.h_j) = 1.$$

En appliquant $\natural$ aux deux membres et en les évaluant en a, on obtient :

$$\sum_j (d_j.(q.h_j))^\natural(a) \neq 0,$$

d'où notre assertion.

C. *Groupes arithmétiques.*

7.11. Dans cette section, V désigne un espace vectoriel sur $\mathbf{C}$ de dimension finie, muni d'une $\mathbf{Q}$-structure. Si G est un sous-groupe algébrique de GL(V) défini sur $\mathbf{Q}$, et L un réseau de $V_{\mathbf{Q}}$, on note G_L, et on appelle *groupe des* L-*unités de* G, le sous-groupe de $G_{\mathbf{Q}}$ laissant L stable : $G_L = \{g \in G_{\mathbf{Q}}, g(L) = L\}$.

Rappelons que deux sous-groupes A, B d'un groupe H sont dits commensurables si $A \cap B$ est d'indice fini dans A et dans B.

DÉFINITION. *Soit* G *un* $\mathbf{Q}$-*sous-groupe de* GL(V). *Un sous-groupe* Γ *de* $G_{\mathbf{Q}}$ *est dit arithmétique s'il existe un réseau* L *de* $V_{\mathbf{Q}}$ *tel que* Γ *soit commensurable à* G_L.

Il résultera de 7.13 que cette propriété est indépendante de L et est invariante par $\mathbf{Q}$-isomorphisme.

Si l'on identifie V à $\mathbf{C}^n$ au moyen d'une base de L, alors G s'identifie à un $\mathbf{Q}$-sous-groupe G′ de $\mathbf{GL}(n, \mathbf{C})$ et G_L à $G'_{\mathbf{Z}}$. Il revient donc au même de dire que Γ est arithmétique s'il existe un plongement $G \subset \mathbf{GL}(n, \mathbf{C})$, défini sur $\mathbf{Q}$, qui applique Γ sur un sous-groupe de $\rho(G)_{\mathbf{Q}}$ commensurable à $\rho(G)_{\mathbf{Z}}$. Un sous-groupe Γ' de Γ est un *sous-groupe de congruence* (ou de congruence principal), s'il existe un entier $m > 0$ tel que :

$$\rho(\Gamma') = \{x \in \rho(\Gamma), \qquad x \equiv 1 \bmod m\}.$$

Un tel sous-groupe est évidemment distingué, d'indice fini.

7.12. PROPOSITION. *Soient* G *un sous-groupe défini sur* $\mathbf{Q}$ *de* $\mathbf{GL}(n, \mathbf{C})$ *et* ρ *une représentation définie sur* $\mathbf{Q}$ *de* G *dans un espace vectoriel* V *muni d'un réseau* L *de* $V_{\mathbf{Q}}$. *Il existe alors un sous-groupe de congruence de* $G_{\mathbf{Z}}$ *laissant* L *stable.*

ρ étant définie sur $\mathbf{Q}$, les coefficients des polynômes $P_{\mu,\nu}$ (on prend pour base de V une base de L), définis par $\rho(g)_{\mu,\nu} = P_{\mu,\nu}(g_{ij})$, sont rationnels. Il en est de même de ceux des polynômes $Q_{\mu,\nu}$ définis par :

$$\rho(g)_{\mu,\nu} - \delta_{\mu,\nu} = Q_{\mu,\nu}(g_{ij} - \delta_{ij}).$$

Mais ceux-ci sont sans terme constant, car $\rho(1) = 1$, et par suite si m est le dénominateur commun à tous leurs coefficients, on a : $Q_{\mu,\nu}(g_{ij} - \delta_{ij}) \in \mathbf{Z}$, dès que $g_{ij} - \delta_{ij} \equiv 0 \pmod{m}$, i.e. $g \equiv 1 \pmod{m}$. Pour un tel choix de g les coefficients $\rho(g)_{\mu,\nu}$ sont entiers, ce qui assure la stabilité de L par $\rho(g)$.

7.13. COROLLAIRE. (1) *Si* Γ *est un sous-groupe arithmétique de* G, *tout réseau* L' *de* $V_{\mathbf{Q}}$ *est contenu dans un réseau invariant par* Γ.
(2) *Soient* φ *un isomorphisme défini sur* $\mathbf{Q}$ *de* G *sur un* $\mathbf{Q}$*-groupe* G' *et* Γ, Γ' *des sous-groupes arithmétiques de* G *et* G'. *Alors* $\varphi(\Gamma)$ *est commensurable à* Γ'.
(3) *Si* φ *est un morphisme de* G *dans* G' *défini sur* $\mathbf{Q}$ *et si* $\Gamma \subset G_{\mathbf{Q}}$ *est arithmétique, il existe un groupe arithmétique* Γ' *de* G' *contenant* $\varphi(\Gamma)$.
(4) *Si* $G = H.N$ *est le produit semi-direct d'un sous-groupe invariant fermé* N *et d'un sous-groupe fermé* H *définis sur* $\mathbf{Q}$, *alors* $H_{\mathbf{Z}}.N_{\mathbf{Z}}$ *est un sous-groupe arithmétique de* G.

Démontrons (1). On peut identifier GL(V) à $\mathbf{GL}(n, \mathbf{C})$ de manière à ce que Γ soit commensurable à $G_{\mathbf{Z}}$ (7.11). Vu 7.12, il existe un sous-groupe Γ' d'indice fini de Γ qui laisse stable L'. L'ensemble des réseaux g(L') transformés de L' par des éléments de Γ est donc fini; la somme de ces réseaux est alors un réseau stable par Γ. (2) et (3) sont immédiats à partir de (1). Soit enfin π la projection de G sur $H = G/N$. Pour tout $g \in G$, on a évidemment $\pi(g)^{-1}.g \in N$. D'après (3), il existe un sous-groupe Γ d'indice fini de $G_{\mathbf{Z}}$ tel que $\pi(\Gamma)$ soit inclus dans $H_{\mathbf{Z}}$. On a alors $\Gamma \subset H_{\mathbf{Z}}.N_{\mathbf{Z}}$.

7.14. *Exemples de groupes arithmétiques.*

1) $\mathbf{GL}(n, \mathbf{Z})$ et $\mathbf{SL}(n, \mathbf{Z})$.
2) Le groupe des unités d'une forme quadratique rationnelle non dégénérée (§ 5).
3) Le groupe $\mathbf{Sp}(2n, \mathbf{Z})$ égal à $\{M \in \mathbf{GL}(2n, \mathbf{Z}) \mid {}^tM.J.M = J\}$, J désignant la matrice :

$$\left(\begin{array}{c|c} 0 & 1_n \\ \hline -1_n & 0 \end{array}\right)$$

4) Si k est un corps de nombres de base $\{\omega_1, \ldots, \omega_d\}$ sur $\mathbf{Q}$, celle-ci permet de plonger k^* dans $\mathbf{GL}(d, \mathbf{Q})$ par la représentation régulière. C'est alors l'ensemble des points rationnels sur $\mathbf{Q}$ d'un groupe G qui est un tore de dimension d défini sur $\mathbf{Q}$; le groupe G est le commutant de k^* dans $\mathbf{GL}(d, \mathbf{C})$.

Si la base $\{\omega_i\}$ est formée d'entiers, $G \cap \mathbf{M}(d, \mathbf{Z})$ s'identifie à l'ensemble des entiers algébriques non nuls de k. Le groupe arithmétique $G_{\mathbf{Z}}$ est alors le groupe des unités du corps de nombres k.

5) Plus généralement, on peut considérer une $\mathbf{Q}$-algèbre A de dimension finie, le groupe G des éléments inversibles de $A_{\mathbf{C}}$ et le groupe arithmétique G_L des unités d'un réseau L de $A_{\mathbf{Q}}$:

$$G_L = \{g \in A \mid gL = L\}.$$

Remarque. La notion de groupe arithmétique adoptée ici est un peu plus générale que la notion traditionnelle (indépendamment du fait que G n'est pas nécessairement un groupe classique). En effet, classiquement, un groupe défini arithmétiquement est un sous-groupe de $G_{\mathbf{Z}}$ caractérisé par des conditions de congruence portant sur les coefficients; en particulier, il contient toujours un sous-groupe de congruence au sens de 7.11. Il peut arriver qu'un groupe arithmétique au sens de 7.11 n'ait pas cette propriété, comme on le sait depuis longtemps lorsque $G = \mathbf{SL}_2$. Cependant, cette condition ne jouera pas de rôle ici. En fait, on verra même que les théorèmes principaux de réduction valent aussi pour tout sous-groupe de $G_{\mathbf{R}}$ (et non pas seulement de $G_{\mathbf{Q}}$) commensurable à $G_{\mathbf{Z}}$.

7.15. Dans ce livre, on considère principalement les groupes réductifs. Le passage de ces derniers au cas général se fait le plus souvent sans difficulté à l'aide du théorème de structure suivant.

THÉORÈME. *Soit k un corps de caractéristique zéro et G un k-groupe. Alors G est produit semi-direct d'un k-groupe réductif H et d'un k-groupe normal unipotent connexe N. Tout k-sous-groupe réductif de G est conjugué par un élément de N_k à un sous-groupe de H.*

Le sous-groupe N est uniquement déterminé par le théorème, c'est le *radical unipotent* de G, i.e. le plus grand sous-groupe normal de G formé de matrices unipotentes, noté quelquefois $R_u(G)$. C'est un groupe nilpotent. Remarquons encore que, N étant connexe, G est connexe si, et seulement si, H l'est. En particulier :

$$G^0 = H^0.N.$$

7.16. *Groupes sur un corps de nombres.* Soient $k \subset \mathbf{C}$ une extension finie de $\mathbf{Q}$, d son degré et S l'ensemble des monomorphismes de k dans $\mathbf{C}$. S contient donc d éléments, et l'on a $d = r_1 + 2r_2$ où r_1 est le nombre de places réelles de k (i.e. de s pour lesquels $s(k) \subset \mathbf{R}$) et r_2 le nombre de places complexes (i.e. de paires d'éléments de S formées d'un s tel que $s(k) \not\subset \mathbf{R}$ et de l'homomorphisme $x \mapsto \overline{s(x)}$). Soit $\mathfrak{o}$ l'anneau des entiers de k.

Soit G un sous-groupe algébrique défini sur k de $\mathbf{GL}(n, \mathbf{C})$. Un sous-groupe de G_k est dit *arithmétique* s'il est commensurable à $G_{\mathfrak{o}}$. Nous voulons indiquer ici, sans démonstration, comment cette notion se ramène à celle, en apparence plus particulière, de 7.11, en utilisant le foncteur $R_{k/\mathbf{Q}}$ de « restriction des scalaires ». Nous renvoyons à [33, Chap. I] pour une description de ce foncteur et nous bornons à indiquer comment construire $R_{k/\mathbf{Q}}G$ dans le cas présent.

Étant donné $s \in S$, notons ${}^sG$ le groupe conjugué de G par s, ou, en termes plus savants, le groupe obtenu à partir de G par changement de base, $s : k \to s(k)$; en termes moins savants, ${}^sG$ est le groupe dont l'idéal de définition dans $s(k)[X_{11}, \ldots, X_{nn}]$ est obtenu en appliquant s aux coefficients des éléments de $k[X_{11}, \ldots, X_{nn}]$ s'annulant sur G. Écrivons les éléments de $\mathbf{M}(n.d, \mathbf{C})$ en blocs de matrices carrées d'ordre n. Si $g \in \mathbf{GL}(n, k)$, notons ${}^sg$ ou $s(g)$ l'élément de $\mathbf{GL}(n, s(k))$ obtenu en appliquant s aux coefficients de g. Soit ι l'application $g \mapsto ({}^{s_1}(g), \ldots, {}^{s_d}(g))$, $(s_i \in S)$ de $\mathbf{GL}(n, k)$ dans $\mathbf{GL}(n.d, \mathbf{C})$. Soient enfin (α_i) une base de $\mathbf{Z}$-module de $\mathfrak{o}$, et A la matrice $(s_i(\alpha_j).I_n)$. On sait qu'elle est inversible. Il existe un sous-groupe G′ de $\mathbf{GL}(n.d, \mathbf{C})$ défini sur $\mathbf{Q}$, tel que :

$$G'_{\mathbf{Q}} = A.G_k.A^{-1}, \qquad G'_{\mathbf{Z}} = A.\iota(G_0).A^{-1}. \tag{1}$$

Le groupe G′ est isomorphe sur $\mathbf{C}$ au produit des ${}^sG$ $(s \in S)$. Enfin, soit J l'ensemble des places archimédiennes de k. On identifie J à une partie de S formée des r_1 places réelles et d'un représentant de chaque paire d'éléments complexes et complexes conjugués de S. Désignons par G_s $(s \in J)$ le groupe ${}^sG_{\mathbf{R}}$ (resp. ${}^sG_{\mathbf{C}}$) si s est réelle (resp. complexe). Alors :

$$G'_{\mathbf{R}} \cong \prod_{s \in J} G_s. \tag{2}$$

Le groupe G′ est le groupe $R_{k/\mathbf{Q}}G$ obtenu par restriction des scalaires de k à $\mathbf{Q}$ à partir de G.

Si $f : G \to H$ est un k-morphisme de k-groupes, alors on en déduit canoniquement un $\mathbf{Q}$-homomorphisme $R_{k/\mathbf{Q}}f : R_{k/\mathbf{Q}}G \to R_{k/\mathbf{Q}}H$. Sur $\mathbf{C}$, c'est le produit des conjugués ${}^sf : {}^sG \to {}^sH$ de f.

Supposons k imaginaire quadratique. Alors J comprend une place complexe. On a $G'_{\mathbf{R}} \cong G_{\mathbf{C}}$. On passe de G à $G'_{\mathbf{R}}$ en associant à $g = x + iy$ $(x, y \in \mathbf{M}(n, \mathbf{R}))$ la matrice $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$. Remarquons que, dans ce cas, G_0 est discret dans G. En général, il n'en est pas ainsi, mais G_0 s'identifie à un sous-groupe discret de $\prod_{s \in J} G_s$ par l'application « diagonale » ι. Un peu plus généralement, si J′ est une partie de J telle que G_s soit compact pour $s \in J$, $s \notin J'$, alors la projection de $\iota(G_0)$ dans le produit des facteurs G_s $(s \in J')$ est discrète.

Note bibliographique

Pour plus de détails sur les notions ou résultats rappelés ici sans démonstration, on renvoie à [1, 9]. En fait, ces exposés s'attachent à développer une théorie valable en toute caractéristique, alors que, pour les besoins de ce livre, la caractéristique zéro suffit amplement. Le lecteur qui préfère se restreindre à cette dernière, et se baser sur les livres de Chevalley [9] prendra garde au fait qu'il y a une légère différence entre les notions de groupe algébrique sur un corps k de [9] et celle de k-groupe algébrique au sens de 7.1.

Le théorème de 7.15 a été démontré tout d'abord pour les algèbres de Lie algébriques par Chevalley. La version globale a été établie par Mostow [20] dans le cadre de [9], ce qui implique que G_k est Zariski-dense dans G. Le passage de là au cas général est donné dans [6, § 5.1]. Le théorème de 7.10 (2) a été démontré par M. Nagata [23] et D. Mumford [22, Chap. I, Theorem 1.1, p. 26].

§ 8. Critère de compacité

On a déjà remarqué (cf. § 1) que l'ensemble $\mathscr{R}$ des réseaux de $\mathbf{R}^n$ s'identifie canoniquement à $\mathbf{GL}(n, \mathbf{R})/\mathbf{GL}(n, \mathbf{Z})$, ce qui permet de le munir de la topologie naturelle de cet espace quotient. Si $G \subset \mathbf{GL}(n, \mathbf{C})$ est un groupe algébrique, $G_{\mathbf{R}}/G_{\mathbf{Z}}$ se plonge de façon évidente dans $\mathscr{R}$.

8.1. PROPOSITION. *Soit* $G \subset \mathbf{GL}(n, \mathbf{C})$ *un* $\mathbf{Q}$*-groupe algébrique qui est soit réductif, soit sans caractère rationnel défini sur* $\mathbf{Q}$ *non trivial. Alors* $G_{\mathbf{R}}/G_{\mathbf{Z}}$ *est fermé dans* $\mathscr{R}$.

Il s'agit de prouver que $G_{\mathbf{R}}.\mathbf{GL}(n, \mathbf{Z})$ est fermé dans $\mathbf{GL}(n, \mathbf{R})$. Dans les deux cas envisagés ici, G possède, vu 7.7, 7.9, la propriété :

(P) Il existe une représentation à droite $\pi : \mathbf{GL}(n, \mathbf{C}) \to \mathrm{GL}(V)$ définie sur $\mathbf{Q}$, et un élément $v \in V_{\mathbf{Q}}$ dont le groupe d'isotropie est G.

D'après 7.13, il existe un réseau L de $V_{\mathbf{Q}}$, contenant v et stable par $\mathbf{GL}(n, \mathbf{Z})$, ce qui montre que $v.\mathbf{GL}(n, \mathbf{Z})$ est fermé dans $V_{\mathbf{R}}$. Or $G_{\mathbf{R}}.\mathbf{GL}(n, \mathbf{Z})$ est l'image réciproque de $v.\mathbf{GL}(n, \mathbf{Z})$ dans $\mathbf{GL}(n, \mathbf{R})$ par l'application $g \mapsto v.g$ de $\mathbf{GL}(n, \mathbf{R})$ dans $V_{\mathbf{R}}$; par suite, $G_{\mathbf{R}}.\mathbf{GL}(n, \mathbf{Z})$ est fermé.

8.2. PROPOSITION. *Soient* $G \subset \mathbf{GL}(n, \mathbf{C})$ *un* $\mathbf{Q}$*-groupe algébrique réductif,* Γ *un sous-groupe arithmétique de* G, *et* M *une partie de* $G_{\mathbf{R}}$. *Les assertions suivantes sont équivalentes :*

(i) M *est relativement compact modulo* Γ.

(ii) M *est relativement compact modulo tout sous-groupe arithmétique de* G.

(iii) $|\det g|$ *est borné supérieurement sur* M *et il existe une constante* $c > 0$ *telle que* $\|g(x)\| \geqq c$ *lorsque* $g \in \mathrm{M}$ *et* $x \in \mathbf{Z}^n - \{0\}$.

(iv) $|\det g|$ *est borné supérieurement sur* M; *si* (v_j) *et* (g_j) $(j = 1, 2, \ldots)$ *sont des suites d'éléments d'un réseau* L *de* $\mathbf{Q}^n$ *et de* M *respectivement telles que* $g_j.v_j \to 0$, *lorsque* $j \to \infty$, *alors* $v_j = 0$ *pour* j *assez grand.*

D'après 8.1, l'image de $G_{\mathbf{R}}/G_{\mathbf{Z}}$ dans $\mathscr{R}$ est fermée dans $\mathscr{R}$.

L'équivalence de (i) et (ii) résulte de ce que deux sous-groupes arithmétiques sont commensurables. Nous ramenant au cas où $\Gamma = G_{\mathbf{Z}}$, on voit que (i) équivaut à dire que l'image de M dans $\mathscr{R}$ est relativement compacte. Les assertions (iii) et (iv) ne sont que des traductions du critère de Mahler (1.9), appliqué à M.

8.3. LEMME. *Soient* G *un* $\mathbf{Q}$*-groupe algébrique,* Γ *un sous-groupe arithmétique,*

$$\pi : G \to \mathrm{GL}(V)$$

une représentation de G *définie sur* $\mathbf{Q}$. *Si* $G_{\mathbf{R}}/\Gamma$ *est compact, alors* $\pi(G_{\mathbf{R}}).v$ *est fermée dans* $V_{\mathbf{R}}$ *pour tout* $v \in V_{\mathbf{Q}}$.

Par hypothèse $G_{\mathbf{R}} = C.\Gamma$, où C est compact, d'où $\pi(G_{\mathbf{R}}).v = \pi(C).(\pi(\Gamma).v))$. Il suffit donc de faire voir que $\pi(\Gamma).v$ est fermé; ce qui résulte de 7.13 (1).

Remarque. Ce lemme est en fait conséquence de 7.13 et de la remarque élémentaire suivante. Soient G un groupe localement compact, H un sous-groupe tel que G/H soit compact. Soient M un espace localement compact sur lequel G opère et $m \in M$ un point dont l'orbite par H est fermée. Alors $G.m$ est fermée.
Si H est discret, cela montre en particulier, en faisant agir G sur lui-même par automorphismes intérieurs, que la classe de conjugaison de tout élément de H est fermée dans G.

8.4. THÉORÈME. *Soient* $G \subset \mathbf{GL}(n, \mathbf{C})$ *un* $\mathbf{Q}$*-groupe réductif et* Γ *un sous-groupe arithmétique de* G. *Les assertions suivantes sont équivalentes :*

(i) $G_{\mathbf{R}}/\Gamma$ *est compact;*
(ii) $X(G^0)_{\mathbf{Q}} = \{1\}$, *et tout élément de* $G_{\mathbf{Q}}$ *est semi-simple.*

Montrons tout d'abord que l'on peut se ramener au cas où G est connexe. Le groupe $(G^0)_{\mathbf{R}}$ est ouvert et fermé, invariant, d'indice fini dans $G_{\mathbf{R}}$, donc $(G^0)_{\mathbf{R}}/(\Gamma \cap G^0)$ est ouvert et fermé dans $G_{\mathbf{R}}/\Gamma$, et ce dernier est réunion d'un nombre fini de translatés de $(G^0_{\mathbf{R}})/(\Gamma \cap G^0)$; par suite, (i) pour G équivaut à (i) pour G^0. D'autre part, en caractéristique zéro, un élément d'ordre fini est toujours semi-simple, donc, vu 7.3, si $G_{\mathbf{Q}}$ contient un élément $u \neq 1$ non semi-simple, toute puissance u^m $(m \neq 0)$ de u est non semi-simple; comme $u^m \in G^0$ pour m convenable, il s'ensuit que (ii) pour G est équivalent à (ii) pour G^0.
Nous supposons dorénavant G connexe.
(i) $\Rightarrow$ (ii). Soit $A : G \to \mathbf{GL}(1)$ un caractère défini sur $\mathbf{Q}$ de G et soit $v \in \mathbf{Q}^*$. D'après 8.3, $A(G_{\mathbf{R}}).v$ est fermé dans $\mathbf{R}$; d'autre part, si A est non trivial, cette orbite contient au moins les nombres réels > 0, mais non l'origine, donc n'est pas fermée, d'où $A = 1$.
Si l'on applique 8.3 à la représentation de G obtenue en faisant opérer G sur $\mathbf{M}(n, \mathbf{C})$ par automorphismes intérieurs, on voit que les classes de conjugaison des éléments de $G_{\mathbf{Q}}$ sont fermées. Or, soit $u \in G_{\mathbf{Q}}$ un élément unipotent $\neq 1$. D'après un théorème de Jacobson-Morosow (*voir* p. ex., Jacobson, Lie algebras, *Intersc. Publ.*, New York, 1962, Lemma 7, p. 98), on peut trouver un morphisme $\sigma : \mathbf{SL}_2 \to G$ qui applique $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = u_0$ sur u. La classe de conjugaison de u_0 dans $\mathbf{SL}(2, \mathbf{R})$ contient les matrices :

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} . u_0 . \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} = \begin{pmatrix} 1 & t^2 \\ 0 & 1 \end{pmatrix}$$

donc admet l'élément neutre dans son adhérence. Il en est alors de même pour l'orbite de la classe de conjugaison de u dans $G_{\mathbf{R}}$. Par suite, $G_{\mathbf{Q}}$ ne possède pas d'élément unipotent $\neq 1$, donc est formé d'éléments semi-simples (7.3).
(ii) $\Rightarrow$ (i). Nous considérons tout d'abord le cas où G est de centre réduit à $\{e\}$. Le groupe G est alors semi-simple et, de plus, la représentation adjointe Ad de G dans son algèbre de Lie $\mathfrak{g}$ est fidèle; comme elle est définie sur $\mathbf{Q}$, on peut supposer que Γ est le groupe de stabilité d'un réseau L de $\mathfrak{g}_{\mathbf{Q}}$. Il suffit de faire voir que les

conditions de 8.2 (iv) sont remplies. La première l'est puisque G est semi-simple, donc $|\det g| = 1$ pour tout $g \in G$. Écrivons le polynôme caractéristique de $x \in \mathfrak{g}$ sous la forme :

$$\det(\mathrm{ad}\, x - T.I) = (-T)^n + \sum P_i(x).T^{n-i},$$

où T est une indéterminée. Les $P_i(x)$ sont des polynômes à coefficients rationnels, par rapport à une base de $\mathfrak{g}$ formée d'éléments de L. Soit $P = \sum_i P_i^2$. Si $x \in L - \{0\}$, alors $\mathrm{ad}\, x$ n'est pas nilpotent puisque $\mathfrak{g}_{\mathbf{Q}}$ ne contient pas d'élément nilpotent $\neq 0$, donc $P(x) \neq 0$. Mais P est à coefficients rationnels, et peut s'écrire sous la forme $P'(x).q$, où P' est à coefficients entiers, et $q \in \mathbf{Q}^*$. Il existe donc un nombre $c > 0$ tel que $x \in L - \{0\}$ entraîne $P(x) \geqq c$. Or si (g_j) et (v_j) sont des suites d'éléments de $G_{\mathbf{R}}$ et de L telles que $\mathrm{Ad}\, g_j(v_j) \to 0$, on a :

$$P(v_j) = P(\mathrm{Ad}\, g_j(v_j)) \to 0,$$

ce qui entraîne $v_j = 0$ pour j suffisamment grand.

Nous passons maintenant au cas général. Soit $G^* = G/Z(G)$ le quotient de G par son centre et (cf. 7.13), soit Γ^* un sous-groupe arithmétique de G^* contenant l'image de Γ par la projection canonique π. Montrons que G^* vérifie (ii). Comme $G^{*0} = \pi(G^0)$, il est clair que $X(G^{*0})_{\mathbf{Q}} = \{1\}$. Supposons que $G^*_{\mathbf{Q}}$ contienne un élément $\neq e$ non semi-simple. Alors (7.3), il contient un élément unipotent $\neq e$, donc d'ordre infini, et $G^{*0}_{\mathbf{Q}}$ contient aussi un élément $x \neq e$ unipotent. Ce dernier fait nécessairement partie du groupe dérivé $\mathcal{D}G^{*0} = H$ de G^{*0}, donc $\log x$ est un élément nilpotent de $\mathfrak{h}_{\mathbf{Q}}$. Comme π est une isogénie de $\mathcal{D}G^0$ sur $\mathcal{D}G^{*0}$, il s'ensuit que l'algèbre de Lie de $\mathcal{D}G^0$ contient un élément $x \neq 0$, rationnel sur $\mathbf{Q}$ et nilpotent. Alors $\exp x$ est un élément unipotent $\neq e$ de $G_{\mathbf{Q}}$, ce qui est en contradiction avec l'hypothèse faite sur G.

D'après ce qui a été déjà démontré, le quotient $G^*_{\mathbf{R}}/\Gamma^*$ est compact. Comme l'image de $G_{\mathbf{R}}/\Gamma$ dans $G^*_{\mathbf{R}}/\Gamma^*$ est fermée (7.4), il suffit de montrer que l'application naturelle $G_{\mathbf{R}}/\Gamma \to G^*_{\mathbf{R}}/\Gamma^*$ est propre. Cela résultera de la proposition plus générale suivante :

8.5. PROPOSITION. *Soient* G, G′ *des* $\mathbf{Q}$*-groupes,* $\pi : G \to G'$ *un* $\mathbf{Q}$*-morphisme surjectif. On suppose* G *réductif,* $X(G^0)_{\mathbf{Q}} = 1$ *et* $\ker \pi$ *commutatif. Soient* Γ, Γ' *des sous-groupes arithmétiques de* G *et* G′ *tels que* $\pi(\Gamma) \subset \Gamma'$ *et soit* $D = \pi^{-1}(\Gamma') \cap G_{\mathbf{R}}$. *Alors* D/Γ *est compact, et l'application* $G_{\mathbf{R}}/\Gamma \to G'_{\mathbf{R}}/\Gamma'$ *définie par* π *est propre.*

L'application $G_{\mathbf{R}}/\Gamma \to G'_{\mathbf{R}}/\Gamma'$ se factorise en $G_{\mathbf{R}}/\Gamma \to G_{\mathbf{R}}/D \to G'_{\mathbf{R}}/\Gamma'$. La première de ces applications est une fibration de fibre D/Γ, et est propre si, et seulement si, D/Γ est compacte. La deuxième est une injection sur un ensemble fermé, donc est propre. Comme un composé d'applications propres est propre, on est ramené à faire voir que D/Γ est compact.

Deux sous-groupes arithmétiques d'un $\mathbf{Q}$-groupe étant commensurables, on voit tout de suite que si notre conclusion est vraie pour une paire de groupes arithmétiques, elle l'est pour toute autre paire. De plus, vu que G^0 est d'indice fini dans G, on se ramène immédiatement au cas où G est connexe. Alors $\ker \pi$ est contenu dans le centre C de G et la projection $G \to G/C$ se factorise par π. Soit Γ^* un

sous-groupe arithmétique de $G^* = G/C$ contenant l'image de Γ' (cf. 7.13). On a les applications :

$$G_{\mathbf{R}}/\Gamma \xrightarrow{\alpha} G'_{\mathbf{R}}/\Gamma' \xrightarrow{\beta} G^*_{\mathbf{R}}/\Gamma^*.$$

Pour montrer que α est propre, il suffit de faire voir que $\beta \circ \alpha$ l'est, ce qui nous ramène au cas où $G' = G/C$. Nous devons prouver que D/Γ est compact. Pour cela, considérons un plongement $i : G \to \mathbf{GL}(n, \mathbf{C})$ défini sur $\mathbf{Q}$. Le centre C de G définit une famille commutative d'endomorphismes semi-simples de $\mathbf{C}^n$. Ce dernier est donc un C-module semi-simple, et le commutant A de C dans $\mathbf{M}(n, \mathbf{C})$ est une $\mathbf{C}$-algèbre et un anneau semi-simple, contenant G. Pour tout $g \in G$, désignons par $\beta(g)$ l'automorphisme intérieur $x \mapsto g.x.g^{-1}$ de A. L'application $\beta : g \mapsto \beta(g)$ est un morphisme défini sur $\mathbf{Q}$ de G dans GL(A), dont l'image s'identifie à $G' = G/C$. L'intersection $L = \mathbf{M}(n, \mathbf{Z}) \cap A$ est un ordre de $A_{\mathbf{Q}}$, et en particulier un réseau de $A_{\mathbf{Q}}$. On identifie GL(A) à $\mathbf{GL}(m, \mathbf{C})$ ($m = \dim A$) à l'aide d'une base de L, et on prend pour Γ et Γ' les groupes $G_{\mathbf{Z}}$ et $G'_{\mathbf{Z}}$ respectivement. On a bien $\beta(\Gamma) \subset \Gamma'$; de plus, $D = \{g \in G_{\mathbf{R}}, g.L.g^{-1} = L\}$.

Pour montrer que D/Γ est compact, on appliquera le critère de Mahler à G opérant sur A *par translations à gauche*. On note $\lambda(g)$ la translation à gauche de A définie par $g \in G$. Soit $\mathfrak{R}$ l'espace des réseaux de $A_{\mathbf{R}}$. Comme A contient l'identité, le groupe de stabilité de L dans $G_{\mathbf{R}}$ n'est autre que Γ. Le groupe $X(G)_{\mathbf{Q}}$ est trivial par hypothèse, donc $\det \lambda(g) = 1$ ($g \in G$). Par suite (8.1), $G_{\mathbf{R}}/\Gamma$ est fermé dans $\mathfrak{R}$ et, vu 8.2, il suffit de vérifier que si (x_j) et (g_j) sont des suites d'éléments de L et D respectivement telles que $g_j.x_j \to 0$, alors $x_j = 0$ pour j assez grand.

Pour cela on peut remplacer L par un sous-réseau arbitraire. Or, A est somme directe de ses idéaux bilatères minimaux définis sur $\mathbf{Q}$, et la somme directe des $L \cap A_i = L_i$ est un réseau de $A_{\mathbf{Q}}$ contenu dans L. Il s'ensuit que l'on peut se borner au cas où $\{x_j\}$ est une suite d'éléments de L_i, pour i fixé. Mettons sur $A_{\mathbf{R}}$ la norme :

$$||a|| = \operatorname{tr} {}^t a.a.$$

On a :

$$(1) \qquad ||a.b|| \leqq ||a||.||b||, \qquad ||a.b|| = ||b.a||.$$

Il suffit de faire voir :

(*) Il existe une constante $c > 0$ telle que $||d.x|| \leqq c$ ($d \in D$, $x \in L_i$) entraîne $x = 0$.

D'après le théorème de Hermite (1.8), il existe une constante $c_1 > 0$ telle que :

$$\min_{x \in L_i - \{0\}} ||g.x|| \leqq c_1.|\det g|^{1/n} \qquad (g \in \mathrm{GL}(A_{i,\mathbf{R}}), \quad n = \dim A_i).$$

Comme $\det g = 1$ si $g \in G$, cela montre que, étant donné $d \in D$, on peut trouver un élément $z_d \in L_i - \{0\}$ tel que $||z_d.d^{-1}|| \leqq c_1$. Choisissons une base (y_t) de L_i et soient :

$$c_2 = \min_{x \in L_i - \{0\}} ||x||, \qquad c_3 = \max ||y_t||.$$

Nous voulons montrer maintenant que (*) est vraie pour tout c vérifiant $0 < c < c_2/c_1c_3$. Soient donc $d \in D$ et $x \in L_i$ tels que $||d.x|| \leqq c$. Le réseau L_i étant un ordre de $A_{i,\mathbf{Q}}$, on a $x.y_t.z_d \in L_i$, d'où, par définition de D :

$$d.x.y_t.z_d.d^{-1} \in L \cap A_i = L_i,$$

z_d étant comme plus haut. Vu (1) et les propriétés des c_i, cela entraîne :

$$||d.x.y_t.z_d.d^{-1}|| \leqq ||d.x||\,||y_t||.||z_d.d^{-1}|| < c_2,$$
$$d.x.y_t.z_d.d^{-1} = 0,$$
$$x.y_t.z_d = 0.$$

Cela valant pour tout élément y_t de la base donnée de L_i, il s'ensuit que $x.A_i.z_d.A_i = 0$. Mais z_d est non nul, rationnel sur $\mathbf{Q}$, et A_i est un idéal bilatère minimal sur $\mathbf{Q}$, donc $A_i.z_d.A_i = A_i$, et finalement $x.A_i = 0$, d'où $x = 0$.

8.6. *Exemples.* Nous donnons ici quelques cas classiques de compacité qui résultent de 8.4, mais étaient bien entendu connus avant, et ont en fait suggéré son énoncé.

(1) Soient F une forme quadratique non dégénérée sur un $\mathbf{Q}$-espace vectoriel $V_{\mathbf{Q}}$ et $G = O(F)$ le groupe orthogonal de F. Soit Γ un sous-groupe arithmétique de G, par exemple le groupe des unités d'un réseau L de $V_{\mathbf{Q}}$ (cf. § 5). Alors $G_{\mathbf{R}}/\Gamma$ est compact si, et seulement si, « F ne représente pas zéro rationnellement », c'est-à-dire $F(x) = 0$, $(x \in V_{\mathbf{Q}})$, entraîne $x = 0$.

Pour déduire cette assertion de 8.4, il suffit de montrer que la condition imposée à F équivaut à : $G_{\mathbf{Q}}$ est formé d'éléments semi-simples et $X(G^0)_{\mathbf{Q}} = \{1\}$.

Soit $n = \dim V \geqq 3$. Alors G est semi-simple, donc $X(G^0) = \{1\}$. Soit $g \in G_{\mathbf{Q}}$ unipotent. Il existe donc $v_1 \in V_{\mathbf{Q}} - \{0\}$ fixe par g. Si v_1 n'est pas isotrope, V est somme directe du sous-espace V_1 engendré par v_1 et de son complément orthogonal V_1', qui est stable par g. Il existe donc $v_2 \in V_1' - \{0\}$ fixe par g. En raisonnant par récurrence, on voit ainsi que si F ne représente pas zéro rationnellement, alors $g = 1$, donc (7.3) $G_{\mathbf{Q}}$ est formé d'éléments semi-simples. Réciproquement, si V contient un vecteur isotrope non nul, il est élémentaire que F est équivalente, sur $\mathbf{Q}$, à une forme du type $x.y + F_1$. Le groupe G contient donc un $\mathbf{Q}$-sous-groupe isomorphe sur $\mathbf{Q}$ au groupe orthogonal de la forme $x.y + z^2$, donc au quotient de $\mathbf{SL}_2$ par son centre. Par suite $G_{\mathbf{Q}}$ contient des éléments unipotents $\neq 1$.

Si $n = 2$, alors G^0 est un tore de dimension un, donc $G_{\mathbf{Q}}$ est formé d'éléments semi-simples. On voit facilement que les conditions suivantes sont équivalentes :

(i) F représente zéro rationnellement; (ii) F est équivalente sur $\mathbf{Q}$ à la forme $x.y$; (iii) G^0 est isomorphe sur $\mathbf{Q}$ au groupe multiplicatif $\mathbf{C}^*$; et on verra ou rappellera dans le § 10 que (iii) équivaut à $X(G^0)_{\mathbf{Q}} \neq \{1\}$.

(2) Soit k un corps de nombres de degré d sur $\mathbf{Q}$. Soient G' le tore associé à k (cf. § 7), G le groupe des éléments de norme 1 de G', et Γ le groupe des unités de k.

On voit facilement que $X(G)_{\mathbf{Q}} = \{1\}$. Comme $G_{\mathbf{Q}}$ s'identifie à k^*, il est formé d'éléments semi-simples, donc (théor. 8.4), $G_{\mathbf{R}}/\Gamma$ est compact.

D'autre part, on vérifie que $G'_{\mathbf{R}} = (\mathbf{R}^*)^{r_1} \times (\mathbf{C}^*)^{r_2}$, où r_1 (resp. r_2) est le nombre d'isomorphismes distincts de k dans $\mathbf{R}$ (resp. le nombre de paires d'isomorphismes complexes conjugués de k dans $\mathbf{C}$), donc que $G_{\mathbf{R}}$ est isomorphe, en tant que groupe de Lie réel, au produit $\mathbf{R}^{r_1+r_2-1} \times \mathbf{SO}(2)^{r_2}$. La compacité de $G_{\mathbf{R}}/\Gamma$ signifie donc que, modulo torsion, Γ est un groupe commutatif libre à $r_1 + r_2 - 1$ générateurs, ce qui est la partie essentielle du théorème des unités de Dirichlet.

(3) Soient G' le groupe des éléments inversibles de $A_{\mathbf{C}}$, où A est une $\mathbf{Q}$-algèbre de dimension finie, Γ le groupe des unités d'un réseau de $A_{\mathbf{Q}}$ et soit G le groupe des éléments de norme réduite 1 (cf. § 7).
On vérifie que $A_{\mathbf{Q}}$ est une algèbre à division, si, et seulement si, $G_{\mathbf{Q}}$ est formé d'éléments semi-simples et $X(G)_{\mathbf{Q}} = \{1\}$. Par conséquent, si $A_{\mathbf{Q}}$ est une algèbre à division, $G_{\mathbf{R}}/\Gamma$ est compact (Théor. de Fräulein Hey):

8.7. THÉORÈME. *Soient* G *un* $\mathbf{Q}$*-groupe et* Γ *un sous-groupe arithmétique de* G. *Alors les conditions suivantes sont équivalentes :*

(i) $G_{\mathbf{R}}/\Gamma$ *est compact,*
(ii) $X(G^0)_{\mathbf{Q}} = \{1\}$, *et tout élément unipotent de* $G_{\mathbf{Q}}$ *fait partie du radical unipotent* (7.15) *de* G.

(a) G est unipotent. Alors (ii) est toujours vérifiée (pour la première partie, cela résulte de 7.3), et on a à montrer que $G_{\mathbf{R}}/\Gamma$ est compact. Vu 8.1 et 8.2, il suffit de faire voir que si $\pi : G \to GL(V)$ est un $\mathbf{Q}$-morphisme, L un réseau de $V_{\mathbf{Q}}$ et (g_j), (v_j) des suites d'éléments de $G_{\mathbf{R}}$ et L vérifiant $\pi(g_j).v_j \to 0$, alors $v_j = 0$ pour j assez grand.
Pour cela on procède par récurrence sur dim V. Dans toute $\mathbf{Q}$-représentation, le groupe G, étant unipotent, admet un vecteur fixe $\neq 0$, rationnel sur $\mathbf{Q}$. En particulier, il existe sur V une forme linéaire $\lambda \neq 0$, définie sur $\mathbf{Q}$, invariante par G. De $\lambda(\pi(g_j).v_j) \to 0$, on déduit alors que $v_j \in \ker \lambda$, donc que v_j fait partie d'un $\mathbf{Q}$-sous-espace propre de V stable par G, pour j assez grand. On peut alors appliquer l'hypothèse de récurrence.
(b) Cas général. On peut écrire $G = H.N$ où H est un $\mathbf{Q}$-groupe réductif et N est un $\mathbf{Q}$-sous-groupe normal connexe unipotent (7.15). Vu 7.13, on peut prendre comme groupe arithmétique un produit semi-direct $\Gamma = \Gamma_1.\Gamma_2$, où Γ_1 (resp. Γ_2) est un groupe arithmétique de H (resp. N). On a vu que $N_{\mathbf{R}}/\Gamma_2$ est compact. Il est alors immédiat que $G_{\mathbf{R}}/\Gamma$ est compact si, et seulement si, $H_{\mathbf{R}}/\Gamma_1$ l'est. D'autre part, $X(N) = \{1\}$, donc $X(G^0) = X(H^0)$ ce qui, compte tenu de 7.3, montre que (ii) pour G équivaut à (ii) pour H. On est ramené à 8.4.

8.8. *Remarque.* La démonstration de 8.4 est remarquablement simple lorsque G est de centre réduit à l'élément neutre. Le raisonnement fait dans ce cas s'étendrait facilement au cas général si l'une quelconque des quatre assertions suivantes était vraie, pour $k = \mathbf{Q}$.
Soient k un corps parfait et G un k-groupe réductif connexe tel que $X(G)_k = \{1\}$ et dont les éléments rationnels sur k sont semi-simples. Alors :

(a) Il existe une k-représentation fidèle $\pi : G \to GL(V)$ telle que l'orbite $\pi(G).v$ de tout élément de V_k n'admette pas l'origine dans son adhérence (en topologie de Zariski);
(b) Il existe une k-représentation fidèle $\pi : G \to GL(V)$ telle que $\pi(G).v$ soit fermée, quel que soit $v \in V_k$;
(c) Pour toute k-représentation $\pi : G \to GL(V)$, et tout $v \in V_k - \{0\}$ l'orbite $\pi(G).v$ n'est pas adhérente à l'origine;

(d) Pour toute k-représentation $\pi : G \to GL(V)$ et tout $v \in V_k$, l'orbite $\pi(G).v$ est fermée.

Je ne sais pas si ces assertions sont vraies, même lorsque $k = \mathbf{Q}$. Par ailleurs, la question peut se poser aussi pour un corps non parfait, en remplaçant l'hypothèse faite sur G par : G est anisotrope sur k (cf. § 10). Des exemples montrent que *(c)* et *(d)* sont inexactes dans ce cas.

Montrons comment *(a)* pour $k = \mathbf{Q}$ entraînerait 8.4. Soient P_i $(1 \leqq i \leqq m)$ des polynômes homogènes à coefficients rationnels sur V, invariants par G, et qui engendrent l'anneau J des invariants de G (7.6), et soit $P = \sum_i P_i^2$. Comme les polynômes invariants séparent les ensembles fermés stables disjoints (7.6), la condition imposée à π entraîne que $P(x) \neq 0$ si $x \in V_{\mathbf{Q}} - \{0\}$. Par suite, étant donné un réseau L de $V_{\mathbf{Q}}$, il existe une constante $c > 0$ telle que $P(x) \geqq c$ pour $x \in L - \{0\}$. Si $(g_j) \in G_{\mathbf{R}}$ et $(v_j) \in L$ $(j = 1, 2, \ldots)$ sont tels que $\pi(g_j).v_j \to 0$, on a alors $P(\pi(g_j).v_j) = P(v_j) \to 0$, donc $v_j = 0$ pour j assez grand, et le critère de Mahler est vérifié.

Nous terminons ce paragraphe en démontrant, à l'aide de 8.5, un théorème sur les isogénies de $\mathbf{Q}$-groupes.

8.9. THÉORÈME. *Soient* G, G′ *des* $\mathbf{Q}$*-groupes,* $r : G \to G'$ *une isogénie définie sur* $\mathbf{Q}$ *et* Γ *un groupe arithmétique de* G. *Alors* $r(\Gamma)$ *est un groupe arithmétique de* G′.

Il est clair qu'il suffit de considérer le cas où G est connexe. On peut trouver (7.13) un sous-groupe arithmétique Γ' de G′ contenant $r(\Gamma)$, et nous devons montrer que $r(\Gamma)$ est d'indice fini dans Γ'.

Supposons tout d'abord G réductif et $X(G)_{\mathbf{Q}} = \{1\}$. D'après 8.5, le quotient $(r^{-1}(\Gamma') \cap G_{\mathbf{R}})/\Gamma$ est compact. Le noyau de r étant fini, le groupe $r^{-1}(\Gamma')$ est discret, le quotient précédent est en fait fini, et $r(\Gamma)$ est d'indice fini dans :

$$H = r(r^{-1}(\Gamma) \cap G_{\mathbf{R}}).$$

Mais, comme $r(G_{\mathbf{R}})$ est d'indice fini dans $G'_{\mathbf{R}}$ (7.4), il est clair que H est d'indice fini dans Γ'. Soit maintenant G réductif. Posons :

$$G_1 = \Big(\bigcap_{\chi \in X(G)_{\mathbf{Q}}} \ker \chi\Big)^0, \qquad G'_1 = \Big(\bigcap_{\chi \in X(G')_{\mathbf{Q}}} \ker \chi\Big)^0.$$

Pour tout caractère $\chi \in X(G)_{\mathbf{Q}}$ on a $\chi(G_{\mathbf{Z}}) = \pm 1$, donc $G_1 \cap \Gamma$ est d'indice fini dans Γ, et de même $G'_1 \cap \Gamma'$ est d'indice fini dans Γ'. D'autre part, il résulte de faits élémentaires sur les caractères, qui seront rappelés ou démontrés dans le § 10, que $r(G_1) = G'_1$ et $X(G_1)_{\mathbf{Q}} = \{1\}$. On est donc ramené au premier cas considéré.

Dans le cas général, on a la décomposition $G = H.N$, avec H réductif, N unipotent distingué, de 7.15 et l'on peut supposer que $\Gamma = \Gamma_1.\Gamma_2$ est le produit semi-direct d'un groupe arithmétique Γ_1 de H et d'un groupe arithmétique Γ_2 de N (7.13). Le groupe G′ est le produit semi-direct de $H' = r(H)$ et de $N' = r(N)$. D'après ce qui a été déjà démontré, $r(\Gamma_1)$ est un sous-groupe arithmétique de H′. D'autre part, $\ker r \cap N = \{e\}$, puisque $\ker r$ est fini, donc r est un isomorphisme de N sur N′, et, vu 7.13, $r(\Gamma_2)$ est un sous-groupe arithmétique de N′. Alors (7.13), $r(\Gamma) = r(\Gamma_1).r(\Gamma_2)$ est un sous-groupe arithmétique de G′.

8.10. COROLLAIRE. *Supposons que* G *soit le produit presque direct de* **Q***-sous-groupes distingués* G_i $(1 \leqq i \leqq m)$. *Alors* Γ *est commensurable au groupe* Γ' *engendré par les intersections* $\Gamma_i = \Gamma \cap G_i$ *et* Γ_i *est arithmétique dans* G_i $(1 \leqq i \leqq m)$.

Il suffit de considérer le cas où $G \subset \mathbf{GL}_n$ et $\Gamma = G_{\mathbf{Z}}$. Alors $\Gamma_i = G_{i\mathbf{Z}}$, donc Γ_i est arithmétique. L'application produit ν des inclusions $G_i \to G$ est une **Q**-isogénie de $G_1 \times \ldots \times G_m$ sur G, donc $\Gamma' = \nu(G_{1\mathbf{Z}} \times \ldots \times G_{m\mathbf{Z}})$ est arithmétique d'après 8.9, et est par suite commensurable à Γ.

8.11. *Remarque.* Le théorème 8.9 s'étend facilement au cas d'un **Q**-morphisme surjectif r, [4]. Nous nous bornons ici à indiquer la démonstration lorsque G est réductif connexe. Soit N la composante neutre du noyau de r. C'est un **Q**-sous-groupe distingué. Comme G est réductif, il existe un **Q**-sous-groupe distingué connexe N′ de G tel que G soit produit presque direct de N et N′. D'après 8.10, Γ est commensurable à $(N \cap \Gamma).(N' \cap \Gamma)$ et $N' \cap \Gamma$ est arithmétique dans N′. Le groupe $r(\Gamma)$ est commensurable à $r(N' \cap \Gamma)$. Comme la restriction de r à N′ est une **Q**-isogénie de N′ sur G′, $r(N' \cap \Gamma)$ est arithmétique (8.9), donc $r(\Gamma)$ est arithmétique.

Note bibliographique

On a déjà mentionné en 8.6 deux antécédents du critère de compacité : l'un est le théorème des unités de Dirichlet et sa généralisation aux algèbres à division; l'autre concerne les groupes d'unités de formes quadratiques ou hermitiennes qui ne représentent pas zéro rationnellement, dont on trouve des exemples déjà dans Fricke-Klein [11], puis dans les travaux de Siegel (par exemple [30]) et de ses élèves. Un théorème général sur les algèbres à involution, qui englobe les cas classiques, se trouve dans [32].

L'énoncé de 8.4 a été conjecturé par R. Godement, et prouvé dans [5], puis dans [21]. C'est cette dernière démonstration qui a été exposée ici. Dans ces deux articles, on considère aussi le cas général de 8.5. Le théorème 8.9 est prouvé, d'une autre manière, dans [5, § 6.11].

§ 9. Ensembles fondamentaux (premier type)

9.1. DÉFINITION. On dit qu'un sous-groupe G de $\mathbf{GL}(n, \mathbf{R})$ est auto-adjoint par rapport à une forme bilinéaire symétrique positive non dégénérée Q sur $\mathbf{R}^n$ si, pour tout $g \in G$, l'adjoint de g par rapport à Q est encore dans G. En particulier si Q est la forme unité, on dira simplement auto-adjoint.

L'adjoint d'un élément a de $\mathbf{GL}(n, \mathbf{R})$ par rapport à la forme unité est le transposé ${}^t a$ de a.

9.2. PROPOSITION. *Soit* G *un sous-groupe algébrique semi-simple de* $\mathbf{GL}(n, \mathbf{R})$ *défini sur* **R**. *Il existe un élément* $u \in \mathbf{GL}(n, \mathbf{R})$ *tel que* $uG_{\mathbf{R}}u^{-1}$ *soit auto-adjoint.*

Il revient au même de prouver que $G_{\mathbf{R}}$ est auto-adjoint par rapport à une forme positive non dégénérée convenable. La démonstration sera précédée de deux lemmes.

9.3. LEMME. *Soient* H *un sous-groupe auto-adjoint de* $\mathbf{GL}(n, \mathbf{R})$ *et* M *un sous-groupe algébrique de* $\mathbf{GL}(n, \mathbf{R})$ *défini sur* $\mathbf{R}$ *tel que* H *soit d'indice fini dans* $M_{\mathbf{R}}$. *Alors* $H = K.P$ *où* $K = \mathbf{O}(n) \cap H$ *et* $P = S \cap H$, S *désignant l'espace des matrices symétriques positives non dégénérées. On a* $P = \exp \mathfrak{p}$ *où* $\mathfrak{p}$ *est l'intersection de l'algèbre de Lie* $\mathfrak{h}$ *de* H *avec l'espace* $\mathfrak{s}$ *des matrices symétriques, et* K *est un sous-groupe compact maximal de* H.

Rappelons que $\mathfrak{gl}(n, \mathbf{R})$ se décompose en la somme directe de l'algèbre de Lie de $\mathbf{O}(n)$ et de $\mathfrak{s}$, que $\mathbf{GL}(n, \mathbf{R}) = \mathbf{O}(n).S$, tout $g \in \mathbf{GL}(n, \mathbf{R})$ s'écrivant de manière unique comme produit d'un élément de $\mathbf{O}(n)$ et d'un élément de S, dépendant continûment de g, et enfin que l'exponentielle définit un homéomorphisme de $\mathfrak{s}$ sur S. D'autre part, tout sous-groupe de S relativement compact est réduit à $\{e\}$. Le lemme 9.3 se ramène donc à l'assertion suivante : si $g = k.s$ est un élément de H ($k \in \mathbf{O}(n)$, $s \in S$) alors $s \in H$ et $s = \exp X$, $X \in \mathfrak{p}$. Or ${}^t g = s.k^{-1}$, et $s^2 = g.{}^t g$ est donc un élément de H par hypothèse. Plus généralement pour tout entier n, $s^{2^n} \in H$. On peut écrire $s = \exp X$ où $X \in \mathfrak{s}$. Montrons que pour $t \in \mathbf{R}$, $\exp tX$ est dans M. Comme M est défini par des équations polynômes et que s peut être supposé diagonal, on voit que l'on est ramené à l'assertion suivante (qui est immédiate) : si P est un polynôme à r variables, la relation :

$$P(e^{nx_1}, e^{nx_2}, \ldots, e^{nx_r}) = 0 \qquad (n \in \mathbf{Z})$$

entraîne :

$$P(e^{tx_1}, e^{tx_2}, \ldots, e^{tx_r}) = 0 \qquad (t \in \mathbf{R}).$$

Ainsi $\exp tX$ appartient à M donc à $M_{\mathbf{R}}$ pour tout $t \in \mathbf{R}$. Comme H est d'indice fini dans $M_{\mathbf{R}}$, $\exp tX \in H$, d'où $X \in \mathfrak{h}$. Enfin, soit L est un sous-groupe compact de $G_{\mathbf{R}}$. Alors un élément x de $L \cap P$ est semi-simple, de valeurs propres réelles, positives de module un, donc $x = e$, et $L \cap P = \{e\}$. Par conséquent, K est compact maximal.

9.4. LEMME. *Il existe un* $u \in \mathbf{GL}(n, \mathbf{R})$ *tel que* $u.G_{\mathbf{R}}^0.u^{-1}$ *soit auto-adjoint.*

Soit en effet $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$ une décomposition de Cartan de l'algèbre de Lie $\mathfrak{g}$ de G.
La forme compacte $\mathfrak{k} + i\mathfrak{p}$ engendre dans $\mathbf{GL}(n, \mathbf{C})$ un groupe compact qui est conjugué à un groupe unitaire. On voit donc qu'après conjugaison, on peut supposer que l'on a :

$$\mathfrak{k} \subset \mathfrak{o}(n) \qquad \text{et} \qquad \mathfrak{p} \subset \mathfrak{s}.$$

Le groupe $G_{\mathbf{R}}^0$ est engendré par $\exp \mathfrak{k}$ et $\exp \mathfrak{p}$; il est donc auto-adjoint.

9.5. *Démonstration de* 9.2. D'après 9.3 et 9.4, on peut supposer, quitte à remplacer $G_{\mathbf{R}}$ par un conjugué, que $G_{\mathbf{R}}^0 = K.P$ où K est le groupe engendré par $\mathfrak{k} = \mathfrak{o}(n) \cap \mathfrak{g}$, et $P = \exp \mathfrak{p}$, $(\mathfrak{p} = \mathfrak{g} \cap \mathfrak{s})$.

Montrons que K est son groupe normalisateur dans $G_{\mathbf{R}}^0$. Il suffit de faire voir que $P \cap \mathrm{Norm}(K) = \{e\}$. Soient $p \in P \cap \mathrm{Norm}(K)$ et $k \in K$; alors :

$$k.p = p.k' = k'.k'^{-1}.p.k' \qquad (k' \in K)$$

d'où $k = k'$ et $p = k'^{-1}.p.k'$. Ainsi p centralise K. L'unique élément $X \in \mathfrak{p}$ tel que $p = \exp X$ fait alors partie du centralisateur de $\mathfrak{k}$. Mais on sait que $\mathfrak{k}$ est son propre normalisateur dans $\mathfrak{g}$ d'où $X = 0$ et $p = e$.
Désignons par K' le normalisateur de K dans $G_{\mathbf{R}}$. On a donc $K' \cap G_{\mathbf{R}}^0 = K$. Comme les décompositions de Cartan de $\mathfrak{g}$ sont conjuguées par automorphismes intérieurs de $G_{\mathbf{R}}^0$, on a $G_{\mathbf{R}} = K'.G_{\mathbf{R}}^0 = K'.P$. Il s'ensuit que :

$$K'/K = K'/(K' \cap G_{\mathbf{R}}^0) = G_{\mathbf{R}}/G_{\mathbf{R}}^0$$

est fini et que K' est compact. Soit Q la moyenne des transformées de la forme unité par K'/K. C'est une forme symétrique positive non dégénérée invariante par K'. D'autre part, K' normalise $\mathfrak{p}$ (qui est le complément orthogonal de $\mathfrak{k}$ par rapport à la forme de Killing), donc aussi P. Les éléments de P sont donc auto-adjoints par rapport à Q. Comme $G_{\mathbf{R}} = K'.P$, la proposition 9.2 est démontrée.

9.6. DÉFINITION. Soient G un groupe algébrique défini sur $\mathbf{Q}$, Γ un sous-groupe arithmétique de G. On dit qu'un ensemble $\Omega \subset G_{\mathbf{R}}$ est fondamental pour Γ s'il vérifie les conditions suivantes :

(F_0) $K.\Omega = \Omega$ pour un sous-groupe compact maximal K convenable de $G_{\mathbf{R}}$;
(F_1) $\Omega.\Gamma = G_{\mathbf{R}}$;
(F_2) Pour tout b de $G_{\mathbf{Q}}$ l'ensemble des γ de Γ tels que $\Omega.b \cap \Omega.\gamma$ est non vide, est fini (« Propriété de Siegel »).

Par exemple les domaines de Siegel assez grands sont des ensembles fondamentaux pour $\Gamma = \mathbf{GL}(n, \mathbf{Z})$ dans $\mathbf{GL}(n, \mathbf{R})$ (cf. §§ 1 et 4).

9.7. *Remarques.* (1) La propriété (F_2) est équivalente à la propriété apparemment plus forte :

(F_2)' Soit C une partie finie de $G_{\mathbf{Q}}$. L'ensemble des $\gamma \in \Gamma$ tels que :

$$\Omega.C \cap \Omega.C.\gamma \neq \varnothing$$

est fini.

En effet, soit $\Gamma' = \Gamma \cap \left(\bigcap_{c \in C} c^{-1}.\Gamma.c \right)$. Ce groupe vérifie $\Gamma'.C^{-1} \subset C^{-1}.\Gamma$ et, vu 7.13, est arithmétique, donc d'indice fini dans Γ. Soit D une partie finie de Γ telle que $\Gamma = D.\Gamma'$. Si $\gamma = d.\gamma'$ ($d \in D$, $\gamma' \in \Gamma'$) et $c_1, c_2 \in C$ sont tels que $\Omega c_1 \cap \Omega.c_2.d.\gamma' \neq \varnothing$, alors on a :

$$\Omega\gamma_1^{-1} \cap \Omega c_2.d.c_1^{-1}. \neq \varnothing \qquad (\gamma_1 = c_1.\gamma'.c_1^{-1} \in \Gamma).$$

Si Ω vérifie (F_2), il n'y a alors qu'un nombre fini de possibilités pour γ_1, d'où (F_2)'.
(2) Une des raisons pour laquelle on impose (F_2) pour tout $b \in G_{\mathbf{Q}}$, et non pas seulement pour $b = e$, est que l'existence d'un ensemble fondamental pour *un* groupe arithmétique de G implique son existence pour tout groupe arithmétique

de G. Pour le voir, il suffit de montrer que si $\Gamma \subset \Gamma'$ sont deux groupes arithmétiques, alors Γ possède un ensemble fondamental si, et seulement si, Γ' en a un.
Soit Ω un ensemble fondamental pour Γ. Il vérifie *a fortiori* (F_0) et (F_1) pour Γ'. Il existe une partie finie C de $G_{\mathbf{Q}}$ telle que $\Gamma' = C.\Gamma$. Si $\gamma' = c.\gamma$ $(c \in C,\ \gamma \in \Gamma)$ est tel que $\Omega.b \cap \Omega\gamma' \neq \emptyset$, alors $\Omega b \cap \Omega C\gamma \neq \emptyset$, donc γ varie dans un ensemble fini (cf. (1)).
Réciproquement, soit Ω' fondamental pour Γ', et soit $\Omega = \Omega'.C$. Il vérifie (F_0) et (F_1) pour Γ. Vu (1), il vérifie (F_2) pour Γ', donc *a fortiori* pour Γ.

9.8. THÉORÈME. *Soient* G *un* $\mathbf{Q}$*-groupe algébrique semi-simple de* $\mathbf{GL}(n, \mathbf{C})$, Γ *un groupe arithmétique de* G *et* $\mathfrak{S}$ *un ensemble de Siegel standard dans* $\mathbf{GL}(n, \mathbf{R})$ *fondamental pour* $\mathbf{GL}(n, \mathbf{Z})$. *Soit* $u \in \mathbf{GL}(n, \mathbf{R})$ *tel que* $u.G_{\mathbf{R}}.u^{-1}$ *soit auto-adjoint* (9.2). *Alors il existe une partie finie* $B \subset \mathbf{GL}(n, \mathbf{Z})$ *telle que* $\Omega = \bigcap_{b \in B} (u^{-1}.\mathfrak{S}.b) \cap G_{\mathbf{R}}$ *soit un ensemble fondamental pour* Γ *dans* $G_{\mathbf{R}}$.

On peut supposer (cf. remarque précédente) que $\Gamma = G_{\mathbf{Z}}$. On peut trouver une représentation à droite définie sur $\mathbf{Q}$ de $\mathbf{GL}(n, \mathbf{C})$ dans un espace vectoriel V, un réseau L de $V_{\mathbf{Q}}$ stable par $\mathbf{GL}(n, \mathbf{Z})$, un point $v \in L$ tels que $v.\mathbf{GL}(n, \mathbf{R})$ soit fermé et que le groupe d'isotropie de v dans $\mathbf{GL}(n, \mathbf{R})$ soit $G_{\mathbf{R}}$ (cf. § 7).
Alors $v' = vu^{-1}$ admet $uG_{\mathbf{R}}u^{-1}$ comme groupe d'isotropie. D'après le lemme de finitude du paragraphe 6, l'ensemble $(v'.\mathfrak{S}) \cap L$ est *fini*. (La condition de diagonalisation (iii) de ce lemme est vérifiée puisque ρ est définie sur $\mathbf{Q}$.) *A fortiori*, $(v'.\mathfrak{S}) \cap (v.\mathbf{GL}(n, \mathbf{Z}))$ est un ensemble fini. Soient $v.b_1^{-1}, \ldots, v.b_m^{-1}$ les points de cet ensemble $(b_i \in \mathbf{GL}(n, \mathbf{Z}))$. Posons $H = u.G_{\mathbf{R}}$. C'est évidemment l'ensemble des $g \in \mathbf{GL}(n, \mathbf{R})$ tels que $v'.g = v$.
Tout $h \in H$ s'écrit $h = s.b$ où $s \in \mathfrak{S}$ et $b \in \mathbf{GL}(n, \mathbf{Z})$. De $v'.s.b = v$, on tire $v'.s = v.b^{-1}$. Ceci est donc un élément de $(v'\,\mathfrak{S}) \cap (v.\mathbf{GL}(n, \mathbf{Z}))$ et il existe i tel que :

$$v'.s = v.b_i^{-1}.$$

Alors $v.b_i^{-1}.b = v$, de sorte que $b_i^{-1}.b$ est dans $G_{\mathbf{R}} \cap \mathbf{GL}(n, \mathbf{Z})$, donc $b \in b_i.G_{\mathbf{Z}}$. Finalement :

$$H \subset \bigcup_i \mathfrak{S} b_i G_{\mathbf{Z}}$$

$$G_{\mathbf{R}} = u^{-1}.H \subset \left(\bigcup_i u^{-1}\mathfrak{S}b_i\right).G_{\mathbf{Z}}.$$

Posons $\Omega = \bigcup_i (u^{-1}\mathfrak{S}b_i \cap G_{\mathbf{R}})$.
On va prouver que Ω est dans $G_{\mathbf{R}}$ un ensemble fondamental pour $G_{\mathbf{Z}}$. On a déjà vu que Ω vérifie (F_1).
Prouvons (F_0). D'après la proposition 9.2, $u.G_{\mathbf{R}}.u^{-1}$ admet un sous-groupe compact maximal K' contenu dans $\mathbf{O}(n)$. En particulier, $K'.\mathfrak{S} = \mathfrak{S}$. Alors $K_1 = u^{-1}K'u$ est un sous-groupe compact maximal de $G_{\mathbf{R}}$ et qui vérifie (F_0).
Reste (F_2). Si $\Omega.b \cap \Omega.\gamma \neq \emptyset$, on peut trouver des indices i et j, tels que :

$$u^{-1}\mathfrak{S}.b_i.b \cap u^{-1}.\mathfrak{S}.b_j.\gamma \neq \emptyset,$$

soit encore :

$$\mathfrak{S} \cap \mathfrak{S}.b_j.\gamma.b^{-1}.b_i^{-1} \neq \emptyset.$$

Une variante immédiate du corollaire du théorème de Siegel (cf. § 4) montre que l'ensemble des γ vérifiant cette relation est fini, d'où le résultat.

9.9. *Remarque.* La proposition 9.2 est en fait valable pour tout $\mathbf{Q}$-groupe réductif. En admettant cela, on voit que le théorème et sa démonstration subsistent sans changement lorsque G est un $\mathbf{Q}$-groupe réductif. En utilisant 7.15, on passe sans difficulté de là au cas d'un $\mathbf{Q}$-groupe quelconque. En effet, si $G = H.N$ (H réductif, N unipotent distingué, H, N définis sur $\mathbf{Q}$), alors on peut prendre pour Γ le produit semi-direct $\Gamma = \Gamma_1.\Gamma_2$ d'un groupe arithmétique Γ_1 de H par un groupe arithmétique Γ_2 de N.
Soient Ω_1 un ensemble fondamental pour Γ_1 dans $H_{\mathbf{R}}$, K un sous-groupe compact maximal de $H_{\mathbf{R}}$ tel que $K.\Omega_1 = \Omega_1$, et (8.7), Ω_2 un compact de $N_{\mathbf{R}}$ tel que $N_{\mathbf{R}} = \Omega_2.\Gamma_2$. Montrons que $\Omega = \Omega_1.\Omega_2$ est un ensemble fondamental pour Γ. Le groupe $N_{\mathbf{R}}$ est homéomorphe à un espace euclidien, donc K est aussi compact maximal dans $G_{\mathbf{R}}$, d'où (F_0). On a :

$$G_{\mathbf{R}} = H_{\mathbf{R}}.N_{\mathbf{R}} = \Omega_1.\Gamma_1.N_{\mathbf{R}} = \Omega_1.N_{\mathbf{R}}.\Gamma_1 = \Omega_1.\Omega_2.\Gamma_2.\Gamma_1 = \Omega.\Gamma,$$

d'où (F_1). Soit $b \in G_{\mathbf{Q}}$ et soit $\gamma \in \Gamma$ tel que $\Omega.b \cap \Omega.\gamma \neq \emptyset$.
On peut écrire de façon unique :

$$b = h.n \qquad (h \in H_{\mathbf{Q}}, \quad n \in N_{\mathbf{Q}}), \qquad \gamma = \gamma_1.\gamma_2 \qquad (\gamma_1 \in \Gamma_1, \quad \gamma_2 \in \Gamma_2).$$

On a alors :

$$(1) \qquad \Omega_1.h.(h^{-1}.\Omega_2.h).n \cap \Omega_1.\gamma_1.(\gamma_1^{-1}.\Omega_2.\gamma_1).\gamma_2 \neq \emptyset,$$

d'où :

$$(2) \qquad \Omega_1.h \cap \Omega_1.\gamma_1 \neq \emptyset,$$

$$(3) \qquad h^{-1}.\Omega_2.h.n \cap (\gamma_1^{-1}.\Omega_2.\gamma_1).\gamma_2 \neq \emptyset.$$

La condition (F_2) pour H, et (2), montrent qu'il n'y a qu'un nombre fini de valeurs possibles pour γ_1. La relation (3) implique alors que γ_2 fait partie d'un compact ne dépendant que de b et Ω, d'où notre assertion.
On verra plus loin que Ω est de volume invariant fini lorsque G est semi-simple ou, plus généralement, lorsque $X(G^0)_{\mathbf{Q}} = \{1\}$.

9.10. Soit $X = K\backslash G_{\mathbf{R}}$. Le groupe Γ opère proprement sur X par translations à droite. Une partie Ω' de X est dite un ensemble fondamental pour Γ si elle vérifie la condition :

(F_1) $\Omega.\Gamma = X$,

et la condition (F_2) de 9.6. Il est clair que la projection naturelle de l'ensemble fondamental Ω pour Γ dans $G_{\mathbf{R}}$ de 9.8 vérifie ces conditions. On sait que l'espace X est connexe et simplement connexe (en fait, il est homéomorphe à un espace euclidien). Il s'ensuit, par un raisonnement topologique familier, que l'image Γ' de Γ dans le groupe des homéomorphismes de X est de présentation finie. On voit aussi, comme en 4.8, que les sous-groupes d'ordre fini de Γ' forment un nombre fini de classes de conjugaison. On en déduit ensuite aisément que ces propriétés sont vraies pour tout groupe arithmétique [3].

9.11. Pour compléter, nous indiquerons encore une généralisation du théorème de finitude de 6.4. Outre le résultat mentionné en 7.10 (i), elle utilise (pour $k = 2$) la généralisation suivante de 9.2 :

« *Soient* $G_1 \supset G_2 \supset \ldots \supset G_k$ *des* $\mathbf{R}$*-sous-groupes réductifs de* $\mathbf{GL}(n, \mathbf{C})$. *Alors il existe* $u \in \mathbf{GL}(n, \mathbf{R})$ *tel que les groupes* $u.G_{i\mathbf{R}}.u^{-1}$ *soient auto-adjoints* $(1 \leqq i \leqq k)$.

THÉORÈME. *Soient* G *un* $\mathbf{Q}$*-groupe réductif,* Γ *un sous-groupe arithmétique de* G. *Soient* $\pi : G \to GL(V)$ *un* $\mathbf{Q}$*-morphisme et* L *un réseau de* $V_{\mathbf{Q}}$ *stable par* Γ. *Soit* $v \in V$ *un point dont l'orbite* $X = G.v$ *par* G *est fermée. Alors* $L \cap X$ *est formée d'un nombre fini d'orbites de* Γ.

On suppose G plongé dans $\mathbf{GL}(n, \mathbf{C})$ de manière à ce que Γ soit contenu dans $\mathbf{GL}(n, \mathbf{Z})$, (7.13).

Soit H le groupe d'isotropie de v. Il est défini sur $\mathbf{Q}$. Comme G/H s'identifie à une variété affine, H est réductif (7.10 (i)). Il existe donc un $\mathbf{Q}$-morphisme :

$$\sigma : \mathbf{GL}(n, \mathbf{C}) \to GL(W),$$

et un point $w \in W_{\mathbf{Q}}$ tels que le groupe d'isotropie de w dans $\mathbf{GL}(n, \mathbf{C})$ soit H et que $\sigma(\mathbf{GL}(n, \mathbf{C}))$ soit fermé (7.7).

Soit M un réseau de $W_{\mathbf{Q}}$ stable par $\mathbf{GL}(n, \mathbf{Z})$. Montrons que $M \cap G.w$ est formé d'un nombre fini d'orbites de Γ. On peut supposer $\Gamma = G_{\mathbf{Z}}$. Soit $u \in \mathbf{GL}(n, \mathbf{R})$ tel que $u.G_{\mathbf{R}}.u^{-1}$ et $u.H_{\mathbf{R}}.u^{-1}$ soient auto-adjoints. On peut trouver un ensemble de Siegel $\mathfrak{S}$ de $\mathbf{GL}(n, \mathbf{R})$ et une partie finie C de $\mathbf{GL}(n, \mathbf{Z})$ tels que $G_{\mathbf{R}} \subset \Omega.\Gamma$, avec $\Omega = u^{-1}.\mathfrak{S}.C$. Il suffit donc de montrer que $M \cap w.G_{\mathbf{R}}$ est fini et pour cela, on peut se borner à faire voir que $w.u^{-1}.\mathfrak{S} \cap M$ est fini. Or soit $w' = w.u^{-1}$. Son groupe d'isotropie $u.H_{\mathbf{R}}.u^{-1}$ dans $\mathbf{GL}(n, \mathbf{R})$ est auto-adjoint, donc on peut appliquer 6.2.

Pour terminer la démonstration du théorème, il suffit de montrer l'existence d'un $\mathbf{Q}$-isomorphisme équivariant $\varphi : X \to Y$ $(Y = G.w)$ qui applique $L \cap X$ dans un réseau M' stable par $\mathbf{GL}(n, \mathbf{Z})$. Or cela est immédiat. En effet, X et Y sont deux réalisations du quotient G/H (cf. 7.7, Remarque). Les applications $g \mapsto g.v$ et $g \mapsto g.w$ induisent des isomorphismes de G/H sur X et Y respectivement, d'où l'existence d'un $\mathbf{Q}$-isomorphisme équivariant φ de X sur Y. Prenons des coordonnées dans V et W par rapport à des bases de L et M respectivement. Alors les coordonnées de $\varphi(x)$ $(x \in X)$ sont des polynômes à coefficients rationnels en les coordonnées de x. Il existe donc un entier q tel que $q.\varphi(x) \in M$ si $x \in L$, d'où $\varphi(X \cap L) \subset (1/q).M$.

9.12. *Applications.* Soient k un corps de nombres, $\mathfrak{o}$ l'anneau des entiers de k et F une forme homogène de degré $m \geqq 2$ sur $\mathbf{C}^n$ à coefficients dans $\mathfrak{o}$, à discriminant non nul. Alors l'ensemble X de ses transformés par $\mathbf{SL}(n, \mathbf{C})$ est fermé (pour $m = 2$, c'est clair (6.3); pour $m \geqq 3$, *voir* (6.5)). En utilisant 9.11 et le passage de k à $\mathbf{Q}$ donné par la restriction des scalaires (7.16), on voit que l'ensemble des formes à coefficients dans $\mathfrak{o}$ contenues dans X est réunion d'un nombre fini d'orbites de $\mathbf{SL}(n, \mathfrak{o})$. Pour $k = \mathbf{Q}(i)$, $\mathfrak{o} = \mathbf{Z}(i)$, c'est le résultat de Jordan mentionné en 6.5.

Plus généralement, on peut remplacer dans 9.11, $\mathbf{Q}$ par k, L par un $\mathfrak{o}$-réseau, et prendre pour Γ un groupe arithmétique au sens de 7.16. Cela se voit comme précédemment si L est libre. Sinon, on utilise le fait que L est d'indice fini dans un $\mathfrak{o}$-réseau libre L', et on remarque que L' est stable par un sous-groupe d'indice fini de Γ (ce qui résulte de 7.13 par restriction des scalaires).

Note bibliographique

La proposition 9.2 et sa généralisation mentionnées en 9.11 sont dues à G. D. Mostow [19]. Une démonstration figure aussi dans [5, § 1].

La construction des ensembles fondamentaux donnée en 9.8 est empruntée à [5]. Elle repose essentiellement sur le lemme de finitude du § 6, et constitue une généralisation du procédé de Hermite décrit dans le § 5. Le théorème 9.11 est démontré dans [5, Theorem 6.9].

Ensembles fondamentaux à pointes

§ 10. Tores algébriques

10.1. Soient k un corps, T un tore défini sur k, $\mathrm{X}(\mathrm{T}) = \mathrm{Mor}(\mathrm{T}, \mathbf{GL}_1)$, le groupe de ses caractères, et $\mathrm{Y}(\mathrm{T})$ le groupe $\mathrm{Mor}(\mathbf{GL}_1, \mathrm{T})$ de ses sous-groupes à un paramètre. Le sous-groupe de $\mathrm{X}(\mathrm{T})$ (resp. $\mathrm{Y}(\mathrm{T})$) formé des caractères (resp. des sous-groupes à un paramètre) définis sur k est désigné par $\mathrm{X}(\mathrm{T})_k$ (resp. $\mathrm{Y}(\mathrm{T})_k$).

DÉFINITION. On dit que T est *décomposé sur k*, ou est *déployé sur k*, si T est isomorphe sur k à un produit de groupes multiplicatifs.
La clôture algébrique $\bar{k}$ d'un corps de définition k décompose évidemment un tore, mais il suffit en fait d'une extension galoisienne finie, ce qui est clair au moins dans le cas où k est parfait.

10.2. Si k est un corps de décomposition du tore T, il existe un isomorphisme défini sur k de T sur le groupe des matrices diagonales :

$$x = \mathrm{diag}\,(x_1, \ldots, x_d)$$

ce qui permet de voir qu'après cette identification un caractère est de la forme :

$$x \mapsto x_1^{m_1} \cdot \ldots \cdot x_d^{m_d}$$

et un sous-groupe à un paramètre :

$$t \mapsto \mathrm{diag}\,(t^{m_1}, \ldots, t^{m_d}) \qquad (t \in \Omega^*)$$

avec $m_i \in \mathbf{Z}$.
Les groupes abéliens $\mathrm{X}(\mathrm{T})$ et $\mathrm{Y}(\mathrm{T})$ associés à un tore T sont donc isomorphes à $\mathbf{Z}^d$, où d désigne la dimension du tore.
D'autre part, si $a \in \mathrm{X}(\mathrm{T})$ et $b \in \mathrm{Y}(\mathrm{T})$, $a.b$ est un caractère de $\mathbf{GL}_1$. Il existe donc un entier $n \in \mathbf{Z}$, tel que $ab(t) = t^n$. La formule $\langle a, b \rangle = n$ permet alors de définir sur $\mathrm{X}(\mathrm{T}) \times \mathrm{Y}(\mathrm{T})$ une forme $\mathbf{Z}$-bilinéaire qui met en fait $\mathrm{X}(\mathrm{T})$ et $\mathrm{Y}(\mathrm{T})$ en dualité.
Le groupe de Galois M d'une extension galoisienne k' d'un corps de définition k de T opère de façon naturelle sur $\mathrm{X}(\mathrm{T})$ et $\mathrm{Y}(\mathrm{T})$. Le transformé ${}^s a = s(a)$ de $a \in \mathrm{X}(\mathrm{T})$ par $s \in \mathrm{M}$ vérifie :

$${}^s a({}^s x) = {}^s(a(x)), \qquad (x \in \mathrm{T}_{k'})$$

et de même pour l'action de M sur $Y(T)$. Les groupes $X(T)_k$ et $Y(T)_k$ apparaissent alors comme les ensembles des points fixes de M, ce sont des facteurs directs. On peut prolonger ces opérations aux espaces vectoriels :

$$X(T)^{\mathbf{Q}} = X(T) \otimes \mathbf{Q}, \qquad Y(T)^{\mathbf{Q}} = Y(T) \otimes \mathbf{Q}.$$

On obtient ainsi deux représentations de M, qui sont contragédientes vu l'égalité :

$$\langle {}^s a, {}^s b \rangle = \langle a, b \rangle, \qquad (a \in X(T), \quad b \in Y(T)),$$

qui résulte immédiatement des définitions. Par suite, $X(T)_k \otimes \mathbf{Q}$ et $Y(T)_k \otimes \mathbf{Q}$ ont même dimension, ou encore :

$$\text{(1)} \qquad \operatorname{rg} X(T)_k = \operatorname{rg} Y(T)_k.$$

Comme $X(T)$ est de type fini, le noyau de ces représentations est d'indice fini dans M, donc les représentations de M dans $X(T)^{\mathbf{Q}}$ et $Y(T)^{\mathbf{Q}}$ sont complètement réductibles.

Remarquons encore qu'il y a correspondance biunivoque entre les k-sous-tores de T et les sous-espaces de $Y(T)^{\mathbf{Q}}$ stables par M. Elle est définie en associant à un k-sous-tore S le sous-espace $Y(S)^{\mathbf{Q}}$ de $Y(T)^{\mathbf{Q}}$ et à un sous-espace V de $Y(T)^{\mathbf{Q}}$ le sous-tore engendré par les images des $b \in V \cap Y(T)$. Si les sous-espaces V_i $(i \in I)$ sont associés aux k-sous-tores S_i, alors $\bigcap_{i \in I} V_i$ correspond à la composante neutre de $\bigcap_i S_i$ et la somme des V_i au tore engendré par les S_i.

10.3. PROPOSITION. *Pour un tore* T *défini sur* k, *les propriétés suivantes sont équivalentes :*

(i) T *est décomposé sur* k.
(ii) $Y = Y_k$.
(iii) $X = X_k$.
(iv) *Pour toute représentation* ρ *définie sur* k, $\rho(T)$ *est un tore déployé sur* k.

Presque toutes les implications (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i) sont triviales. Prouvons simplement (iv) à partir de (iii). Si K/k est une extension galoisienne décomposant T, l'espace V de la représentation s'écrit sur K comme somme directe d'espaces :

$$V_\chi = \{ v \in V \mid \rho(t).v = \chi(t).v, \qquad (t \in T) \}.$$

Si s est un élément du groupe de Galois M de K/k, il est clair que l'on a l'égalité :

$$s(V_\chi) = V_{s(\chi)}, \qquad (\chi \in X(T)).$$

L'hypothèse $X = X_k$ signifie que pour tout $\chi \in X(T)$, on a $\chi = s(\chi)$, $(s \in M)$. Les espaces V_χ sont donc invariants par M, ce qui prouve qu'ils sont définis sur k.

10.4. COROLLAIRE. (i) *Un quotient d'un tore décomposé sur* k *est décomposé sur* k.
(ii) *Si la suite de tores :*

$$0 \to T' \to T \to T'' \to 0$$

est exacte et définie sur k, *le tore* T *est décomposé sur* k *si, et seulement si,* T′ *et* T″ *le sont.*

La première assertion traduit simplement l'implication (i) $\Rightarrow$ (iv) de la proposition. L'exactitude de la suite d'espaces vectoriels :

$$0 \to X(T'')^{\mathbf{Q}} \to X(T)^{\mathbf{Q}} \to X(T')^{\mathbf{Q}} \to 0$$

résulte aussitôt de celle de la suite des tores. Vu la complète réductibilité de l'action du groupe de Galois d'une extension galoisienne décomposant les trois tores, la suite des espaces de points fixes :

$$0 \to X(T'')_k^{\mathfrak{g}} \to X(T)_k^{\mathfrak{g}} \to X(T')_k^{\mathfrak{g}} \to 0$$

est aussi exacte. On en déduit l'égalité :

$$\operatorname{rg} X(T)_k = \operatorname{rg} X(T')_k + \operatorname{rg} X(T'')_k$$

ce qui permet de conclure grâce à 10.3 (iii) et à l'absence de torsion dans les quotients du type $X(T)/X(T)_k$.

10.5. DÉFINITION. Un groupe algébrique réductif (7.5) G est dit *anisotrope sur k* s'il est défini sur k, et ne contient aucun tore décomposé sur k et $\neq \{e\}$. Lorsqu'il n'y a pas de doute sur k, on dira aussi anisotrope pour anisotrope sur k.
Si $\operatorname{car} k = 0$, cette condition équivaut à : G_k est formé d'éléments semi-simples, et $X(G^0)_k = \{0\}$.

10.6. PROPOSITION. (i) *Si k est un corps de définition commun à un tore* T *et à un sous-tore* S, *il existe un sous-tore* S' *de* T *défini sur k, tel qu'on ait :* $T = S.S'$ *avec* $S \cap S'$ *fini.*
(ii) *Un k-tore* T *peut s'écrire sur k comme produit presque direct de deux sous-tores :* $T = T_d.T_c$, *où* T_d *est décomposé sur k et* T_c *anisotrope sur k. Cette décomposition est unique, préservée par les k-morphismes.* T_d *est le plus grand sous-tore décomposé sur k, et* T_c *le plus grand sous-tore anisotrope sur k de* T. *Le tore* T_c *est la composante neutre de l'intersection des noyaux des caractères définis sur k de* T.

(i) Si K/k est une extension galoisienne finie qui décompose T, son groupe de Galois M opère de façon complètement réductible dans $Y(T) \otimes \mathbf{Q}$ et laisse stable le sous-espace $Y(S) \otimes \mathbf{Q}$; on peut donc trouver un supplémentaire de ce sous-espace, qui soit stable par M et qui définit donc un sous-tore S' convenable.
(ii) Soit M comme dans (i). Le sous-espace $V = Y(T)_k \otimes \mathbf{Q}$ des points fixes de M dans $Y(T)^{\mathfrak{g}}$ admet un et un seul sous-espace supplémentaire W stable par M. Le tore T est produit presque direct des k-sous-tores associés à V et W (10.2) et le premier (resp. second) est déployé (resp. anisotrope) sur k vu 10.3 (resp. 10.2 (i)), ce qui établit la première assertion de (ii). Soit S un k-sous-tore de T. S'il est déployé sur k, il est associé à un sous-espace de V vu 10.4, donc est contenu dans T_d; s'il est anisotrope sur k, il correspond à un sous-espace U de $Y(T)^{\mathfrak{g}}$ stable par M ne contenant pas la représentation triviale de M, donc contenu dans W, et $S \subset T_c$. Enfin, il est clair que l'image par un k-morphisme d'un tore anisotrope sur k est anisotrope sur k; celle d'un tore déployé sur k est déployée sur k vu 10.4, d'où la dernière assertion de (ii).

10.7. PROPOSITION. (a) *Soient* G *un k-groupe connexe et* G' *un k-sous-groupe distingué connexe de* G. *Alors l'image de l'homomorphisme de restriction* $i^* : X(G)_k \to X(G')_k$ *est d'indice fini. Si* G *est réductif, et* $G' = Z(G)^0$, *alors i^* est injectif.*
(b) *Un k-groupe réductif connexe est le produit presque direct d'un tore* S *déployé sur k et d'un groupe* G_1 *tel que* $X(G_1)_k = \{0\}$. *Ce groupe est la composante neutre de l'intersection des caractères définis sur k de* G. *Cette décomposition est unique et compatible avec les k-morphismes.*

(a) Supposons tout d'abord G réductif, et $G' = Z(G)^0$. On sait que G est le produit presque direct de G' et de son groupe dérivé H. Tout caractère de G est évidemment trivial sur H, donc i^* est injective. D'autre part, si $a \in X(G')_k$, il existe une puissance a^m de a qui est triviale sur le groupe fini $H \cap G'$, donc a^m est dans l'image de i^*, donc coker i^* est fini dans ce cas.

Soit toujours G réductif. Alors G' est aussi réductif. Posons :

$$S = Z(G)^0 \qquad \text{et} \qquad S' = Z_{G'}(G')^0.$$

On a un diagramme commutatif, où les flèches désignent des homomorphismes de restriction :

$$\begin{array}{ccc} X(G)_k & \xrightarrow{\mu} & X(G')_k \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ X(S)_k & \xrightarrow{\nu} & X(S')_k \end{array}$$

On a déjà vu que α, β sont injectifs, de conoyau fini. D'autre part, 10.6 entraîne immédiatement que le conoyau de ν est fini. Il en est alors de même pour le conoyau de μ.

Dans le cas général, soit U le radical unipotent de G (cf. 7.15). Le quotient G/U est réductif (comme cela résulte de 7.15, si l'on veut, mais est en fait beaucoup plus élémentaire). Alors $G' \cap U$ est le radical unipotent de G'. On a le diagramme commutatif :

$$\begin{array}{ccc} X(G)_k & \xrightarrow{\mu} & X(G')_k \\ \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \beta} \\ X(G/U)_k & \xrightarrow{\nu} & X(G'/(G' \cap U))_k \end{array}$$

où μ, ν sont induits par les applications d'inclusion, α, β par les projections canoniques. Ces dernières sont des isomorphismes puisque $X(U) = X(G' \cap U) = \{1\}$. On est donc ramené au cas réductif.

(b) En vertu de 10.6, le tore $Z(G)^0$ s'écrit de façon unique comme produit presque direct $S.S_c$ d'un tore S déployé sur k et d'un tore S_c anisotrope sur k. On pose alors $G_1 = S_c.(G, G)$. Il est clair que $G_1 \subset \left(\bigcap_{a \in X(G)_k} \ker a\right)^0$. L'inclusion contraire résulte immédiatement de *(a)*. La dernière assertion est alors conséquence de 10.6.

10.8. *Application au cas réel.* Soient T un tore défini sur $\mathbf{R}$, et d la dimension de T. Le groupe de Galois $M = \mathbf{Z}/2\mathbf{Z}$ de $\mathbf{C}/\mathbf{R}$ opère sur $Y(T)^{\mathbf{Q}}$ qui se décompose en somme de d droites invariantes. Le tore est donc produit presque direct de d tores à une dimension. Il reste à déterminer la structure de T lorsque $d = 1$. Dans ce

cas, T admet une représentation fidèle dans un espace vectoriel V de dimension deux, et ce dernier se décompose en somme. Il faut distinguer deux cas :

(i) M opère trivialement sur X(T), donc (10.3), T est isomorphe sur $\mathbf{R}$ à $\mathbf{GL}_1$, et $T_{\mathbf{R}} = \mathbf{R}^*$.

(ii) M n'opère pas trivialement sur X(T). Il transforme alors tout caractère en son inverse, et V est somme directe de deux droites stables V_a, $V_{a^{-1}}$, où a engendre X(T). Le groupe $T \subset GL(V)$ est isomorphe sur $\mathbf{C}$ au groupe de matrices

$$\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}, \qquad (z \in \mathbf{C}^*),$$

i.e. au groupe orthogonal propre de la forme $x.y$. Le groupe T est alors isomorphe sur $\mathbf{R}$ au groupe orthogonal unimodulaire $\mathbf{SO}(2, \mathbf{C})$, et $T = \mathbf{SO}(2)$ est compact. Revenant au cas où d est quelconque, on voit donc que :

$$T_{\mathbf{R}}^0 = (\mathbf{SO}(2))^a \times (\mathbf{R}_+^*)^b, \qquad (a = \dim T_c, \quad b = \dim T_d).$$

En particulier, les conditions suivantes sont équivalentes : (i) T est anisotrope sur $\mathbf{R}$, (ii) $T_{\mathbf{R}}$ est compact; (iii) L'élément non trivial de $M = \mathrm{Gal}\,\mathbf{C}/\mathbf{R}$ transforme $a \in X(T)$ en a^{-1}. Si ces conditions sont remplies, $T_{\mathbf{R}}$ est un tore au sens usuel, et est connexe. On a donc en général, vu (10.6), $T_{\mathbf{R}} = T_{c,\mathbf{R}} \cdot T_{d,\mathbf{R}}$. En particulier, $T_{\mathbf{R}}/(T_{\mathbf{R}})^0$ est un groupe de type $(2, 2, \ldots, 2)$.

10.9. Mentionnons pour terminer que si G est un k-groupe connexe, T un k-sous-tore de G décomposé sur k, alors l'application $G_k \to (G/T)_k$ est surjective. Cela résulte de la nullité du groupe $H^1(k, T)$ au sens de la cohomologie galoisienne (*voir*, par exemple [28, Chap. X, § 1], ou, pour une démonstration (non cohomologique) d'un résultat plus général ([26], [1, § 15])).

Note bibliographique

Pour plus de détails sur le contenu de ce paragraphe, on peut consulter [7, § 1] qui donne également d'autres références, ou [1, § 8].

Les groupes X(T) et Y(T) ont été introduits dans [10, Exp. 9]. Pour les résultats de 10.2 à 10.6, on a suivi l'exposé de [7, § 1].

§ 11. Sous-groupes paraboliques. Décomposition de Bruhat

A. *Généralités.*

11.1. DÉFINITION. On appelle *sous-groupe parabolique* du groupe algébrique connexe G un sous-groupe fermé H, tel que le quotient G/H soit une variété complète.

On sait que, lorsque B est un sous-groupe de Borel de G (c'est-à-dire un sous-groupe

résoluble connexe maximal), G/B est une variété projective. On en tire aisément que les sous-groupes paraboliques de G sont les sous-groupes fermés qui contiennent un sous-groupe de Borel.
Donnons tout d'abord un théorème d'existence de sous-groupes paraboliques.

11.2. THÉORÈME. *Soit* G *un groupe réductif connexe défini sur* k. *Les deux conditions suivantes sont équivalentes :*

(i) *G possède un sous-groupe parabolique propre défini sur* k ;
(ii) *G contient un tore décomposé sur* k *non central ;*
et, sont équivalentes à la suivante lorsque G *est semi-simple et* k *de caractéristique zéro :*
(iii) G_k *contient un élément unipotent distinct de e.*

On considère désormais un groupe G défini sur k et un tore S décomposé sur k maximal. Grâce au théorème de conjugaison affirmant que « *les tores décomposés sur* k *maximaux sont conjugués par* G_k », on peut voir que les définitions que nous allons poser ne dépendent pas essentiellement du choix de S.

11.3. DÉFINITION.

(1) On appelle *k-rang* de G la dimension $r_k(G)$ de S.
(2) Le groupe fini $N(S)/Z(S)$ est « le » *k-groupe de Weyl* de G; on le note ${}_kW(G)$ ou ${}_kW$.
(3) Les *k-racines* de G sont les caractères non triviaux de S dans la représentation adjointe ; elles forment un ensemble fini noté ${}_k\Phi(G)$ ou ${}_k\Phi$.
Ainsi $\alpha \in {}_k\Phi$ signifie qu'il existe un élément non nul X de $\mathfrak{g}$, tel qu'on ait pour tout s de S :

$$\mathrm{Ad}\,(s).X = sXs^{-1} = \alpha(s)\,X.$$

Le groupe fini ${}_kW$ opère de façon naturelle sur X(S) et Y(S); par exemple, si $\chi \in X(S)$ et si $x_w \in N(S)$ représente $w \in {}_kW$, on a :

$$(w\chi)\,(s) = \chi(x_w^{-1}.s.x_w).$$

Comme cette opération laisse ${}_k\Phi$ invariant, ${}_kW$ opère sur l'ensemble des k-racines. On peut énoncer à présent le théorème indiquant la structure des sous-groupes paraboliques minimaux et la décomposition de Bruhat.

11.4. THÉORÈME. *Soit* G *un groupe réductif connexe défini sur* k.

(i) *Les k-sous-groupes paraboliques minimaux sont conjugués par* G_k. *Chacun d'eux s'écrit comme le produit semi-direct :*

$$P = Z(S).U$$

de son radical unipotent U *(invariant) par le centralisateur (réductif) d'un tore* S *décomposé sur* k *maximal. De plus, si* $M = \left(\bigcap_{x \in X(Z(S))_k} \ker x\right)^0$, *alors* M *est le plus grand sous-groupe anisotrope connexe de* Z(S), $M \cap S$ *est fini et* $Z(S) = M.S$, *ce qui donne finalement :*

$$P = M.S.U.$$

(ii) *On a à la fois la « décomposition de Bruhat » pour* G_k *:*

$$G_k = U_k.N(S)_k.U_k$$

et l'égalité :

$$N(S) = N(S)_k.Z(S)$$

ce qui permet d'écrire G_k *comme réunion finie de « cellules » mutuellement disjointes :*

$$G_k = \bigcup_{w \in {}_kW} U_k.x_w.P_k$$

où $\{x_w\}$ *est un système de représentants de* ${}_kW$ *dans* $N(S)_k$.

(iii) ${}_kW$ *est engendré, en tant que groupe opérant dans* $Y(S)^{\mathbf{Q}}$, *par les symétries par rapport aux hyperplans définis par les k-racines. L'ensemble des k-racines* ${}_k\Phi$ *est un « système de racines », qui, lorsque* G *est semi-simple, engendre* $X(S)^{\mathbf{Q}}$.

Pour préciser cette dernière assertion, il faut définir la notion abstraite de « systèmes de racines ».

11.5. DÉFINITION. Étant donné un $\mathbf{Q}$-espace vectoriel V muni d'un produit scalaire $(\ |\ )$ positif non dégénéré, une partie finie R de V est appelée *système de racines* si elle vérifie les axiomes suivants :

(i) $0 \notin R$ et $\alpha \in R \Rightarrow -\alpha \in R$.

(ii) $\alpha, \beta \in R \Rightarrow n_{\alpha,\beta} = 2\dfrac{(\alpha|\beta)}{(\beta|\beta)} \in \mathbf{Z}$.

(iii) $\alpha, \beta \in R \Rightarrow s_\beta(\alpha) = \alpha - n_{\alpha,\beta}\beta \in R$.

On peut montrer que ces axiomes entraînent que si deux racines sont liées par $\alpha = c\beta$, alors $c = \pm 1/2, \pm 1$ ou ± 2.
Étant donné un ordre linéaire sur ${}_k\Phi$, toute k-racine est combinaison linéaire à coefficients entiers tous de même signe de $r_k(G)$ racines positives : ce sont les *racines simples* associées à l'ordre choisi. On note ${}_k\Delta$ l'ensemble de ces racines simples. Dans la situation du théorème 11.4, V est l'espace vectoriel $X(S)^{\mathbf{Q}}$, sur lequel on a mis un produit scalaire positif non dégénéré, invariant par le groupe fini ${}_kW$.

11.6. *Remarques sur* 11.4.

(1) *La partie anisotrope* M *de* Z(S) *est normalisée par* N(S) : on le voit aussitôt à partir de l'égalité $N(S) = N(S)_k.Z(S)$.
(2) On appelle *chambres de Weyl* de G les composantes connexes dans $Y(S)^{\mathbf{R}}$ du complémentaire de la réunion des hyperplans définis par les racines. Le groupe ${}_kW$ les permute de façon simplement transitive. Chaque chambre C définit un ordre sur ${}_k\Phi$: la racine α est positive, si elle prend des valeurs positives sur C.
(3) On peut ordonner ${}_k\Phi$ de telle sorte que l'algèbre de Lie de U soit :

$$\mathfrak{u} = \bigoplus_{\alpha > 0} \mathfrak{g}_\alpha,$$

où :

$$\mathfrak{g}_\alpha = \{X \in \mathfrak{g} \mid \forall s \in S, \quad \mathrm{Ad}\,(s).X = \alpha(s)\,X\}.$$

On dira alors que l'ordre sur ${}_k\Phi$ est associé à U. Il y a ainsi correspondance biunivoque entre :

(i) les ensembles d'éléments positifs, ou les ensembles de racines simples pour les différents ordres sur ${}_k\Phi$;
(ii) les chambres de Weyl dans $Y(S)^{\mathbf{R}}$;
(iii) les sous-groupes paraboliques définis sur k minimaux qui contiennent $Z(S)$;
(iv) les sous-groupes unipotents définis sur k et normalisés par S maximaux.

Lorsqu'on a une décomposition $P = M.S.U$, il est sous-entendu que ${}_k\Phi$ est muni d'un ordre associé à U; le groupe U détermine donc un certain ensemble de racines simples ${}_k\Delta$.

(4) Chaque cellule $G_{w,k} = U_k.x_w.P_k$ de la décomposition de Bruhat de G_k peut conduire à une décomposition unique de tout élément qu'elle contient. Il suffit pour cela de l'écrire :

$$G_{w,k} = U'_{w,k}.x_w.P_k,$$

où l'on pose :

$$U'_w = x_w.U^-.x_w^{-1} \cap U,$$

où U^- désigne le sous-groupe unipotent correspondant à l'ordre opposé de celui défini par U sur ${}_k\Phi$. Soit encore :

$$U''_w = x_w.U.x_w^{-1} \cap U.$$

Le groupe U est égal à $U'_w.U''_w$ et, en fait, l'application produit :

$$U'_w \times U''_w \to U$$

est un isomorphisme de variétés algébriques. Quant à l'algèbre de Lie de U'_w, elle est égale à la somme des $\mathfrak{g}_\alpha$, où α parcourt les racines $\alpha > 0$ telles que $w^{-1}(\alpha) < 0$. Il faut enfin ajouter que la cellule ouverte $G_{w,k}$ correspond à l'élément du groupe de Weyl w qui transforme U en U^-, i.e. qui transforme l'ordre défini sur ${}_k\Phi$ en l'ordre opposé.

11.7. Pour classer tous les sous-groupes paraboliques définis sur k de G, nous allons construire à partir de la situation standard $P = Z(S).U$ une famille de sous-groupes paraboliques, qui seront des représentants des classes de conjugaison par G_k. On associe pour cela à toute partie θ de ${}_k\Delta$ le sous-tore de S :

$$S_\theta = \Big(\bigcap_{\alpha \in \theta} \ker \alpha\Big)^0,$$

et le k-sous-groupe parabolique contenant P :

$$P_\theta = Z(S_\theta).U.$$

En fait, ce groupe est le produit semi-direct :

$$P_\theta = Z(S_\theta).U_\theta$$

de son radical unipotent U_θ par $Z(S_\theta)$. Les caractères de S dans $\mathfrak{u}_\theta$ sont les racines positives contenant au moins une racine simple extérieure à θ. Quant aux racines de $Z(S_\theta)$, ce sont celles dont les composantes simples sont dans θ.

On voit donc que les k-racines de P_θ sont, d'une part, les racines positives et, d'autre

part, les racines négatives qui sont combinaisons de racines simples appartenant à θ. L'application :

$$\theta \mapsto P_\theta$$

est visiblement croissante et de plus :

$$P_\theta \cap P_{\theta'} = P_{\theta \cap \theta'}.$$
$$P_\emptyset = P, \qquad P_{k\Delta} = G.$$

Soit $[\theta]$ l'ensemble des k-racines qui sont combinaisons linéaires des éléments de θ. Il existe un k-sous-groupe semi-simple connexe L_θ de $Z(S_\theta)$, de k-rang égal au nombre d'éléments de θ, dont $T_\theta = (L_\theta \cap S)^0$ est un k-tore déployé sur k maximal et $[\theta]$ le système de k-racines, et un k-sous-groupe connexe Q_θ de M tels que $Z(S_\theta)$ soit le produit presque direct de Q_θ, L_θ, S_θ. En caractéristique zéro, L_θ a comme algèbre de Lie la somme des sous-espaces $\mathfrak{g}_\alpha + [\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}]$, où α parcourt $[\theta]$.

11.8. THÉORÈME. *Soit* G *un k-groupe réductif connexe.*

(i) *Tout k-sous-groupe parabolique de* G *est conjugué par* G_k *à un et un seul sous-groupe* P_θ.
(ii) *Deux k-sous-groupes paraboliques de* G *conjugués sur* Ω *sont conjugués sur k.*
(iii) *Tout sous-groupe parabolique de* G *est égal à son normalisateur.*
(iv) *La fibration de* G *par un k-sous-groupe parabolique* P *admet des sections locales définies sur k. En particulier, l'application* $G_k \to (G/P)_k$ *est surjective et* $(G/P)_k = G_k/P_k$.

Supposons k de caractéristique zéro. Alors les notions de tore déployé sur k et de k-sous-groupe parabolique minimal sont conservées par un k-morphisme surjectif $f : G \to G'$. Si f est une isogénie, cela résulte facilement de 10.4 et 10.6. Par conséquent, si $G = G_1 . G_2$ est le produit presque direct de k-sous-groupes connexes G_1 et G_2, et P (resp. S) un k-sous-groupe parabolique minimal (resp. tore déployé sur k maximal) de G, alors $P = (P \cap G_1) . (P \cap G_2)$ (resp. $S = (S \cap G_1)^0 . (S \cap G_2)^0$), et $P \cap G_i$ (resp. $(S \cap G_i)^0$) est un k-sous-groupe parabolique minimal (resp. un tore déployé sur k maximal) de G_i. Si maintenant N est la composante connexe du noyau de f, alors, comme G est réductif connexe, on peut trouver un k-sous-groupe connexe N' de G tel que G soit produit presque direct de N et N', et $f : N' \to G'$ est une isogénie. On utilise alors les remarques précédentes. (Si car $(k) \neq 0$, cela reste vrai si l'on suppose f séparable, et les algèbres de Lie de N et N' transverses.)

11.9. Soient P et P' deux sous-groupes paraboliques conjugués. Un élément $x \in G$ tel que $x . P . x^{-1} = P'$ définit canoniquement un isomorphisme $a \to {}^x a$ de $X(P)$ sur $X(P')$, caractérisé par ${}^x a(g) = a(x^{-1} . g . x)$, $(g \in P)$. Comme P est égal à son normalisateur, tout élément $y \in G$ tel que $y . P . y^{-1} = P'$ est de la forme $x . p$ $(p \in P)$. Mais un groupe agit trivialement par automorphismes intérieurs sur son groupe de caractères, donc ${}^x a = {}^y a$, $(a \in X(P))$. Par suite, étant donnés deux sous-groupes paraboliques conjugués, il existe un isomorphisme canonique $X(P) \xrightarrow{\sim} X(P')$. Si P et P' sont de plus définis sur k, alors on peut supposer $x \in G_k$, d'où aussi un isomorphisme canonique de $X(P)_k$ sur $X(P')_k$. On identifiera souvent $X(P)$ et $X(P')$, ou $X(P)_k$ et $X(P')_k$, par cet isomorphisme.

11.10. Soit $G \subset \mathbf{GL}(n, \Omega)$ un k-groupe. Il est dit *trigonalisable* sur k s'il existe un élément $x \in \mathbf{GL}(n, k)$ tel que $x.G.x^{-1}$ soit contenu dans le groupe des matrices triangulaires supérieures. G est alors résoluble. Si G est connexe, et k parfait, cette condition équivaut à l'existence d'une suite de composition :

$$G = G_0 \supset G_1 \supset \ldots \supset G_s = \{e\}$$

formée de k-sous-groupes connexes telle que le quotient G_i/G_{i+1} soit isomorphe sur k soit au groupe additif de Ω soit à $\mathbf{GL}_1$ $(i = 1, \ldots, s-1)$. Un k-groupe vérifiant cette dernière condition est un *k-groupe résoluble déployé sur k*, ou décomposé sur k. Le résultat de Rosenlicht cité en 10.9 implique en fait plus généralement que si G est un sous-groupe résoluble déployé sur k d'un k-groupe connexe H, alors la fibration de H par G est localement triviale sur k. En particulier, l'application $H_k \to (H/G)_k$ est surjective, et $(H/G)_k = H_k/G_k$.

Supposons G réductif connexe, et k de caractéristique zéro. Alors tout k-sous-groupe connexe de G trigonalisable sur k (resp. unipotent) est conjugué sur k à un sous-groupe du sous-groupe S.U (resp. U), de 11.6.

Nous allons démontrer, pour finir, quelques lemmes techniques, qui seront utilisés dans les paragraphes suivants. On conserve les notations précédentes.

11.11. LEMME. *Soient $\alpha \in {}_k\Delta$ et $w \in {}_k\mathrm{W}$, tels que pour tout $\beta \in {}_k\Delta$ on ait :*

$$w(\beta) = \Sigma m(\gamma, \beta).\gamma \quad \text{avec} \quad m(\alpha, \beta) \geqq 0.$$

Alors tout représentant x_w de w appartient au sous-groupe parabolique propre maximal :

$$\mathrm{P}_{k\Delta - \{\alpha\}}.$$

Comme les k-racines de $\mathrm{P}' = \mathrm{P}_{k\Delta-\{\alpha\}}$ sont les sommes $\sum_{\gamma \in {}_k\Delta} q(\gamma).\gamma$ où l'on exige $q(\alpha) \geqq 0$, l'hypothèse signifie que toute racine simple est transformée par w en une racine de P'; il en est alors de même pour toute racine positive; comme x_w normalise Z(S), il s'ensuit que $x_w.\mathrm{P}.x_w^{-1} \subset \mathrm{P}'$. En vertu de la conjugaison des sous-groupes paraboliques minimaux de P' (11.4), il existe $y \in \mathrm{P}'$, tel que :

$$y.x_w.\mathrm{P}.x_w^{-1}.y^{-1} = \mathrm{P}.$$

Or P est égal à son normalisateur (11.8), donc $y.x_w \in \mathrm{P}$ et $x_w \in \mathrm{P}'$.

11.12. LEMME. *On considère soit deux sous-ensembles de S_k, soit deux k-sous-groupes algébriques de* S. *Notons-les par* A *et* A', *supposons les conjugués par $g \in \mathrm{G}_k$. Alors il existe $h \in \mathrm{N}(\mathrm{S})_k$, tel que :*

$$h.a.h^{-1} = g.a.g^{-1} \qquad (a \in \mathrm{A}).$$

En effet $\mathrm{S}' = g.\mathrm{S}.g^{-1}$ est un tore décomposé sur k maximal inclus dans Z(A'), tout comme S. Il existe donc $z \in \mathrm{Z}(\mathrm{A}')_k$, tel que :

$$z.\mathrm{S}'.z^{-1} = \mathrm{S}.$$

L'élément $h = z.g$ appartient à $\mathrm{N}(\mathrm{S})_k$ et comme $g.a.g^{-1} \in \mathrm{A}'$, on a :

$$z.g.a.g^{-1}.z^{-1} = g.a.g^{-1}, \qquad (a \in \mathrm{A}).$$

11.13. LEMME. *Soit* N *un groupe unipotent défini sur un corps k de caractéristique* 0. *On suppose donnée une suite d'idéaux* $\{\mathfrak{n}_i\}_{0 \leqslant i \leqslant q+1}$ *de son algèbre de Lie* $\mathfrak{n}$, *telle que :*

$$[\mathfrak{n}, \mathfrak{n}_i] \subset \mathfrak{n}_{i+1},$$

$$\{0\} = \mathfrak{n}_{q+1} \subset \ldots \subset \mathfrak{n}_{i+1} \subset \mathfrak{n}_i \subset \ldots \subset \mathfrak{n}_0 = \mathfrak{n}.$$

Soit $\mathfrak{n} = \mathfrak{a} \oplus \mathfrak{b}$ *une décomposition de* $\mathfrak{n}$ *en somme de deux sous-espaces telle que :*

$$\mathfrak{n}_i = (\mathfrak{n}_i \cap \mathfrak{a}) \oplus (\mathfrak{n}_i \cap \mathfrak{b}). \qquad (i = 1, \ldots, q).$$

Alors, l'application :

$$\varphi : (a, b) \mapsto e^a . e^b$$

est un isomorphisme de la variété $\mathfrak{a} \times \mathfrak{b}$ *sur* N.

D'après l'hypothèse $\mathfrak{n}_q$ est central : on peut considérer la projection π de N sur le groupe quotient $N' = N/N_q$; on pose $\mathfrak{a}' = d\pi(\mathfrak{a})$ et $\mathfrak{b}' = d\pi(\mathfrak{b})$ et l'on choisit un supplémentaire $\mathfrak{a}''$ (resp. $\mathfrak{b}''$) de $\mathfrak{n}_q \cap \mathfrak{a}$ (resp. $\mathfrak{n}_q \cap \mathfrak{b}$) dans $\mathfrak{a}$ (resp. $\mathfrak{b}$). La démonstration se fait par récurrence sur l'entier q; si $g \in N$:

$$\pi(g) = e^{a'} . e^{b'} = \pi(e^{a''} . e^{b''})$$

où a', b' sont des fonctions régulières de $\pi(g)$, donc de g, d'où :

$$g = e^{a''} . e^{b''} . z \qquad \text{où} \qquad z \in N_q, \quad a'' \in \mathfrak{a}'', \quad b'' \in \mathfrak{b}''.$$

Mais, toujours par récurrence :

$$z = e^u . e^v, \qquad \text{où} \qquad u \in \mathfrak{n}_q \cap \mathfrak{a} \qquad \text{et} \qquad v \in \mathfrak{n}_q \cap \mathfrak{b}$$

avec u, v dépendant alors régulièrement de z, a'', b'', donc de g, et :

$$g = e^{a''} e^{b''} e^u e^v = e^{a''+u} e^{b''+v},$$

puisque $\mathfrak{n}_q$ est central.

B. *Exemples.*

11.14. $G = \mathbf{GL}_n$ ou $\mathbf{SL}_n$.

On prend comme tore décomposé sur k maximal le tore D des matrices diagonales; c'est un sous-groupe de Cartan, $Z(D) = D$. Une matrice de D s'écrivant $\mathrm{diag}\{\lambda_i\}$, on peut choisir comme racines positives les applications λ_i/λ_j avec $i < j$, ce qui donne pour racines simples les $\alpha_i = \lambda_i/\lambda_{i+1}$. Le sous-groupe parabolique minimal correspondant à cet ordre est le groupe résoluble des matrices triangulaires supérieures, égal à D.N, où N est le sous-groupe unipotent des matrices ayant des 1 sur la diagonale. Ainsi G/P est la variété des drapeaux usuelle. Plus généralement, on peut associer à une suite croissante d'entiers :

$$1 \leqslant d_1 < \ldots < d_p \leqslant n - 1,$$

le drapeau canonique de type $(d_1, \ldots, d_p)$:

$$(e_1, \ldots, e_{d_1}) \subset \ldots \subset (e_1, \ldots, e_{d_p}).$$

Leurs groupes de stabilité sont précisément les sous-groupes paraboliques contenant P. On a donc, en particulier :

$$D = \left\{\begin{pmatrix}\lambda_1 & & 0\\ & \ddots & \\ 0 & & \lambda_n\end{pmatrix}\right\} \qquad N = \left\{\begin{pmatrix}1 & & *\\ & \ddots & \\ 0 & & 1\end{pmatrix}\right\} \qquad P = \left\{\begin{pmatrix}\lambda_1 & & *\\ & \ddots & \\ 0 & & \lambda_n\end{pmatrix}\right\}$$

$$P_{\alpha_j} = \left\{\begin{pmatrix}\lambda_1 & & & & *\\ & \ddots & & & \\ & & \lambda_{j-1} & & \\ & & & B & \\ & & & & \lambda_{j+2} \\ & & & & & \ddots \\ 0 & & & & & & \lambda_n\end{pmatrix}\right\}, \qquad (B \in \mathbf{GL}(2, \mathbf{R})),$$

$$P_j = P_{\Delta-\{\alpha_j\}} = \{(a_{ik}) \in G,\ a_{ik} = 0 \quad (k \leqq j < i)\}.$$

11.15. G est *déployé sur k*, c'est-à-dire S est un sous-groupe de Cartan : $Z(S) = S$. Alors P est résoluble. Pour toute extension k' du corps de base k, on a l'isomorphisme :

$$_{k'}\Phi \xrightarrow{\sim} {}_k\Phi.$$

Les groupes $\mathbf{GL}_n$, $\mathbf{SL}_n$ sont déployés sur le corps premier. Un autre cas particulier important est celui du *groupe symplectique :*

$$\mathbf{Sp}\ (2n, \Omega) = \{X \in \mathbf{GL}(2n, \Omega),\ {}^tX.J.X = J\} \qquad \left(J = \begin{pmatrix} 0 & I_n \\ -I_n & 0\end{pmatrix}\right).$$

Les matrices diagonales de $\mathbf{Sp}\ (2n, \Omega)$ sont les matrices de la forme :

$$\begin{pmatrix}\lambda_1 & & & & & \\ & \ddots & & & 0 & \\ & & \lambda_n & & & \\ & & & \lambda_1^{-1} & & \\ & 0 & & & \ddots & \\ & & & & & \lambda_n^{-1}\end{pmatrix}.$$

Elles forment un tore déployé sur k de dimension n, qui est un sous-groupe de Cartan. Si l'on identifie $\mathbf{Sp}\ (2n, \Omega)$ au groupe des automorphismes G de Ω^{2n} qui laissent invariante la forme bilinéaire de matrice :

$$\begin{pmatrix} 0 & J'_n \\ -J'_n & 0\end{pmatrix}, \qquad J'_n = \begin{pmatrix} 0 & & & 1 \\ & & \iddots & \\ & \iddots & & \\ 1 & & & 0\end{pmatrix},$$

alors on peut prendre pour S (resp. P) l'intersection de G avec le groupe des matrices diagonales (resp. triangulaires supérieures). On voit alors tout de suite que les racines de G sont les caractères $\lambda_i^{\pm 1}.\lambda_j^{\pm 1}$ $(1 \leqq i \leqq j \leqq n)$ avec multiplicité un (en notation multiplicative).

11.16. $G = O(F)$, groupe orthogonal d'une forme quadratique non dégénérée sur k^n.

Si p est l'indice de F, c'est-à-dire la dimension des sous-espaces isotropes maximaux, la décomposition de Witt (Bourbaki, *Alg.*, chap. 9, § 4, n° 2) permet d'écrire la matrice de F sous la forme :

$$\begin{pmatrix} 0 & 0 & J \\ 0 & F_0 & 0 \\ J & 0 & 0 \end{pmatrix}, \qquad \text{où} \qquad J = \begin{pmatrix} 0 & & 1 \\ & \cdot^{\cdot} & \\ 1 & & 0 \end{pmatrix}$$

est d'ordre p et où F_0 ne représente pas 0 sur k :

$$F(x) = 2(x_1 x_n + \ldots + x_p x_{n-p+1}) + F_0(x_{p+1}, \ldots, x_{n-p}).$$

On peut alors prendre pour tore décomposé sur k maximal le sous-groupe :

$$S = \left\{ \begin{pmatrix} \lambda_1 & & & & \\ & \ddots & & 0 & \\ & & \lambda_p & & \\ & & & I_{n-2p} & \\ & 0 & & & \lambda_p^{-1} \\ & & & & & \ddots \\ & & & & & & \lambda_1^{-1} \end{pmatrix} \right\}.$$

Le centralisateur de S est $Z(S) = S \times O(F_0)$. Si Q est le drapeau isotrope canonique : $(e_1) \subset (e_1, e_2) \subset \ldots \subset (e_1, \ldots, e_p)$, son groupe de stabilité est le sous-groupe parabolique minimal :

$$P = \left\{ \begin{pmatrix} P_1 & P_2 & P_3 \\ 0 & P_4 & P_5 \\ 0 & 0 & P_6 \end{pmatrix} \right\},$$

où P_1 et P_6 sont triangulaires supérieures, où P_4 appartient au groupe orthogonal $O(F_0)$, P_6 étant déterminée par P_1 et P_3, et P_5 par P_1, P_2 et P_4. D'ailleurs le radical unipotent U de P (tel que : $P = Z(S).U$) est l'ensemble des matrices :

$$U = \left\{ \begin{pmatrix} P_1 & P_2 & P_3 \\ 0 & I & P_5 \\ 0 & 0 & P_6 \end{pmatrix} \right\},$$

avec cette fois P_1 et P_6 unipotentes : on peut lire les liens entre $P_1, \ldots, P_6$ sur l'algèbre de Lie de U :

$$\mathfrak{u} = \left\{ \begin{pmatrix} A_1 & A_2 & A_3 \\ 0 & 0 & A_5 \\ 0 & 0 & A_6 \end{pmatrix} \right\}.$$

A_1 et A_6 sont triangulaires supérieures avec des éléments diagonaux nuls. Comme une matrice X de $\mathfrak{u}$ est assujettie à :

$${}^tXF + FX = 0,$$

on a les relations :

$$\begin{aligned} {}^tA_1 J + JA_6 &= 0 \\ {}^tA_2 J + F_0 A_5 &= 0 \\ {}^tA_3 J + JA_3 &= 0 \end{aligned}$$

ce qui indique en particulier l'antisymétrie de A_3 par rapport à la diagonale non principale.

Les k-racines positives s'obtiennent en regardant comment opère S sur $\mathfrak{u}$ par la représentation adjointe :

dans A_1, on trouve λ_i/λ_j avec $1 \leqslant i \leqslant j \leqslant p$ et 1 pour multiplicité;
dans A_6, on trouve encore les mêmes racines avec la même multiplicité;
dans A_3, on a les racines $\lambda_i\lambda_j$ avec $1 \leqslant i < j \leqslant p$ et 1 pour multiplicité;
enfin, si $F_0 \neq 0$, on obtient dans A_2 et A_5 globalement des sous-espaces de dimension $n - 2p$, propres pour la racine λ_i avec $1 \leqslant i \leqslant p$.

On voit que les k-racines simples sont :

$$\alpha_i = \lambda_i \lambda_{i+1}^{-1} \qquad \text{pour} \qquad 1 \leqslant i \leqslant p-1,$$

avec, en outre, α_p égale dans le cas $n = 2p$ $(F_0 = 0)$ à $\lambda_{p-1}\lambda_p$, et dans le cas $n \neq 2p$ $(F_0 \neq 0)$, à λ_p.

On peut relever certains cas particuliers intéressants :

1) $n = 2p$ *ou* $2p+1$: $Z(S) = S$, et S est un sous-groupe de Cartan; c'est le cas déployé.

2) $n = 2p+2$: $Z(S)$ est un tore; c'est un sous-groupe de Cartan, mais distinct de S; c'est le cas du groupe *quasi déployé* sur k; P est encore résoluble.

C. *Étude du cas réel.*

Nous nous proposons ici tout d'abord de comparer les décompositions d'Iwasawa, de Bruhat et de Cartan du groupe des points réels d'un **R**-groupe réductif. Le cas essentiel est bien entendu celui des groupes semi-simples. Cependant, il est plus commode pour la suite de se placer directement dans le cas réductif.

11.17. *Décomposition de Cartan.* Soient G un **R**-groupe réductif, Z et G′ le centre connexe et le groupe dérivé de G^0, et K un sous-groupe compact maximal de $G_{\mathbf{R}}$. Alors $K \cap Z$ et $K \cap G'$ sont des sous-groupes compacts maximaux de $Z_{\mathbf{R}}$ et $G'_{\mathbf{R}}$. Soient $\mathfrak{p}$ la somme directe de l'algèbre de Lie du groupe des points réels du plus grand tore Z_d décomposé sur **R** de Z et du complément orthogonal de $\mathfrak{g}' \cap \mathfrak{k}$ dans $\mathfrak{g}'_{\mathbf{R}}$ par rapport à la forme de Killing. On a alors :

$$\mathfrak{g}_{\mathbf{R}} = \mathfrak{k} \oplus \mathfrak{p}$$

et l'application $(k, p) \mapsto k.\exp p$ $(k \in K,\ p \in \mathfrak{p})$ est un homéomorphisme analytique de $K \times \mathfrak{p}$ sur $G_{\mathbf{R}} = K.e^{\mathfrak{p}}$. Ce sont les décompositions de Cartan de $\mathfrak{g}_{\mathbf{R}}$ et $G_{\mathbf{R}}$. L'involution de Cartan associée est dans $\mathfrak{g}_{\mathbf{R}}$ l'automorphisme involutif :

$$\theta : k + p \mapsto k - p \qquad (k \in \mathfrak{k},\quad p \in \mathfrak{p})$$

et dans $G_{\mathbf{R}}$ l'unique automorphisme involutif dont l'ensemble des points fixes est K et la restriction à $Z_{\mathbf{R}}$ est l'involution de Cartan de $Z_{\mathbf{R}}$ au sens de 10.8.

11.18. *Décomposition d'Iwasawa.* On part d'une décomposition de Cartan de $G_{\mathbf{R}}$; on choisit dans $\mathfrak{p}$ une sous-algèbre $\mathfrak{a}$ maximale (elle est commutative) et un ordre linéaire sur l'ensemble de ses racines. Soit :

$$\mathfrak{n} = \sum_{\alpha>0} \mathfrak{g}_\alpha \qquad (\mathfrak{g}_\alpha = \{x \in \mathfrak{g}_{\mathbf{R}}, \quad [a, x] = \alpha(a).x \quad (a \in \mathfrak{a})\}.$$

La décomposition d'Iwasawa :

$$\mathfrak{g}_{\mathbf{R}} = \mathfrak{k} \oplus \mathfrak{a} \oplus \mathfrak{n}$$

de $\mathfrak{g}_{\mathbf{R}}$ correspond à la décomposition d'Iwasawa :

$$G_{\mathbf{R}} = K.A.N \qquad (A = \exp \mathfrak{a}, \quad N = \exp \mathfrak{n})$$

de $G_{\mathbf{R}}$. L'application produit est un homéomorphisme analytique de $K \times A \times N$ sur $G_{\mathbf{R}}$, et de même :

$$(k, a, n) \mapsto k.e^a.e^n \qquad (k \in K, \quad a \in \mathfrak{a}, \quad n \in \mathfrak{n})$$

est un homéomorphisme analytique de $K \times \mathfrak{a} \times \mathfrak{n}$ sur $G_{\mathbf{R}}$.

Le groupe N est normalisé par A. Notons que N est unipotent, A commutatif, et que N et A sont homéomorphes à des espaces euclidiens. Les décompositions d'Iwasawa et de Cartan fournissent donc deux manières de représenter $G_{\mathbf{R}}$ comme produit topologique d'un espace euclidien et d'un sous-groupe compact maximal, On voit en particulier que K rencontre toute composante connexe de $G_{\mathbf{R}}$.

Tout sous-groupe compact maximal de $G_{\mathbf{R}}$ est conjugué par automorphisme intérieur à K et son intersection avec AN est réduite à $\{e\}$. Il s'ensuit que les assertions précédentes restent valables si l'on remplace K par n'importe quel sous-groupe compact maximal de $G_{\mathbf{R}}$. On appellera aussi décomposition d'Iwasawa les décompositions correspondantes de $\mathfrak{g}_{\mathbf{R}}$ et $G_{\mathbf{R}}$.

11.19. Soit $G_{\mathbf{R}} = K.A.N$ une décomposition d'Iwasawa de $G_{\mathbf{R}}$. Alors il existe un unique **R**-sous-groupe parabolique minimal P de G et un tore décomposé sur **R** maximal S de P tels que l'on ait :

$$P = M.S.U = Z(S).U,$$

(notation de 11.4) avec :

$$A = (S_{\mathbf{R}})^0, \qquad N = U_{\mathbf{R}}, \qquad M_{\mathbf{R}} \subset K.$$

Comme $P_{\mathbf{R}} \supset A.N$, l'espace homogène :

$$G_{\mathbf{R}}/P_{\mathbf{R}} = \bigcup_{w \in {}_{\mathbf{R}}W} U'_{w,\mathbf{R}}.x_w,$$

(cf. 11.6) est un quotient de K, ce qui permet de choisir un système de représentants du groupe de Weyl relatif ${}_{\mathbf{R}}W$ dans K, et en fait même dans K^0, car on va voir que $G_{\mathbf{R}}/P_{\mathbf{R}}$ est connexe.

Soit $P' = P_\theta = M'.S'.U'$ un **R**-sous-groupe parabolique contenant P de G^0, où $S' = S_\theta$ et M' est le plus grand sous-groupe anisotrope sur **R** du centralisateur $Z(S')^0$ de S' dans G^0.

Les groupes $S'_{\mathbf{R}}$ et $M'_{\mathbf{R}}$ sont stables par l'involution de Cartan associée à K, donc

$K \cap Z(S')_{\mathbf{R}}$ et $K \cap M'_{\mathbf{R}}$ sont des sous-groupes compacts maximaux de $Z(S')_{\mathbf{R}}$ et $M'_{\mathbf{R}}$, et $K \cap S'$ est l'ensemble des éléments d'ordre deux de $S'_{\mathbf{R}}$.

On a :

$$(1) \qquad G_{\mathbf{R}} = K.P_{\mathbf{R}} = K.P'^{0}_{\mathbf{R}} = K.M'^{0}_{\mathbf{R}}.A'.N' \qquad (N' = U'_{\mathbf{R}}, \quad A' = S'^{0}_{\mathbf{R}}).$$

L'application produit définit un homéomorphisme de $(K.M'^{0}_{\mathbf{R}}) \times A' \times N'$ sur $G_{\mathbf{R}}$ et une application propre de $K \times M'^{0}_{\mathbf{R}}$ sur $K.M'^{0}_{\mathbf{R}}$. En fait, $K.M'^{0}_{\mathbf{R}}$ est le quotient de $K \times M'^{0}_{\mathbf{R}}$ par la relation d'équivalence :

$$(x, y) \approx (x.k, k^{-1}.y) \qquad (x \in K, \ y \in M'^{0}_{\mathbf{R}}, \ k \in K \cap M'^{0}_{\mathbf{R}}).$$

On peut donc écrire tout élément $g \in G_{\mathbf{R}}$ sous la forme :

$$(2) \qquad g = k.m.a.n \qquad (k \in K, \ m \in M'^{0}_{\mathbf{R}}, \ a \in A', \ n \in N').$$

Les éléments a, n et le produit $k.m$ sont déterminés uniquement par G et en dépendent analytiquement, tandis que k et m sont déterminés au produit par un élément du groupe compact $K \cap M'^{0}_{\mathbf{R}}$ près.

On peut aussi considérer la décomposition plus grossière :

$$g = k.p, \qquad (k \in K, \quad p \in P^{0}_{\mathbf{R}}),$$

où k et p sont déterminés au produit par un élément de $K \cap P^{0}_{\mathbf{R}}$ près. Ce dernier est un sous-groupe compact maximal de $P^{0}_{\mathbf{R}}$. Il en résulte que si K' est un sous-groupe compact maximal de $G_{\mathbf{R}}$, alors :

$$G = K'.P'^{0}_{\mathbf{R}},$$

et $K' \cap P'^{0}_{\mathbf{R}}$ est un sous-groupe compact maximal de $P'^{0}_{\mathbf{R}}$. En effet, il existe $a \in G_{\mathbf{R}}$ tel que $K' = a.K.a^{-1}$. Comme K est transitif sur $G_{\mathbf{R}}/P_{\mathbf{R}}$, les groupes d'isotropie des points de $G_{\mathbf{R}}/P_{\mathbf{R}}$ relativement à K sont conjugués dans K. En particulier, $K' \cap P'^{0}_{\mathbf{R}} = a(K \cap a^{-1}.P'^{0}_{\mathbf{R}}.a).a^{-1}$ est isomorphe à $K \cap P'^{0}_{\mathbf{R}}$. C'est donc nécessairement un sous-groupe compact maximal de $P'^{0}_{\mathbf{R}}$.

11.20. PROPOSITION. *Soient* G *un* **R***-groupe algébrique connexe et* P *un* **R***-sous-groupe parabolique de* G. *Alors* $G_{\mathbf{R}}/P_{\mathbf{R}}$ *est connexe.*

Comme P contient le radical unipotent de G, on peut, en passant au quotient, se ramener au cas où G est réductif.

Supposons tout d'abord que P soit minimal parmi les **R**-sous-groupes paraboliques. D'après la décomposition de Bruhat, on a :

$$G_{\mathbf{R}}/P_{\mathbf{R}} = \bigcup_{w \in {}_{\mathbf{R}}W} U'_{w,\mathbf{R}}.x_w.$$

De plus, une de ces « cellules » est ouverte (11.6 (4)), donc dense. Comme elle est connexe, il s'ensuit que $G_{\mathbf{R}}/P_{\mathbf{R}}$ est connexe, ce qui démontre notre assertion pour P minimal.

Dans le cas général, soit P' un **R**-sous-groupe parabolique minimal de G contenu dans P. L'application canonique $G_{\mathbf{R}}/P'_{\mathbf{R}} \to G_{\mathbf{R}}/P_{\mathbf{R}}$, est surjective et continue, donc $G_{\mathbf{R}}/P_{\mathbf{R}}$ est aussi connexe.

Vu 11.8, on a $(G/P)_{\mathbf{R}} \cong G_{\mathbf{R}}/P_{\mathbf{R}}$, d'où aussi le :

11.21. COROLLAIRE. *L'application*

$$(G_{\mathbf{R}})^0 \to (G/P)_{\mathbf{R}}$$

est surjective.

Il en résulte qu'on peut trouver des représentants du groupe de Weyl de G dans $(G_{\mathbf{R}})^0$, par relèvement à partir de $G_{\mathbf{R}}/P_{\mathbf{R}}$; on peut donc en trouver dans K^0.

11.22. PROPOSITION. *Si* G *est un groupe réductif, connexe et anisotrope sur* $\mathbf{R}$, *le groupe* $G_{\mathbf{R}}$ *est compact et connexe pour la topologie ordinaire.*

G est isogène au produit de son groupe dérivé G', qui est semi-simple, et de son centre connexe T, qui est un tore anisotrope sur $\mathbf{R}$ (10.4). Le groupe $T_{\mathbf{R}}$ est compact connexe (10.8) et $G_{\mathbf{R}}^0 = G_{\mathbf{R}}'^0 . T_{\mathbf{R}}^0$ est d'indice fini dans $G_{\mathbf{R}}$ (7.4). On est donc ramené pour la première assertion au cas où G est semi-simple connexe. On peut alors écrire (11.17, 11.18) :

$$G_{\mathbf{R}} = K.A.N = K.e^{\mathfrak{p}}.$$

Mais N est formé d'éléments unipotents, donc est réduit à $\{e\}$, d'où aussi $A = \{e\}$ et $G_{\mathbf{R}} = K$ est compact.

D'après un théorème de Chevalley [9, III, p. 230], tout sous-groupe compact L de $\mathbf{GL}(n, \mathbf{R})$ est « algébrique », au sens de [9, II]; cela revient à dire ici que L est le groupe de *tous* les points réels d'un $\mathbf{R}$-sous-groupe de $\mathbf{GL}(n, \mathbf{C})$, que l'on peut supposer être le plus petit sous-groupe algébrique $L_{\mathbf{C}}$ de $\mathbf{GL}(n, \mathbf{C})$ contenant L. On a $\mathfrak{l} = \mathfrak{gl}(n, \mathbf{R}) \cap \mathfrak{l}_{\mathbf{C}}$ et $\dim_{\mathbf{R}} \mathfrak{l} = \dim_{\mathbf{C}} \mathfrak{l}_{\mathbf{C}}$. Comme un groupe algébrique sur $\mathbf{C}$ est connexe en topologie ordinaire si, et seulement si, il est connexe en topologie de Zariski, il s'ensuit que L et $L_{\mathbf{C}}$ sont simultanément connexes ou non. Si $G_{\mathbf{R}}$ n'était pas connexe, alors $(G_{\mathbf{R}}^0)_{\mathbf{C}}$ serait strictement contenu dans G, et de même dimension que G, ce qui est absurde puisque G est connexe.

11.23. PROPOSITION. *Soient* G *un groupe connexe défini sur* $\mathbf{R}$ *et* S *un tore décomposé sur* $\mathbf{R}$ *maximal de* G. *L'application canonique :*

$$\pi_0(S_{\mathbf{R}}) \to \pi_0(G_{\mathbf{R}}),$$

est surjective, π_0 *désignant le groupe des composantes connexes en topologie ordinaire.*

G est produit semi-direct d'un groupe réductif H et de son radical unipotent N. $N_{\mathbf{R}}$ étant homéomorphe à un espace euclidien, la suite exacte d'homotopie appliquée à $G_{\mathbf{R}}/N_{\mathbf{R}} \cong H_{\mathbf{R}}$ donne l'isomorphisme :

$$\pi_0(H_{\mathbf{R}}) \xleftarrow{\sim} \pi_0(G_{\mathbf{R}}).$$

On peut donc supposer G réductif, et choisir alors un $\mathbf{R}$-sous-groupe parabolique minimal P contenant Z(S). Le groupe Z(S) étant isomorphe au quotient de P par son radical unipotent, on obtient comme ci-dessus un isomorphisme :

$$\pi_0(Z(S)_{\mathbf{R}}) \xleftarrow{\sim} \pi_0(P_{\mathbf{R}}).$$

Il ne reste plus qu'à démontrer la surjectivité des applications :

$$\pi_0(P_{\mathbf{R}}) \to \pi_0(G_{\mathbf{R}}),$$

et

$$\pi_0(S_{\mathbf{R}}) \to \pi_0(Z(S)_{\mathbf{R}}),$$

ce qui, vu la suite exacte d'homotopie, revient à prouver que $G_{\mathbf{R}}/P_{\mathbf{R}}$ et $Z(S)_{\mathbf{R}}/S_{\mathbf{R}}$ sont connexes. Pour $G_{\mathbf{R}}/P_{\mathbf{R}}$, *voir* 11.20. Comme enfin, S est décomposé sur $\mathbf{R}$, le groupe $Z(S)_{\mathbf{R}}/S_{\mathbf{R}}$ est isomorphe au groupe $(Z(S)/S)_{\mathbf{R}}$ (10.9); mais ce dernier est connexe, puisque Z(S)/S est réductif, connexe et anisotrope sur $\mathbf{R}$ (11.22).

11.24. DÉFINITION. Soit $G \subset \mathbf{GL}_n$ un groupe algébrique semi-simple défini sur $\mathbf{R}$. On dit qu'une décomposition d'Iwasawa K.A.N de $G_{\mathbf{R}}$ est *bien placée par rapport à une décomposition d'Iwasawa* $K_0.A_0.N_0$ de $\mathbf{GL}(n, \mathbf{R})$, si les conditions suivantes sont satisfaites :

(i) $K \subset K_0$, $A \subset A_0$ et $N \subset N_0$;
(ii) la restriction à A d'un caractère de A_0, positif pour un ordre associé à N_0, est un caractère de A positif pour un ordre associé à N.
On peut noter que l'inclusion $N \subset N_0$ est une conséquence immédiate de (ii).

11.25. PROPOSITION. *Soit* $G \subset \mathbf{GL}_n$ *un groupe algébrique semi-simple défini sur* $\mathbf{R}$. *Étant donné une décomposition d'Iwasawa* K.A.N *de* $G_{\mathbf{R}}$, *on peut, par conjugaison par un élément de* $\mathbf{GL}(n, \mathbf{R})$, *rendre* $G_{\mathbf{R}}$ *auto-adjoint et « bien placer » par rapport à la décomposition d'Iwasawa canonique de* $\mathbf{GL}(n, \mathbf{R})$.

Notons :

$$\mathfrak{k} \oplus \mathfrak{a} \oplus \mathfrak{n} = \mathfrak{k} \oplus \mathfrak{p},$$

la décomposition d'Iwasawa-Cartan de $\mathfrak{g}_{\mathbf{R}}$ associée à K.A.N. En vertu de 9.3, 9.4, 9.9 une première conjugaison par un élément de $\mathbf{GL}(n, \mathbf{R})$ permet de plonger K dans $K_0 = \mathbf{O}(n)$ et $e^{\mathfrak{p}}$ dans l'espace S des matrices symétriques positives non dégénérées. Ces inclusions ne seront pas altérées par les conjugaisons qui vont suivre, car elles seront effectuées par des éléments de $\mathbf{O}(n)$, et par suite $G_{\mathbf{R}}$ restera auto-adjoint.
Deux sous-algèbres abéliennes maximales de l'espace $\mathbf{S}$ des matrices symétriques réelles étant conjuguées par $\mathbf{O}(n)$, il existe $a \in \mathbf{O}(n)$, tel que ${}^aA \subset A_0$.
On peut alors prolonger un ordre sur $X({}^aA)$ associé à ${}^aN$ en un ordre linéaire sur $X(A_0)$; pour revenir à l'ordre usuel défini sur $X(A_0)$ par N_0, il suffit d'effectuer une conjugaison par un certain élément b de $N(D) \cap \mathbf{O}(n)$ (cf. 11.6 (2), (3)). Le groupe ${}^{ba}A$ est encore inclus dans A_0 et la condition (ii) de la définition 11.24 est satisfaite pour ${}^{ba}A$ et ${}^{ba}N$.

Remarque : On pourrait évidemment énoncer la même proposition pour une décomposition d'Iwasawa $K_0.A_0.N_0$ quelconque de $\mathbf{GL}(n, \mathbf{R})$ en substituant à « auto-adjoint » « stable par une involution de Cartan compatible avec $K_0.A_0.N_0$ ».

Note bibliographique

Pour les démonstrations des résultats énoncés en (A), on renvoie à [7] où l'on trouvera également d'autres références. Les résultats sur les décompositions de Cartan et d'Iwasawa rappelés en 11.17, 11.18 sont classiques pour les groupes semi-simples réels. L'analogue pour les groupes réductifs est établi dans [9] ou [5, § 1]. La Prop. 11.22 est due à Matsumoto (*Proc. Japan Ac.*, 40 (1964), 4-7). Nous avons donné ici la démonstration de [7, § 14].

§ 12. Ensembles de Siegel

Dans ce paragraphe, F *est un sous-corps de* $\mathbf{R}$, G *un* F*-groupe réductif,* P *un* F*-sous-groupe parabolique minimal de* G^0, S *un tore décomposé sur* F *maximal de* P, U *le radical unipotent de* P*;* M *le* F*-sous-groupe anisotrope sur* F *maximal du centralisateur* $Z(S)^0$ *de* S *dans* G^0, *et* ${}_F\Delta$ *l'ensemble des* F*-racines simples de* G *par rapport à* S, *pour un ordre associé à* U.

12.1. On écrira ${}_FA$ pour S_R^0. Pour tout $t > 0$, on pose :

$$ {}_FA_t = \{ a \in {}_FA \mid a^\alpha \leqq t \qquad (\alpha \in {}_F\Delta) \}$$
$$ P_t = \{ p \in P_R \mid |p^\alpha| \leqq t \qquad (\alpha \in {}_F\Delta) \}, \quad P_t^0 = P_t \cap P^0.$$

On a $P_R^0 = M_R^0 . {}_FA . U_R$, donc :

$$P_t^0 = P_t \cap P_R^0 = M_R^0 . {}_FA_t . U_R.$$

12.2. LEMME. *Soient* ω *un sous-ensemble relativement compact de* $M_R . U_R$ *et* $t > 0$. *Alors la réunion des ensembles* $a . \omega . a^{-1}$ $(a \in {}_FA_t)$ *est relativement compacte.*

L'ensemble ω est contenu dans le produit d'un compact de M_R et d'un compact de U_R. Comme M_R centralise ${}_FA$, il suffit de considérer le cas où $\omega \subset U_R$. L'application exponentielle est un homéomorphisme de $\mathfrak{u}_R$ sur U_R, qui commute à P_R, opérant sur $\mathfrak{u}_R$ par la représentation adjointe, sur U_R par automorphismes intérieurs. Il reste donc à montrer que si ω est compact dans $\mathfrak{u}_R$, alors la réunion des ensembles $\mathrm{Ad}\, a(\omega)$ $(a \in {}_FA_t)$ est relativement compacte. Or $\mathfrak{u}_R$ admet une base formée de vecteurs propres de S_R, correspondant aux F-racines positives. Comme ces dernières sont combinaisons linéaires à coefficients $\geqq 0$ des F-racines simples, il existe une constante $t' > 0$ telle que $a^\alpha \leqq t'$ pour toute racine positive et tout $a \in {}_FA_t$. Les restrictions à $\mathfrak{u}_R$ des opérateurs $\mathrm{Ad}\, a$ $(a \in {}_FA_t)$ forment donc un ensemble borné d'opérateurs, d'où le lemme.

12.3. DÉFINITION. Soit K un sous-groupe compact maximal de $G_{\mathbf{R}}$. Un *ensemble de Siegel* de $G_{\mathbf{R}}$ (par rapport à K, P, S) est l'ensemble produit :

$$\mathfrak{S} = \mathfrak{S}_{t,\omega} = K.{}_F A_t.\omega, \tag{1}$$

où ω est un voisinage compact de e dans $M^0_{\mathbf{R}}.U_{\mathbf{R}}$.

On définit de même un *ensemble de Siegel ouvert*, en prenant pour ω un voisinage ouvert relativement compact de e dans $M^0_{\mathbf{R}}.U_{\mathbf{R}}$, et en remplaçant $\leqq$ par $<$ dans la définition de ${}_F A_t$.

On dira que $\mathfrak{S}$ est *normal* si ${}_F A$ est stable par rapport à l'involution de Cartan associée à K.

On remarquera que la notion d'ensemble de Siegel dépend du corps de définition choisi; il faudrait en fait parler d'ensemble de Siegel *sur* F, précision que l'on omettra lorsque cela ne semblera pas prêter à confusion.

Soit F′ un sous-corps de $\mathbf{R}$ contenant F. Alors tout ensemble de Siegel sur F de $G_{\mathbf{R}}$ est contenu dans un ensemble de Siegel sur F′. En effet, on peut prendre un F′-sous-groupe parabolique minimal $P' = M'.S'.U'$ de G^0, tel que l'on ait :

$$S' \supset S, \qquad U' \supset U, \qquad M' \subset M,$$

et supposer que l'on a fixé des ordres compatibles sur X(S′) et X(S). On a $P' = {}_F P_\theta$ où θ est une partie de ${}_F\Delta$ (notations de 11.7). D'autre part, les restrictions à S des F′-racines simples sont des F-racines simples (ou zéro). De là, on voit tout de suite que $\mathfrak{S}$ est contenu dans un ensemble de la forme $K.L.\omega$, où ω est compact dans $M'_{\mathbf{R}}.U'_{\mathbf{R}}$ et où :

$$L = \{a \in {}_{F'}A_u, \quad a^\alpha \geqq u' > 0 \quad (a \in \theta)\}$$

pour des constantes $u > u' > 0$ convenables.

En particulier, $\mathfrak{S}$ est un ensemble de Siegel sur F′ si $\mathrm{rg}_F(G) = \mathrm{rg}_{F'}(G)$.

Si G est anisotrope sur F, alors un ensemble de Siegel est simplement un voisinage compact (ou relativement compact) de l'élément neutre invariant à gauche par K.

Si G est un tore décomposé sur $\mathbf{R}$, alors $\mathfrak{S} = G_{\mathbf{R}}$.

Supposons que G soit le produit presque direct de deux F-sous-groupes G_1, G_2, soient $\mathfrak{S}_i$ un ensemble de Siegel de G_i $(i = 1, 2)$, et K un sous-groupe compact maximal de $G_{\mathbf{R}}$ contenant le sous-groupe compact maximal K_i de $G_{i\mathbf{R}}$ intervenant dans la définition de $\mathfrak{S}_i$ $(i = 1, 2)$. Alors $K.\mathfrak{S}_1.\mathfrak{S}_2$ est un ensemble de Siegel de $G_{\mathbf{R}}$. Cela résulte de la définition et des remarques à 11.8. On ne peut toujours se borner à prendre $\mathfrak{S}_1.\mathfrak{S}_2$ car $G_{1\mathbf{R}}.G_{2\mathbf{R}}$ peut être un sous-groupe propre (toujours d'indice fini cependant) de $G_{\mathbf{R}}$. Par suite, le produit $K_1.K_2$ de sous-groupes compacts maximaux de $G_{1\mathbf{R}}$ et $G_{2\mathbf{R}}$ est un sous-groupe ouvert, qui peut être propre, d'un sous-groupe compact maximal K de $G_{\mathbf{R}}$. Dans ce cas, $K.\mathfrak{S}_1.\mathfrak{S}_2$ est la réunion des translatés de $\mathfrak{S}_1.\mathfrak{S}_2$ par un système de représentants de $K/K_1.K_2$.

En utilisant 11.8 et ce qui précède, on voit de même que si $f : G \to G'$ est un morphisme surjectif, et $\mathfrak{S}$ un domaine de Siegel de G, par rapport à K, P, S, alors $f(\mathfrak{S})$ est contenu dans un domaine de Siegel, par rapport à $f(P)$, $f(S)$ et à un sous-groupe compact maximal contenant $f(K)$.

Si $F = \mathbf{R}$, ou plus généralement si S est aussi décomposé maximal sur $\mathbf{R}$, et si $\mathfrak{S}$ est normal, alors $M_{\mathbf{R}} \subset K$ et l'on peut prendre pour ω un compact de $U_{\mathbf{R}}$. On retrouve

en particulier les ensembles de Siegel de $\mathbf{GL}(n, \mathbf{R})$ introduits au § 1, qui seront appelés *ensembles de* Siegel *standards de* $\mathbf{GL}(n, \mathbf{R})$.

12.4. Il est clair que $K.\mathfrak{S} = \mathfrak{S}$. D'autre part, si η est un compact de $P_{\mathbf{R}}^0$, alors il existe $t' > 0$ et ω' compact dans $M_{\mathbf{R}}^0.U_{\mathbf{R}}$ tels que :

$$\mathfrak{S}_{t,\omega}.\eta \subset \mathfrak{S}_{t',\omega'}. \tag{1}$$

Il suffit de montrer cela lorsque $\eta = \alpha.\beta.\gamma$, où α, β, γ sont des compacts de ${}_{\mathrm{F}}A$, $M_{\mathbf{R}}^0$ et $U_{\mathbf{R}}^0$ respectivement. Or, on a :

$${}_{\mathrm{F}}A_t.\omega.\alpha.\beta.\gamma = {}_{\mathrm{F}}A_t.\alpha.(\alpha^{-1}.\omega.\alpha).\beta.\gamma.$$

Il suffit donc de prendre $t' > 0$ tel que ${}_{\mathrm{F}}A_t.\alpha \subset {}_{\mathrm{F}}A_{t'}$ et de poser :

$$\omega' = \alpha^{-1}.\omega.\alpha.\beta.\gamma.$$

Dans le même ordre d'idées, remarquons que si η est un compact de $G_{\mathbf{R}}$, alors il existe $t' > 0$ tel que :

$$\eta.K.P_t \subset K.P_{t'}, \qquad \eta.K.P_t^0 \subset K.P_{t'}^0. \tag{2}$$

Comme $G_{\mathbf{R}} = K.P_{\mathbf{R}}^0$, on peut se borner au cas où $\eta \subset P_{\mathbf{R}}^0$ et est un produit $\eta = \alpha.\beta.\gamma$, avec α, β, γ compacts dans $M_{\mathbf{R}}^0.{}_{\mathrm{F}}A$ et $U_{\mathbf{R}}$ respectivement. Il suffit alors de choisir t' tel que $\beta.{}_{\mathrm{F}}A_t \subset {}_{\mathrm{F}}A_{t'}$.

12.5. LEMME. *Supposons* $X(G^0)_{\mathrm{F}} = \{1\}$. *Alors un ensemble de Siegel est de mesure de Haar finie.*

La démonstration est en principe semblable à celle donnée au § 1, pour les ensembles de Siegel de $\mathbf{SL}(n, \mathbf{R})$. L'application : $(k, p) \mapsto k.p$ est une application propre de $K \times P_{\mathbf{R}}^0$ sur $G_{\mathbf{R}}$. L'image réciproque d'une mesure de Haar de $G_{\mathbf{R}}$ est invariante par translations à gauche de K et à droite de $P_{\mathbf{R}}^0$. C'est donc le produit d'une mesure de Haar dk sur K par une mesure de Haar invariante à droite dp de $P_{\mathbf{R}}^0$. On a :

$$\int_{\mathfrak{S}} dg \leqq \int_K dk. \int_{{}_{\mathrm{F}}A_t.\alpha.\beta} dp,$$

où α (resp. β) est un voisinage compact de e dans $M_{\mathbf{R}}^0$ (resp. $U_{\mathbf{R}}$). Le groupe $P_{\mathbf{R}}^0$ est le produit semi-direct de $Z(S)_{\mathbf{R}}^0$ et du sous-groupe normal $U_{\mathbf{R}}$, qui sont tous deux unimodulaires. Par suite, on a $dp = ds.du.\rho(z)$ où ds (resp. du) est une mesure de Haar sur $Z(S)_{\mathbf{R}}^0$ (resp. $U_{\mathbf{R}}$) et où :

$$\rho(z) = |\det(\mathrm{Ad}\ z)_{\mathfrak{u}_{\mathbf{R}}}| \qquad (z \in Z(S)_{\mathbf{R}}^0).$$

D'autre part, $Z(S)_{\mathbf{R}}^0 = M_{\mathbf{R}}^0.{}_{\mathrm{F}}A$ et comme M est anisotrope sur F, le caractère ρ est égal à un sur M. On peut donc écrire :

$$ds = dm.da.\rho(a),$$

où dm et da sont des mesures de Haar sur $M_{\mathbf{R}}$ et ${}_{\mathrm{F}}A$ respectivement, d'où :

$$\int_{\mathfrak{S}} dg = c \int_\alpha dm \int_\beta du \int_{{}_{\mathrm{F}}A_t} \rho(a)\, da. \tag{1}$$

Les deux premières intégrales de droite sont finies, non nulles. Le caractère ρ est la somme des racines positives (chacune comptée avec sa multiplicité), et peut s'écrire sous la forme $\rho = \sum_{\alpha \in {}_F\Delta} c_\alpha . \alpha$, avec c_α entier > 0. L'exponentielle est un isomorphisme de ${}_F\mathfrak{a}$ sur ${}_F\mathrm{A}$ qui transporte une mesure de Lebesgue en une mesure de Haar. Comme $\mathrm{X}(\mathrm{G}^0)_F = \{1\}$, les α forment une base de $\mathrm{X}(\mathrm{S})$. Leurs différentielles forment donc un système de coordonnées sur $\mathfrak{s}_\mathbf{R}$. La dernière intégrale de droite dans (1) est donc de la forme :

$$c' . \prod_{\alpha \in {}_F\Delta} \int_{-\infty}^{\log t} e^{c_\alpha . \alpha} \, d\alpha$$

et est finie puisque $c_\alpha > 0 \quad (\alpha \in {}_F\Delta)$.

12.6. PROPOSITION. *Soit $\mathfrak{S}$ un domaine de Siegel sur* F *de* G, *et soit $c \in \mathrm{G}_\mathbf{R}$ tel que $\mathfrak{S}.c \cap \mathfrak{S}$ ne soit pas compact. Alors c fait partie d'un sous-groupe parabolique propre contenant* P. *Plus précisément, on a $c \in \mathrm{P}_\theta$ où θ est le complément dans ${}_F\Delta$ de l'ensemble ψ des k-racines simples β pour lesquelles on peut trouver une suite d'éléments $x_j \in \mathfrak{S}$ telle que $x_j^\beta \to 0$ et $x_j . c \in \mathfrak{S}$.*

(i) On suppose tout d'abord $c \in \mathrm{G}_\mathbf{F}$. On a pour $\eta \in {}_F\Delta$:

$$\mathrm{P}_{{}_F\Delta - \psi} \cap \mathrm{P}_{{}_F\Delta - \eta} = \mathrm{P}_{{}_F\Delta - (\psi \cup \eta)}.$$

Il suffit donc de prouver que si $x_j^\beta \to 0 \quad (x_j, x_j . c \in \mathfrak{S}; \quad j = 1, 2, \ldots)$ alors $c \in \mathrm{P}_\theta \quad (\theta = {}_F\Delta - \{\beta\})$.

Soient :

$$x_j = k_j . m_j . s_j . n_j, \qquad x_j c = k'_j . m'_j . s'_j . n'_j,$$

des décompositions de x_j, et $x_j . c$ suivant K, M, S, U et :

$$c = u . q . v \qquad (u, v \in \mathrm{U}_\mathbf{F}; \quad q \in \mathrm{N}(\mathrm{S})_\mathbf{F})$$

la décomposition de Bruhat de c. On a remarqué (11.19) que :

$$\mathrm{N}(\mathrm{S})_\mathbf{R} = (\mathrm{K} \cap \mathrm{N}(\mathrm{S})) . \mathrm{Z}(\mathrm{S})_\mathbf{R}.$$

On peut donc écrire $q = w . z \quad (w \in \mathrm{K} \cap \mathrm{N}(\mathrm{S})_\mathbf{R}, \quad z \in \mathrm{Z}(\mathrm{S})_\mathbf{R})$, et l'on a :

$$k_j . m_j . s_j . n_j . u . w . z . v = k'_j . m'_j . s'_j . n'_j.$$

On a :

$$k_j . m_j . s_j . n_j . u . w . z . v = k_j . {}^{m_j s_j}(n_j . u) \; m_j . s_j . w . z . v$$

$$k_j . m_j . s_j . n_j . u . w . z . v = k_j . w . d_j . {}^{w^{-1}}m_j . {}^{w^{-1}}s_j . z . v \qquad (d_j = {}^{w^{-1} . m_j . s_j}(n_j . u)).$$

Les éléments m_j et n_j restent dans des compacts puisque $x_j \in \mathfrak{S}$, donc, vu 12.2, l'élément d_j reste borné lorsque $j \to \infty$. Il en est alors de même de ses composantes suivant K, M, S, U. Comme $w^{-1} . m_j . w \in \mathrm{M}$ (11.6), on voit tout de suite que :

$$s'_j = s_{d_j} . {}^{w^{-1}}s_j . s_z$$

où s_z et s_{d_j} sont les composantes en S de z et d_j. Soit $\alpha \in {}_F\Delta$. Comme s_{d_j} est borné, et que $s_j'^{\alpha} \prec 1$ (puisque $x_j . c \in \mathfrak{S}$), il s'ensuit que :

$$({}^{w^{-1}}s_j)^\alpha = s_j^{w(\alpha)} \prec 1 \qquad (j = 1, 2, \ldots; \quad \alpha \in {}_F\Delta).$$

Posons comme en 11.11, $w(\alpha) = \sum_{\gamma} n_{\alpha\gamma}(w).\gamma$. On a donc :

$$s_j^{w(\alpha)} = \prod_{\gamma \in {}_F\Delta} s_j^{n_{\alpha\gamma}.\gamma} \prec 1.$$

Supposons $\eta_{\alpha\beta} < 0$, alors $w(\alpha) < 0$, donc $n_{\alpha\gamma} \leqq 0$ pour tout γ, et chaque facteur de droite est > 1. Comme le produit est $\prec 1$, cela entraîne $s_j^{\beta} \asymp 1$, contrairement à l'hypothèse. Par suite, on a $n_{\alpha\beta} \geqq 0$ pour tout $\alpha \in {}_F\Delta$, et 11.11 montre que $c \in {}_F\mathfrak{P}_\theta$.
(ii) Soit T un tore décomposé sur $\mathbf{R}$ maximal contenant S, avec $\mathfrak{t}_{\mathbf{R}}$ orthogonal à $\mathfrak{k}$. On munit $\mathbf{X}(T)$ et $\mathbf{X}(S)$ d'ordres compatibles, le deuxième étant associé à P. Soit P' un $\mathbf{R}$-sous-groupe parabolique minimal correspondant aux $\mathbf{R}$-racines positives. Alors $\mathfrak{S}$ est contenu dans un domaine de Siegel $\mathfrak{S}'$ sur $\mathbf{R}$, relatif à K, P', T (12.3). Soit η l'ensemble des éléments de ${}_{\mathbf{R}}\Delta$ dont la restriction à S est un élément de ψ. La partie (i) de la démonstration, appliquée à $k = \mathbf{R}$ et $\mathfrak{S}'$ montre que c fait partie du $\mathbf{R}$-groupe parabolique ${}_{\mathbf{R}}\mathfrak{P}_\zeta$, avec $\zeta = {}_{\mathbf{R}}\Delta - \eta$. Mais il résulte des définitions que ${}_{\mathbf{R}}\mathfrak{P}_\zeta = {}_F\mathfrak{P}_\theta$.

12.7. Pour obtenir les théorèmes de réduction lorsque G n'est pas connexe, nous aurons besoin d'un léger renforcement de 12.4. On conserve les notations précédentes et on note H le sous-groupe de $G_{\mathbf{R}}$ formé des composantes connexes de $G_{\mathbf{R}}$ qui contiennent un élément n du normalisateur de ${}_FA$. Évidemment Int n transforme les racines positives en racines positives pour un autre ordre donc, vu 11.12, 11.21, la composante $n.G_{\mathbf{R}}^0$ contient aussi un élément n' normalisant ${}_FA$ et permutant les racines positives. Dans ce cas, n' normalise aussi $U_{\mathbf{R}}$, et $P_{\mathbf{R}} = \mathrm{Norm}_{G_{\mathbf{R}}}(U_{\mathbf{R}})$. Cela étant dit, montrons que 12.4 reste vrai si $\mathfrak{S}$ est normal, et η est remplacé par un compact du normalisateur Q de $P_{\mathbf{R}}$ dans H.
Le groupe $L = N_H({}_FA) \cap Q$ rencontre toute composante connexe de $P_{\mathbf{R}}$ puisque $P_{\mathbf{R}} = Z(A)_{\mathbf{R}}.U_{\mathbf{R}}$, et toute composante connexe de H par définition de H. Comme $L \cap U_{\mathbf{R}} = \{e\}$ et $L.U_{\mathbf{R}} \supset P_{\mathbf{R}}$, il s'ensuit immédiatement que Q est le produit semi-direct de L et $U_{\mathbf{R}}$. D'autre part, L est stable par l'involution de Cartan associée à K, donc (9.3) le groupe $L \cap K$ est un sous-groupe compact maximal de L et $L = (L \cap K).Z({}_FA)_{\mathbf{R}}^0$. Vu 12.4, on est donc ramené au cas où $\eta \subset L \cap K$. Soit $g \in L$. Alors Int g laisse S et U stables donc permute les F-racines simples, d'où $g.{}_FA_t.g^{-1} = {}_FA_t$. D'autre part, g normalise $M_{\mathbf{R}}^0.U_{\mathbf{R}}^0$ car ce groupe est la composante neutre de l'intersection des noyaux des $\alpha \in {}_F\Delta$, vus comme caractères de $P_{\mathbf{R}}$. On a donc, si $\eta \in L \cap K$:

$$K.{}_FA_t.\omega.\eta \subset K.\eta.{}_FA_t.(\eta^{-1}.\omega.\eta) = K.{}_FA_t.\omega', \qquad (\omega' = \eta^{-1}.\omega.\eta),$$

d'où notre assertion.

§ 13. Ensembles fondamentaux (deuxième type)

Le but de ce paragraphe est de démontrer le théorème 13.1, qui fournit des ensembles fondamentaux en général plus maniables que ceux du § 9. En fait, on se bornera ici à établir qu'ils vérifient les conditions (F_0) et (F_1) de 9.6, réservant au § 15 l'étude de la propriété de Siegel.

13.1. THÉORÈME. *Soient* G *un* $\mathbf{Q}$*-groupe réductif,* P *un* $\mathbf{Q}$*-sous-groupe parabolique minimal de* G, S *un tore décomposé sur* $\mathbf{Q}$ *maximal de* P *et* K *un sous-groupe compact maximal de* $G_{\mathbf{R}}$. *Soit* Γ *un sous-groupe arithmétique de* G. *Alors il existe un ensemble de Siegel (par rapport à* K, P, S) $\mathfrak{S}$ *et une partie finie* C *de* $G_{\mathbf{Q}}$ *tels que :*

$$G_{\mathbf{R}} = \mathfrak{S}.C.\Gamma \tag{1}$$

Avant de passer à la démonstration, indiquons un corollaire.

13.2. COROLLAIRE. *Si* $X(G^0)_{\mathbf{Q}} = \{1\}$, *alors* $G_{\mathbf{R}}/\Gamma$ *est de mesure invariante finie.*

Cela résulte du théorème et du fait que $\mathfrak{S}$ est de mesure de Haar finie (12.5).

13.3. Nous montrons tout d'abord que si 13.1 est vrai pour un choix de K, il l'est pour tout autre sous-groupe compact maximal K'. D'après 12.4, il existe $t' > 0$ tel que :

$$K.P_t \subset K'.P_{t'}. \tag{1}$$

Soit $\Gamma' = \Gamma \cap \left(\bigcap_{c \in C}{}' {}^c\Gamma \right)$. C'est un groupe arithmétique (7.13), qui vérifie visiblement :

$$\Gamma'.C \subset C.\Gamma. \tag{2}$$

D'après le critère de compacité (8.7), il existe des compacts $\alpha \subset M^0_{\mathbf{R}}$, $\beta \subset U_{\mathbf{R}}$ tels que :

$$M^0_{\mathbf{R}} = \alpha.(\Gamma' \cap M), \qquad U_{\mathbf{R}} = \beta.(\Gamma' \cap U). \tag{3}$$

Utilisant le fait que $K'.P^0_t = K'.M^0_{\mathbf{R}}.{}_{\mathbf{Q}}A_t.U_{\mathbf{R}}$, on voit que :

$$K'.P_{t'}.C \subset K'.{}_{\mathbf{Q}}A_{t'}.\alpha.(M \cap \Gamma').U_{\mathbf{R}}.C = \\ = K'.{}_{\mathbf{Q}}A_{t'}.\alpha.U_{\mathbf{R}}(M \cap \Gamma').C \subset K'.{}_{\mathbf{Q}}A_{t'}.\alpha.\beta.\Gamma'.C$$

d'où, vu (1), (2) :

$$K.P_t.C \subset K'.A_{t'}.\omega'.C.\Gamma \qquad (\omega' = \alpha.\beta). \tag{4}$$

13.4. Comme K rencontre chaque composante connexe de $G_{\mathbf{R}}$, il suffit évidemment de démontrer le théorème lorsque $G_{\mathbf{C}}$ est connexe. Supposons G plongé dans $\mathbf{GL}_n$. On a vu (9.8, 9.9) qu'étant donné $u \in \mathbf{GL}(n, \mathbf{R})$ tel que $u.G_{\mathbf{R}}.u^{-1}$ soit auto-adjoint, il existe un domaine de Siegel standard $\mathfrak{S}$ de $\mathbf{GL}(n, \mathbf{R})$ et une partie finie B de $\mathbf{GL}(n, \mathbf{Q})$ tels que $G_{\mathbf{R}} = (u^{-1}.\mathfrak{S}.B \cap G_{\mathbf{R}}).\Gamma$.

D'autre part, on sait que l'on peut trouver u tel que $u.G_{\mathbf{R}}.u^{-1}$ soit auto-adjoint et même « bien placé » dans $\mathbf{GL}(n, \mathbf{R})$ (cf. 11.25). Le théorème 13.1 est donc conséquence des faits qui viennent d'être rappelés et du

13.5. THÉORÈME. *Nous conservons les hypothèses et notations de* 13.1, *supposons* G *connexe, et* $S_{\mathbf{R}}$ *stable par l'involution de Cartan associée à* K. *Soient* u *un élément de* $\mathbf{GL}(n, \mathbf{R})$ *tel que* $u.G_{\mathbf{R}}.u^{-1}$ *soit bien placé,* $b \in \mathbf{GL}(n, \mathbf{Q})$ *et* $\mathfrak{S}_0$ *un ensemble de Siegel standard de* $\mathbf{GL}(n, \mathbf{R})$. *Alors il existe un ensemble de Siegel* $\mathfrak{S}$ *de* $G_{\mathbf{R}}$, *par rapport à* K, P, S, *et une partie finie* C *de* $G_{\mathbf{Q}}$ *tels que :*

$$u^{-1}.\mathfrak{S}_0.b \cap G_{\mathbf{R}} \subset \mathfrak{S}.C.\Gamma. \tag{1}$$

La démonstration est dans son principe tout à fait semblable à celle du § 7 de [5], qui établit la finitude du volume en prouvant une inégalité semblable à la précédente, mais où $\mathfrak{S}$ désigne un domaine de Siegel sur $\mathbf{R}$ de $G_{\mathbf{R}}$ et C une partie finie de $G_{\mathbf{R}}$.

13.6. *Notations.* K_0, A_0, N_0 est la décomposition d'Iwasawa standard de $\mathbf{GL}(n, \mathbf{R})$. On écrit ${}_{\mathbf{Q}}A$ pour $S^0_{\mathbf{R}}$. Soit $G_{\mathbf{R}} = K.A.N$ une décomposition d'Iwasawa de $G_{\mathbf{R}}$ telle que $A \supset {}_{\mathbf{Q}}A$, et que N et U soient associés aux racines positives pour des ordres compatibles sur $X(A_{\mathbf{C}})$ et $X(S)$. En particulier $N \supset U_{\mathbf{R}}$. Comme les décompositions d'Iwasawa de $G_{\mathbf{R}}$ sont conjuguées, on peut, quitte à remplacer u par $u.v$ ($v \in G_{\mathbf{R}}$), supposer que :

$$(1) \qquad {}^uK = K_0 \cap {}^uG, \qquad {}^uA = A_0 \cap {}^uG, \qquad {}^uN = N_0 \cap {}^uG$$

et qu'il y a compatibilité entre l'ordre sur $X(A_{0,\mathbf{C}})$ et l'ordre sur $X({}^uA_{\mathbf{C}})$ obtenu, par l'isomorphisme induit par u, à partir de l'ordre donné sur $X(A_{\mathbf{C}})$.

13.7. *(a)* Remarquons tout d'abord que, vu 13.3 (4), il suffit d'établir l'existence de $t > 0$ et d'une partie finie C de $G_{\mathbf{Q}}$ telle que :

$$(1) \qquad u^{-1}.\mathfrak{S}_0.b \cap G_{\mathbf{R}} \subset K.P_t.C.$$

(b) Soit $q \in \mathbf{GL}(n, \mathbf{Q})$. Montrons que si l'assertion (1) est vraie pour ${}^qG$, elle l'est pour G. Pour cela on applique (1), en remplaçant u, G, b par $u.q^{-1}$, ${}^qG$ et $b.q^{-1}$. Cela montre l'existence de $t > 0$ et d'une partie finie C′ de ${}^qG_{\mathbf{Q}}$ tels que :

$$(2) \qquad q.u^{-1}.\mathfrak{S}_0.b.q^{-1} \cap {}^qG \subset {}^qK.{}^qP_t.C'.$$

Il suffit alors de conjuguer les deux membres de cette relation par $\mathrm{Int}\, q^{-1}$ pour obtenir (1).

(c) Quitte à remplacer G par ${}^qG$ ($q \in \mathbf{GL}(n, \mathbf{Q})$), on peut supposer que $S \subset D$ (D étant le groupe des matrices diagonales de $\mathbf{GL}_n$), $U_{\mathbf{R}} \subset N_0$ et que les ordres sur $X(D)$ et $X(S)$ sont compatibles.

En appliquant à $\mathbf{GL}_n$ le théorème de conjugaison des sous-groupes trigonalisables sur $\mathbf{Q}$ (11.10), on peut tout d'abord se ramener au cas où :

$$(3) \qquad S \subset D, \qquad U_{\mathbf{R}} \subset N.$$

Vu 13.6, on a :

$${}^u_{\mathbf{Q}}A \subset {}^uA \subset A_0, \qquad {}^uU_{\mathbf{R}} \subset {}^uN \subset N_0.$$

Ainsi, ${}^uS$ et S sont deux sous-tores de D, conjugués par un élément de $\mathbf{GL}(n, \mathbf{R})$. Comme D est un tore décomposé sur D maximal de $\mathbf{GL}_n$, il existe (11.12) un élément $v \in N(D)_{\mathbf{Q}} = N(A)$, tel que :

$$v.x.v^{-1} = u.x.u^{-1}, \qquad (x \in {}_{\mathbf{Q}}A).$$

On a donc $u = z.v$ ($z \in Z({}^uS)_{\mathbf{Q}}$). Les ordres sur $X(D)$ et $X({}^uA_{\mathbf{C}})$ d'une part, sur $X({}^uA_{\mathbf{C}})$ et $X({}^uS) = X({}^vS)$ d'autre part, étant compatibles, il en est de même des ordres sur $X(S)$ et $X({}^vS)$; en particulier, ${}^vU_{\mathbf{R}} \subset N$. Le groupe ${}^vG$ vérifie

donc les conditions énoncées dans *(c)*, d'où notre assertion, compte tenu de *(b)*.
(d) L'algèbre de Lie $\mathfrak{n}_0$ de N_0 est somme directe de la sous-algèbre :

$$\mathfrak{n}_1 = \mathfrak{n}_0 \cap \mathfrak{z}(S) = \sum_{\alpha>0,\,\alpha(S)=1} \mathfrak{g}_{\alpha\mathbf{R}}$$

et du sous-espace :

$$\mathfrak{n}^+ = \sum_{\alpha>0,\,\alpha(S)\neq 1} \mathfrak{g}_{\alpha\mathbf{R}}$$

qui est visiblement un idéal. Par suite (11.13), l'application produit est un homéomorphisme de $N_1 \times N^+$ sur N_0 ($N_1 = \exp \mathfrak{n}_1$, $N^+ = \exp \mathfrak{n}^+$).
Le groupe $Z(S)$ laisse $\mathfrak{g}_\alpha$ et $\mathfrak{g}_\alpha \cap \mathfrak{u}$ stables. Comme il est réductif, défini sur $\mathbf{Q}$, il existe un $\mathbf{Q}$-sous-espace $\mathfrak{n}_{\alpha,2}$ supplémentaire de $\mathfrak{g}_\alpha \cap \mathfrak{u}$ dans $\mathfrak{g}_\alpha$, stable par $Z(S)$. Soient $\mathfrak{n}_2$ la somme des $\mathfrak{n}_{\alpha,2}$ ($\alpha > 0$, $\alpha(S) \neq 1$) et $N_2 = \exp \mathfrak{n}_{2,\mathbf{R}}$. Pour tout $\beta > 0$ non trivial sur S, la somme des sous-espaces $\mathfrak{g}_{\alpha\mathbf{R}}$ ($\alpha \geqq \beta$, $\alpha(S) \neq \{1\}$) est un idéal de $\mathfrak{n}^+$. Le lemme 11.13 montre donc que l'application produit est un homéomorphisme de $N_2.U_{\mathbf{R}}$ sur N^+, d'où finalement une décomposition topologique $N_0 = N_1.N_2.U_{\mathbf{R}}$ (qui est en fait birégulière sur $\mathbf{Q}$, mais nous n'aurons pas besoin de ce fait). Nous nous proposons maintenant de prouver qu'il suffit de démontrer (1) lorsque :

$$b = q^{-1}.v \qquad (q \in N(D)_{\mathbf{Q}},\quad v \in N_1.N_2). \tag{4}$$

En utilisant la décomposition de Bruhat de $\mathbf{GL}(n, \mathbf{Q})$ (cf. § 3), on peut écrire :

$$b = n'.t.w.n \qquad (n, n' \in N_{0,\mathbf{Q}},\quad t \in D_{\mathbf{Q}},\quad w \in N(D)_{\mathbf{Q}} \cap \mathbf{O}(n)). \tag{5}$$

D'autre part, $n = v.v'$ ($v \in N_1.N_2$, $v' \in U_{\mathbf{R}}$). Il existe un domaine de Siegel standard $\mathfrak{S}'$ de $\mathbf{GL}(n, \mathbf{R})$ tel que $\mathfrak{S}_0.n'.t \subset \mathfrak{S}'$, d'où :

$$u^{-1}.\mathfrak{S}.b \cap G \subset u^{-1}.\mathfrak{S}'.w.v.v' \cap G \subset (u^{-1}.\mathfrak{S}'.w.v \cap G).v'$$

et notre assertion.

(e) Comme $S \subset D$, le groupe $Z(S)$ est auto-adjoint dans $\mathbf{GL}(n, \mathbf{R})$, donc les composantes k, a, n de u dans la décomposition d'Iwasawa standard de $\mathbf{GL}(n, \mathbf{R})$ font partie de $Z(S)$. Posons :

$$K' = {}^{u^{-1}}K_0 = {}^{n^{-1}.a^{-1}}K_0, \qquad A' = {}^{n^{-1}.a^{-1}}A_0 = {}^{n^{-1}}A_0.$$

Évidemment, $N_0 = {}^{n^{-1}.a^{-1}}N_0$, donc $K'.A'.N_0$ est la décomposition d'Iwasawa de $\mathbf{GL}(n, \mathbf{R})$ conjuguée de $K_0.A_0.N_0$ par $n^{-1}.a^{-1}$. Écrivant $\mathfrak{S}_0$ sous la forme $\mathfrak{S}_0 = K_0.A_{0,t}.\omega$ (ω compact dans N_0), on a :

$$u^{-1}.\mathfrak{S}_0.q^{-1}.v = u^{-1}.K_0.A_{0,t}.\omega.q^{-1}.v = n^{-1}.a^{-1}.K_0.A_{0,t}.\omega.q^{-1}.v$$
$$u^{-1}.\mathfrak{S}_0.q^{-1}.v \subset K.n^{-1}.A_{0,t'}.\omega.q^{-1}.v \subset K'.A'_{t'}.\omega'.(n^{-1}q^{-1}n).n^{-1}.v$$

où t' est tel que $a^{-1}.A_{0,t} \subset A_{0,t'}$ et où $\omega' = n^{-1}.\omega.n$ Comme $n^{-1}q^{-1}n \in N(A')$, que $n.v \in N_1.N_2$, et que $K'.A'_{t'}.\omega'$ est un ensemble de Siegel par rapport à K', A', N_0, on est ramené au lemme suivant :

13.8. LEMME. *On conserve les notations de* 13.5. *Soient* $K'.A'.N_0$ *une décomposition d'Iwasawa de* $\mathbf{GL}(n, \mathbf{R})$ *telle que* $K' \supset K$, $A' \supset_{\mathbf{Q}} A$, $N_0 \supset U_{\mathbf{R}}$, *et que* N_0 *et* $U_{\mathbf{R}}$ *soient associés aux racines positives d'ordres compatibles sur* $X(A'_0)$ *et* $X(S)$. *Soient* $\mathfrak{S}'$ *un ensemble*

de Siegel de $\mathbf{GL}(n, \mathbf{R})$ *par rapport à* K', A', N_0, *et* $q \in N(A')_{\mathbf{R}}$, $v \in N_1 . N_2$ (*notation de* 13.7). *Pour tout* $w \in {}_{\mathbf{Q}}W(G, S)$, *soit* x_w *un représentant de* w *dans* $N(S)_{\mathbf{Q}}$. *Alors, il existe* $t > 0$ *tel que :*

$$\mathfrak{S}' . q^{-1} . v \subset \bigcup_{w \in {}_{\mathbf{Q}}W(G)} K . P_t . x_w .$$

Chaque composante de N(A') modulo Z(A') rencontre K' (11.19). Il existe donc $z \in Z(A')$ tel que $z . q^{-1} \in N(A') \cap K'$. Comme $\mathfrak{S}' . z$ est contenu dans un domaine de Siegel par rapport à K', A', N_0, on voit que l'on peut supposer :

$$q \in N(A') \cap K',$$

ce que nous ferons.

Soit $x \in \mathfrak{S}'$ et soit $x = k' . a' . n$ sa décomposition d'Iwasawa, par rapport à K', A', N_0. Supposons de plus $x \in G . v^{-1} . q$. On peut écrire :

$$x . q^{-1} . v = k' . a' . n . q^{-1} . v = k . m . s . u \tag{1}$$

où : $k \in K$, $m \in M^0_{\mathbf{R}}$, $s \in {}_{\mathbf{Q}}A$, $u \in U_{\mathbf{R}}$,

(11.19). Comme on l'a remarqué, le produit $k . m$, s et u sont complètement déterminés par le membre de gauche, et dépendent continûment de x. Les éléments k et m sont déterminés seulement au produit par un élément arbitraire du groupe compact $K \cap M^0_{\mathbf{R}}$ près. Mais cette indétermination est sans importance pour nous ici, car nous nous intéressons seulement à savoir si des éléments parcourent des parties bornées de $G_{\mathbf{R}}$.

(i) *A montrer : L'ensemble des éléments* ${}^{ms}u$ (*notations de* (1)), *où* x *parcourt* $\mathfrak{S}' \cap G . v^{-1} . q$, *est borné.*

On a :

$$x . q^{-1} . v = k' . q^{-1} . {}^{qa'}n . {}^{q}a' . v_1 . v_2 \qquad (v_1 \in N_1, \quad v_2 \in N_2). \tag{2}$$

Soit $c = {}^{qa'}n$. On peut l'écrire sous la forme :

$$c = k_c . m_c . a_c . n_c \qquad (k_c \in K', \quad m_c \in M^0_{\mathbf{R}}, \quad a_c \in {}_{\mathbf{Q}}A, \quad n_c \in N^+_{\mathbf{R}}). \tag{3}$$

Comme c est borné lorsque x parcourt $\mathfrak{S}'$, d'après 12.2, chaque facteur du membre de droite est aussi borné. Substituant dans (2), on obtient :

$$x . q^{-1} . v = k'' . m_c . a_c . {}^{q}a' . ({}^{q}a')^{-1} . n_c . {}^{q}a' . v_1 . v_2 \qquad (k'' = k' . q^{-1} . k_c \in K').$$

$$x . q^{-1} . v = (k'' . m_c . a_c . {}^{q}a' . v_1) . (v_1^{-1} . ({}^{q}a')^{-1} . n_c . {}^{q}a' . v_1) . v_2. \tag{4}$$

Comme $n_c \in N^+ = N_2 . U_{\mathbf{R}}$ et que ${}^{q}a' \in A'$ et $v_1 \in N^1$ normalisent N^+, le deuxième produit entre parenthèses du membre de droite est dans N^+, le premier fait partie de $K' . Z(S)_{\mathbf{R}}$. Comme $v_2 \in N^+$, on obtient, en comparant (1) et (4) :

$$m . s \in K' . m_c . a_c . {}^{q}a' . v_1 \in K' . Z(S)_{\mathbf{R}}, \qquad u . v_2^{-1} = v_1^{-1} . ({}^{q}a)^{-1} . n_c . {}^{q}a . v_1 \in N^+. \tag{5}$$

L'élément $m . s \in Z(S)$ laisse $U_{\mathbf{R}}$ et N_2 stables (cf. 13.7.*c*), donc ${}^{m . s}u$ est la composante dans $U_{\mathbf{R}}$ de ${}^{ms}(u . v_2^{-1})$. Il suffit par conséquent de voir que ce dernier élément est borné. Vu (5), cela revient à prouver que :

$$z = \mathrm{Int}\,(m_c . a_c . {}^{q}a . v_1) . \mathrm{Int}\,(v_1^{-1} . ({}^{q}a)^{-1})\,(u_c) = \mathrm{Int}\,(m_c . a_c)\,(u_c)$$

est borné, mais cela résulte du fait remarqué plus haut (cf. (3)), que m_c, a_c, u_c sont bornés.

(ii) *Démonstration du lemme* 13.8 : Soit :

$$C = \{a \in {}_{\mathbf{Q}}A \mid a^{\alpha} \leqq 1, \quad (\alpha \in {}_{\mathbf{Q}}\Delta)\}.$$

Soit, pour $w \in {}_{\mathbf{Q}}^{\mathbf{R}}W(G, S)$:

$$M_w = \{x \in \mathfrak{S}'.q^{-1}.v \cap G \mid x_w.s.x_w^{-1} \in C\},$$

où s est défini par (1). Comme C est un domaine fondamental pour ${}_{\mathbf{Q}}W$ dans ${}_{\mathbf{Q}}A$, $\mathfrak{S}'.q^{-1}.v \cap G$ est la réunion des M_w $(w \in {}_{\mathbf{Q}}W)$, et il suffit de montrer qu'il existe $t > 0$ tel que :

$$M_w \subset K.P_t.x_w. \tag{6}$$

On peut trouver (11.19) un élément $y_w \in K$ tel que $y_w.x_w^{-1} \in Z(S)$. Il existe donc $t' > 0$ tel que :

$$P_t.y_w \subset P_{t'}.x_w,$$

et on est ramené à prouver que l'on a :

$$M_w \subset K.P_t.y_w \tag{7}$$

pour $t > 0$ convenable. On a (cf. (1)) :

$$x.q^{-1}.v = k.m.s.u = k.{}^{ms}u.m.s$$

$$z = x.q^{-1}.v.y_w^{-1} = k.y_w^{-1}.y_w.({}^{m.s}u).y_w^{-1}.(y_w.m.y_w^{-1}).(y_w.s.y_w^{-1}).$$

Posons $d = y_w.({}^{m.s}u).y_w^{-1}$. On a une décomposition :

$$d = k_d.m_d.s_d.u_d \qquad (k_d \in K, \quad m_d \in M_{\mathbf{R}}^0, \quad s_d \in {}_{\mathbf{Q}}A, \quad u_d \in U_{\mathbf{R}}),$$

d'où :

$$z = k''.m_d.s_d.u_d.(y_w.m.y_w^{-1}).(y_w.s.y_w^{-1}), \qquad (k'' = k.y_w^{-1}.k_d \in K).$$

L'élément y_w normalise S, donc M (cf. 11.6). Comme M normalise $U_{\mathbf{R}}$, on voit que l'on peut écrire :

$$z = (k''.m_d.y_w.m.y_w^{-1}).(s_d.y_w.s.y_w^{-1}).(u'),$$

où $u' \in U_{\mathbf{R}}$ est un conjugué de u_d dans $P_{\mathbf{R}}$, et où les trois facteurs définis par les parenthèses sont les composantes de z dans $K.M_{\mathbf{R}}^0$, ${}_{\mathbf{Q}}A$ et $U_{\mathbf{R}}$ respectivement. Ainsi la composante s_z en ${}_{\mathbf{Q}}A$ de z est égale à $s_d.(y_w.s.y_w^{-1})$. D'après (i), s_d parcourt un ensemble borné lorsque $x \in \mathfrak{S}'.q^{-1}.v \cap G$. Supposons $x \in M_w$. Alors $y_w.s.y_w^{-1} \in C$. Il existe donc $t > 0$ tel que :

$$s_z = s_d.y_w.s.y_w^{-1} \in {}_{\mathbf{Q}}A_t$$

ce qui établit (7).

Note bibliographique

Dans le cas du groupe linéaire sur une algèbre à division sur $\mathbf{Q}$, le théorème 13.1 est équivalent à un théorème de réduction classique, que l'on trouve par exemple dans [32]. Le cas général est annoncé dans [2], et la démonstration donnée ci-dessus est celle à laquelle [2] fait allusion. Une démonstration très différente, basée sur la considération du groupe adélique de G, a été ensuite obtenue par Godement-Weil [12]. Nous en donnerons un analogue sur $G_{\mathbf{R}}$ au § 16.

14. Représentations fondamentales. Fonctions associées

14.1. Soient G un **R**-groupe réductif connexe, P un **R**-sous-groupe parabolique de G, et $\chi \in X(P)$. On dira qu'une fonction continue Φ sur $G_{\mathbf{R}}$, à valeurs réelles positives, est de type (P, χ) si elle vérifie :

$$\Phi(g.p) = \Phi(g).|p^{\chi}|, \qquad (g \in G_{\mathbf{R}}, \quad p \in P_{\mathbf{R}}).$$

Nous faisons tout d'abord quelques remarques simples sur les fonctions de ce type.

14.2. *(a)* Il existe toujours une fonction > 0 de type (P, χ), invariante à gauche par un sous-groupe compact maximal donné K. En effet, on a la décomposition $G_{\mathbf{R}} = K.P_{\mathbf{R}}^0$, et il est clair que $|p^{\chi}| = 1$ si p appartient à un sous-groupe compact de $P_{\mathbf{R}}$, en particulier, si $p \in K \cap P$. En posant $\Phi(k.p) = |p^{\chi}|$, on obtient donc une fonction sur $G_{\mathbf{R}}$ vérifiant nos conditions.
(b) Soient Φ, Φ' deux fonctions de type (P, χ), et supposons $\Phi' > 0$. Alors $\Phi \prec \Phi'$ sur $G_{\mathbf{R}}$.
La fonction Φ/Φ' a une borne supérieure $c > 0$ sur K. Comme $G_{\mathbf{R}} = K.P_{\mathbf{R}}^0$, et que l'on a :

$$(\Phi/\Phi')(g.p) = (\Phi/\Phi')(g) \qquad (g \in G_{\mathbf{R}}, \quad p \in P_{\mathbf{R}}),$$

il s'ensuit que $\Phi(g) \leqq c.\Phi'(g)$, $(g \in G_{\mathbf{R}})$.
En particulier, on voit que si Φ, Φ' sont toutes deux strictement positives, alors $\Phi \asymp \Phi'$.
(c) Soit C un compact de $G_{\mathbf{R}}$ et soit $\Phi > 0$ de type (P, χ). Alors :

$$\Phi(c.g) \asymp \Phi(g) \qquad (g \in G_{\mathbf{R}}; \quad c \in C).$$

En effet, on a, en posant $g = k.p$ $(k \in K, \ p \in P_{\mathbf{R}})$:

$$\Phi(c.g)/\Phi(g) = \Phi(c.k)/\Phi(k),$$

et il suffit de remarquer que, puisque K est compact, le membre de droite est $\asymp 1$ lorsque $c \in C$, $k \in K$.

14.3. Soit $\pi : G \to GL(V)$ une représentation de dimension finie de G. Supposons que V contienne une droite D stable par P, et soit χ le caractère de la représentation induite de P dans D. Munissons V d'une norme hilbertienne $||\ ||$, et soit e_0 un vecteur sous-tendant D. Alors, la fonction :

$$\Phi(g) = ||\pi(g).e_0||$$

est évidemment > 0, de type (P, χ); si $\pi(h)$ $(h \in G)$ est unitaire, alors Φ est invariante à gauche par h.
Les propriétés les plus importantes des fonctions de type (P, χ) seront établies en considérant des fonctions construites par ce procédé.

14.4. Soit k un sous-corps de **R**, et supposons que P soit un k-groupe parabolique minimal. Soit S un tore décomposé sur k maximal de P et ${}_k\Delta$ l'ensemble des racines

simples de G par rapport à S, pour un ordre associé à P. On suppose $\mathbf{X}(S) \otimes \mathbf{Q}$ muni d'un produit scalaire $(\ ,\ )$ euclidien invariant par le groupe de Weyl relatif ${}_kW(G)$. Un élément $\chi \in \mathbf{X}(P)_k$ est dit *dominant* si $(\chi, \alpha) \geqq 0$ $(\alpha \in {}_k\Delta)$. Pour tout $\alpha \in {}_k\Delta$, on choisit un élément $\Lambda_\alpha \in \mathbf{X}(P)_k$, trivial sur $Z(G)^0$, vérifiant :

$$(\Lambda_\alpha, \beta) = d_\alpha . \delta_{\alpha\beta} \qquad (d_\alpha > 0, \quad \alpha, \beta \in {}_k\Delta) \tag{1}$$

et on appellera les Λ_α les *k-poids dominants fondamentaux* de $\mathfrak{D}G$. Un élément $\chi \in \mathbf{X}(P)_k$ est donc dominant si, et seulement si, un multiple positif de χ est somme d'une combinaison linéaire à coefficients entiers $\geqq 0$ des Λ_α, et d'un caractère trivial sur $P \cap \mathfrak{D}G$.

Étant donné un poids dominant χ, trivial sur $Z(G)^0 \cap \mathfrak{D}G$, il existe une représentation irréductible $\pi : G \to GL(V)$ définie sur k, et une droite $D_\pi \subset V$, définie sur k, stable par P, sur laquelle P agit par l'intermédiaire de χ. Pour $\mu \in \mathbf{X}(S)$, soit :

$$V_\mu = \{ v \in V, \pi(s) . v = s^\mu . v (s \in S) \}.$$

C'est un k-sous-espace de V. On dit que μ est un k-poids de π si $V_\mu \neq 0$. On sait que V est la somme directe des V_μ, que V_χ est de dimension un, et que tout k-poids de π est de la forme :

$$\mu = \chi - \sum_{\alpha \in {}_k\Delta} c_\alpha(\mu) . \alpha \qquad (c_\alpha(\mu) \in \mathbf{N}). \tag{2}$$

En fait, cela est démontré dans [7, § 12] lorsque G est semi-simple. Mais l'extension au cas considéré ici est immédiate; en effet, soient χ_1, χ_2 les restrictions de χ à $Z(G)^0$ et $DG \cap P$, et σ la représentation de DG de poids dominant χ_2 donnée par [7, *loc. cit.*]. Alors, vu que χ est supposé trivial sur $Z(G)^0 \cap DG$, il est clair que $\chi_1 \otimes \sigma$ est une représentation de G ayant les propriétés requises. Remarquons encore que si χ est dominant, il admet toujours un multiple positif trivial sur $DG \cap Z(G)^0$, puisque ce groupe est fini.

Un groupe compact maximal K d'algèbre de Lie orthogonale à celle de $S_\mathbf{R}$ étant choisi, on munit $V_\mathbf{R}$ d'un produit scalaire euclidien par rapport auquel $\rho(g)$ est unitaire (resp. auto-adjoint) si $g \in K$ (resp. $g \in S_\mathbf{R}$), ce qui est toujours possible. En particulier, les sous-espaces V_μ sont mutuellement orthogonaux. La fonction $\Phi_\pi : g \mapsto \| \pi(g) . e_0 \|$ (e_0 : vecteur unitaire sous-tendant D_π) est alors > 0, de type (P, χ), invariante à gauche par K. On notera Φ_α la fonction ainsi obtenue pour $\chi = \Lambda_\alpha$. Étant donné $\chi \in \mathbf{X}(P)_k$ on obtient une fonction > 0 de type (P, χ) en posant :

$$\Phi = \prod_{\alpha \in {}_k\Delta} \Phi_\alpha^{d_\alpha}, \tag{3}$$

où les d_α sont les nombres rationnels positifs tels que $m\chi - \sum m d_\alpha \Lambda_\alpha$ soit un caractère trivial sur $Z(G)^0$ pour $m \in \mathbf{N}$ convenable.

Vu (14.2 *b*) toute fonction de type (P, χ) (resp. et > 0) est essentiellement dominée (resp. est comparable) à cette dernière.

Utilisant la décomposition $P = M.S.U$ de P, on peut écrire $g \in G_\mathbf{R}$ sous la forme :

$$g = k_g . m_g . s_g . u_g \qquad (k_g \in K, \quad m_g \in M_\mathbf{R}, \quad s_g \in S^0_\mathbf{R}, \quad u_g \in U_\mathbf{R}).$$

On a alors $\pi(g) . e_0 = \pi(k_g) . s_g^\chi . e_0$, d'où :

$$\Phi_\pi(g) = s_g^\chi. \tag{4}$$

14.5. *Exemple.* Soit $G = \mathbf{SL}_n$. Soient P (resp. S) le groupe des matrices triangulaires supérieures (resp. diagonales) de $\mathbf{SL}_n$ et $K = \mathbf{SO}(n)$. Les représentations fondamentales de G sont les puissances extérieures $\wedge^i$ $(1 \leqq i \leqq n-1)$ de la représentation identique. Dans les notations du § 1, les racines simples sont les quotients $a_{ii}/a_{i+1,i+1}$ $(i = 1, \ldots, n-1)$, la base duale Λ_α est formée de :

$$\Lambda_i = a_{11} \cdot \ldots \cdot a_{ii} \qquad (i = 1, \ldots, n-1);$$

la représentation irréductible de poids dominant Λ_i est la i-ème puissance extérieure. Dans $\wedge^i \mathbf{R}^n$, la droite stable par P est sous-tendue par $e_1 \wedge \ldots \wedge e_i$. Dans ce cas, les fonctions Φ_α ne sont donc autres que les fonctions Φ_i du § 1.

14.6. PROPOSITION. *On conserve les notations précédentes. Soient* $\chi \in X(P)_k$ *dominant et* Φ *une fonction* > 0 *de type* (P, χ). *Soit* $\mathfrak{S}$ *un domaine de Siegel de* $G_{\mathbf{R}}$ *par rapport à* K, P, S. *Alors :*

$$\Phi(x.y) \succ \Phi(x).\Phi(y) \qquad (x \in \mathfrak{S};\quad y \in G_{\mathbf{R}}).$$

Il suffit de démontrer cela pour la fonction $\Phi = \Phi_\pi$ de 14.4. On peut écrire :

$$\pi(g).e_0 = \sum_\mu f_\mu(g), \qquad (f_\mu(g) \in V_\mu;\quad g \in G_{\mathbf{R}}), \tag{1}$$

où μ parcourt les k-poids de π, d'où, puisque les espaces V_μ sont deux à deux orthogonaux :

$$\Phi(g)^2 = \sum \| f_\mu(g) \|^2.$$

En utilisant les décompositions $P = M.S.U$ et $G_{\mathbf{R}} = K.P^0_{\mathbf{R}}$ (cf. 11.19), on a :

$$x = k_x m_x s_x u_x \qquad (k_x \in K,\quad m_x \in M^0_{\mathbf{R}},\quad s_x \in S^0_{\mathbf{R}},\quad u_x \in U_{\mathbf{R}}),$$

d'où :

$$\| \pi(x.y).e_0 \| = \| \pi(s_x).\pi(m_x.u_x.y).e_0 \|$$

On a :

$$\pi(s_x).\pi(m_x.u_x.y).e_0 = \sum_\mu s_x^\mu . f_\mu(m_x.u_x.y),$$

donc

$$\Phi(x.y)^2 = \sum_\mu (s_x)^{2\mu} \| f_\mu(m_x.u_x.y) \|^2;$$

mais (14.4 (4)), on a $\Phi(x) = s_x^\varkappa$, donc compte tenu de (14.4 (2)).

$$\Phi(x.y)^2 = \Phi(x)^2 \sum_\mu \left(\prod_\alpha s_x^{-2c_\alpha(\mu).\alpha} \right) . \| f_\mu(m_x.u_x.y) \|^2. \tag{2}$$

Comme x est dans un domaine de Siegel, on a $s_x^\alpha \leqslant t$. Les $c_\alpha(\mu)$ étant $\geqq 0$, il en résulte que le produit figurant devant $\| f_\mu(m_x.u_x.y) \|^2$ dans (2) est $\succ 1$ lorsque $x \in \mathfrak{S}$, d'où :

$$\Phi(x.y)^2 \succ \Phi(x)^2 . \left(\sum_\mu \| f_\mu(m_x.u_x.y) \|^2 \right) = \Phi(x)^2 . \Phi(m_x.u_x.y)^2 \qquad (x \in \mathfrak{S},\quad y \in G_{\mathbf{R}}).$$

Les éléments m_x et u_x varient dans des compacts puisque $x \in \mathfrak{S}$, donc (14.2 *(c)*), $\Phi(m_x.u_x.y) \asymp \Phi(y)$, d'où le lemme.

14.7. NOTATION. Dans les paragraphes suivants, on utilisera simultanément des décompositions d'Iwasawa et de Bruhat. On écrira la décomposition de $x \in G_{\mathbf{R}}$ suivant K, M, S, U :

$$(1) \qquad x = k_x . m_x . s_x . n_x \qquad (k_x \in K, \quad m_x \in M^0_{\mathbf{R}}, \quad s_x \in S^0_{\mathbf{R}}, \quad n_x \in U_{\mathbf{R}}).$$

D'autre part, nous désignerons par la même lettre un élément $w \in {}_k W(G)$ et un représentant de w dans $N(S)_k$, choisi une fois pour toutes. Soit $\mathfrak{W}$ l'ensemble de ces représentants. Soit U^- le k-sous-groupe unipotent maximal correspondant aux k-racines négatives et soit U'_w le plus grand sous-groupe V de U tel que $w^{-1}.V.w \subset U^-$. On sait (§ 11) qu'étant donné $g \in G_k$, il existe un et un seul $w_g \in \mathfrak{W}$ tel que l'on ait :

$$(2) \qquad g = u_g . w_g . z_g . v_g, \qquad (u_g \in U'_{w_g,k}; \quad z_g \in Z(S)_k; \quad v_g \in U_k),$$

les facteurs de droite étant tous univoquement déterminés par g.

14.8. PROPOSITION. *On conserve les notations de* 14.6. *Soit* Φ *une fonction* > 0 *de type* (P, χ), *où* χ *est dominant. Alors :*

(i) $\Phi(s_g) \asymp \Phi(g) \asymp s_g^{\chi}$, $\qquad (g \in G_{\mathbf{R}})$,

(ii) $\Phi(u) \succ 1$, $\qquad (u \in U_{\mathbf{R}}^-)$.

(iii) *Une partie* C *de* $U_{\mathbf{R}}^-$ *est bornée si, et seulement si,* $\psi \asymp 1$ *sur* C *pour toute fonction* $\psi > 0$ *de type* (P, η) *et tout* $\eta \in X(P)_k$ *dominant.*

Démonstration. (i) Vu 14.2 *(b)*, il suffit de démontrer (i) pour la fonction Φ_π; dans ce cas on a égalité (14.4 (4)).

(ii) Il suffit de considérer la fonction Φ_π de 14.4. Or, on sait que U^- laisse stable la somme des espaces V_μ $(\mu \neq \chi)$, donc :

$$\pi(u).e_0 = e_0 + \sum_{\mu \neq \chi} f_\mu(u), \qquad (u \in U^-),$$

$$\Phi(u)^2 = 1 + \sum_{\mu \neq \chi} ||f_\mu(u)||^2 \geqq 1.$$

(iii) Comme $U^- \subset \mathfrak{D}G$, on peut se borner au cas où G est semi-simple. La nécessité de la condition est évidente. Soit η un poids dominant qui n'est orthogonal à aucune k-racine simple. Nous voulons montrer réciproquement que si $\Phi > 0$ de type (P, η) est $\asymp 1$ sur C, alors C est borné. On peut supposer que Φ est associée à une représentation irréductible (π, V) de poids dominant η. L'hypothèse faite sur η implique que P est tout le groupe de stabilité de la droite D_π engendrée par e_0 [7, § 12]. Par suite, l'application $\varphi : u \mapsto \pi(u).e_0$ est une application injective de U^- dans V. D'après un théorème de Rosenlicht [27, Thm. 2], $\varphi(U^-)$ est fermée. Par suite, φ induit un homéomorphisme de U^- sur $\varphi(U^-)$. Comme l'hypothèse signifie que l'image $\varphi(C)$ de C est bornée, il s'ensuit que C est borné.

14.9. COROLLAIRE. *Soit* B *une partie de* $G_{\mathbf{R}}$. *Alors l'ensemble des composantes* s_b $(b \in B)$ *est borné si, et seulement si,* $\Phi \asymp 1$ *sur* B *pour toute fonction* $\Phi > 0$ *de type* (P, χ) *et tout poids dominant* χ.

La nécessité de la condition résulte de 14.8 (i). Réciproquement, si cette condition est remplie, on a, vu 14.8, $s_b^\chi \asymp 1$ $(b \in B)$ pour tout χ dominant. Comme l'ensemble de ces caractères contient un système de coordonnées sur $S_{\mathbf{R}}^0$, la réciproque s'ensuit.

14.10. COROLLAIRE. *Dans les notations de* 14.7, *on a, pour tout poids dominant* χ *et toute fonction* $\Phi > 0$ *de type* (P, χ) :

$$\Phi(g) \asymp \Phi(s_g) \succ \Phi(z_g) \qquad (g \in G_k).$$

On peut se borner à une fonction $\Phi = \Phi_\pi$. On a :

$$\Phi(g) = \Phi(w_g.w_g^{-1}.u_g.w_g.z_g.v_g) \asymp \Phi(w_g^{-1}.u_g.w_g.z_g) = \Phi(w_g^{-1}.u_g.w_g).\Phi(z_g).$$

Comme $w_g^{-1}.u_g.w_g \in U^-$, le corollaire résulte alors de 14.8 (i), (ii).

§ 15. La propriété de Siegel

Nous nous proposons ici d'étendre au cas d'un groupe réductif les résultats du § 4, par des démonstrations semblables.

15.1. Dans ce paragraphe, k est un corps de caractéristique zéro, G un k-groupe réductif, P un k-sous-groupe parabolique minimal de G^0, S un tore décomposé sur k maximal de P. On fixe sur $\mathbf{X}(S)$ un ordre associé à P, et on dénote par D une base de $\mathbf{X}(S) \otimes \mathbf{Q}$ contenue dans $\mathbf{X}(S)$ et formée de l'ensemble ${}_k\Delta$ des k-racines simples de G et de caractères triviaux sur $S \cap \mathfrak{D}G$.

Pour tout $w \in {}_kW(G, S)$ et $\alpha \in {}_k\Delta$, on pose :

$$w(\alpha) = \sum_{\beta \in {}_k\Delta} n_{\alpha\beta}(w).\beta. \tag{1}$$

Les coefficients $n_{\alpha\beta}(w)$ sont donc des entiers, tous de même signe.

Le théorème suivant est dû à Harish-Chandra (non publié) lorsque $k = \mathbf{R}$. La démonstration dans le cas plus général considéré ici est essentiellement la même.

15.2. THÉORÈME. *Supposons* $k \subset \mathbf{R}$ *et* G *connexe. Soit* $\mathfrak{S}$ *un domaine de Siegel de* $G_{\mathbf{R}}$ *par rapport à* K, P, S. *Soit* $C = C^{-1}$ *une partie symétrique de* G_k *telle que* $|z_c^\chi| > 1$ *sur* C *pour tout poids dominant* χ. *Alors* $C_{\mathfrak{S}} = \{c \in C,\ \mathfrak{S}.c \cap \mathfrak{S} \neq \emptyset\}$ *est relativement compact dans* $G_{\mathbf{R}}$.

Remarquons tout d'abord que la condition imposée à C peut aussi s'exprimer par $\Phi(z_c) > 1$ sur C pour tout poids dominant χ et toute fonction > 0 de type (P, χ).

(i) *A montrer : u_c, s_c et s_{z_c} sont bornés lorsque c parcourt* $C_{\mathfrak{S}}$.

Soit $c \in C_{\mathfrak{S}}$. On peut donc trouver $x \in \mathfrak{S}$ tel que $x.c \in \mathfrak{S}$. Vu 14.6, on a, pour tout poids dominant χ et toute fonction $\Phi > 0$ de type (P, χ) :

$$\Phi(x) = \Phi(x.c.c^{-1}) \succ \Phi(x.c).\Phi(c^{-1}) \succ \Phi(x).\Phi(c).\Phi(c^{-1}) \quad (c \in C_{\mathfrak{S}};\ x \in \mathfrak{S}c^{-1} \cap \mathfrak{S}).$$

Cela entraîne :

(1) $$\Phi(c).\Phi(c^{-1}) \prec 1, \qquad (c \in C_{\mathfrak{S}}).$$

Comme $C = C^{-1}$ et que $\Phi(c) \succ \Phi(z_c)$ (cf. 14.10), l'hypothèse et (1) impliquent que $\Phi \asymp 1$ sur $C_{\mathfrak{S}}$, d'où aussi $\Phi(s_c) \asymp 1 \asymp \Phi(z_c)$ sur $C_{\mathfrak{S}}$; cela montre que s_c et z_{s_c} sont bornés.

Mais on a (dém. de 14.10) :

$$\Phi(c) \asymp \Phi(w_c^{-1}.u_c.w_c).\Phi(z_c),$$

donc $\Phi(w_c^{-1}.u_c.w_c) \asymp 1$. La Prop. 14.8 implique alors que $w_c^{-1}.u_c.w_c$ est borné. Il en est donc de même de u_c.

(ii) Pour démontrer le théorème, on procède par induction sur le k-rang de G. S'il est nul, alors $\mathfrak{S}$ est compact, et le théorème est évident. Nous supposons donc $\mathrm{rg}_k(G) > 0$ et le théorème vrai pour G' si $\mathrm{rg}_k(G') < \mathrm{rg}_k(G)$. Nous considérons tout d'abord le cas où $\mathbf{X}(G)_k = \{1\}$. Pour tout $w \in {}_k\mathrm{W}$, posons :

$$C_{\mathfrak{S},w} = C_{\mathfrak{S}} \cap (P_k.w.P_k),$$

où, de nouveau, nous notons aussi w un représentant de w dans $N(S)_k$ choisi une fois pour toutes. Nous avons à prouver que $C_{\mathfrak{S},w}$ est borné et distinguons pour cela deux cas :

(a) *w ne fait partie d'aucun sous-groupe parabolique propre contenant* P. Soient :

(1) $$M = \mathfrak{S} \cap \mathfrak{S}.C_{\mathfrak{S},w}^{-1}, \qquad M' = \mathfrak{S} \cap \mathfrak{S}.C_{\mathfrak{S},w}.$$

On a $C_{\mathfrak{S},w} \subset M^{-1}.M'$. Il suffit donc de montrer que M et M' sont bornés.

Soient $x \in M$ et $y = x.c$. Cette égalité peut s'écrire, en utilisant les décompositions d'Iwasawa de x, y et la décomposition de Bruhat de c :

$$k_x.m_x.s_x.n_x.u_c.w.z_c.v_c = k_y.m_y.s_y.n_y.$$

Nous voulons aussi écrire le membre de gauche en décomposition d'Iwasawa de manière à pouvoir comparer les composantes des deux membres. On a :

$$y = k_x.m_x.{}^{s_x}(n_x.u_c).s_x.w.z_c.v_c = k_x.m_x.w.{}^{w^{-1}.s_x}(n_x.u_c).{}^{w^{-1}}s_x.z_c.v_c.$$

Posons :

$$d = w.{}^{w^{-1}.s_x}(n_x.u_c) = k_d.m_d.s_d.n_d.$$

Alors $k_d.m_d.s_d$ est la décomposition d'Iwasawa de w, donc k_d normalise M, d'où :

$$s_y = s_d.{}^{w^{-1}}s_x.s_{z_c}.$$

D'après 12.2, l'élément d est borné, donc s_d est borné. D'autre part, s_{z_c} est borné d'après (i). On a donc, pour tout $\alpha \in {}_k\Delta$:

(2) $$s_y^\alpha \asymp (w^{-1}.s_x.w)^\alpha = s_x^{w(\alpha)}.$$

On a, dans les notations de 15.1 :

$$s_x^{w(\alpha)} = \prod_\beta s_x^{n_{\alpha\beta}(w).\beta}.$$

Fixons $\beta \in {}_k\Delta$. Vu l'hypothèse faite sur w, et 11.11, il existe $\alpha \in {}_k\Delta$ tel que $n_{\alpha\beta}(w) < 0$. On a alors $n_{\gamma\beta}(w) \leqq 0$ pour tout $\gamma \in {}_k\Delta$, donc chaque facteur de droite est $\succ 1$. Mais $s_y^\beta \prec 1$ puisque $y \in \mathfrak{S}$; par conséquent, on doit avoir :

$$s_x^{n_{\gamma\beta}(w).\beta} \asymp 1 \qquad (\gamma \in {}_k\Delta).$$

Vu que $n_{\alpha\beta}(w) \neq 0$, cela donne en particulier $s_x^\beta \asymp 1$, et, étant valable pour tout $\beta \in {}_k\Delta$, montre que s_x est borné. Mais m_x et u_x le sont automatiquement, donc M est borné. Tenant compte de (2), on voit que s_y est borné, donc y est aussi borné.

(b) *L'élément w fait partie d'un sous-groupe parabolique propre* P' *contenant* P. On a alors $C_{\mathfrak{S}.w} \subset P'$ et il suffit donc de montrer que $C' = C_{\mathfrak{S}} \cap P'$ est borné. Soient $x, y \in \mathfrak{S}$ tels que $x.c = y$ $(c \in C')$. En multipliant les deux membres par k_x^{-1}, on voit que l'on peut supposer $x \in P \subset P'$, donc aussi $y \in P'$. Par suite :

$$C'^{-1} = C' = \{c \in C \cap P', \quad (\mathfrak{S} \cap P').c \cap (\mathfrak{S} \cap P') \neq \varnothing\}. \tag{3}$$

Il suffit de considérer le cas où P' est propre maximal. Vu 11.8, 11.9, il existe alors $\beta \in {}_k\Delta$ tel que $P' = P_\theta$ $(\theta = {}_k\Delta - \{\beta\})$, et l'on a les décompositions canoniques :

$$P' = Z(S_\theta).V_\theta, \qquad Z(S_\theta) = L_\theta.M_\theta.S_\theta, \tag{4}$$

où $\mathrm{rg}_k(L_\theta) = \mathrm{rg}_k(G) - 1$, $\mathrm{rg}_k(M_\theta) = 0$, et S_θ est de dimension un. Le groupe L_θ est semi-simple, et θ s'identifie à l'ensemble des k-racines simples de L_θ pour un ordre associé à $P \cap L_\theta$.

On peut supposer $w \in L_\theta$. Le radical unipotent U de P est produit semi-direct sur k de $L_\theta \cap U$ par V_θ. La première égalité de (4) représente aussi un produit semi-direct sur k. Dans l'égalité :

$$c = u_c.w.z_c.v_c = h_c.b_c, \qquad (h_c \in Z(S_\theta)_k, \quad b_c \in V_{\theta,k});$$

en utilisant la décomposition de Bruhat de h_c dans $Z(S_\theta)_k$, on voit que l'on peut supposer :

$$h_c = u_c.w.z_c.b_c', \quad v_c = b_c'.b_c \qquad (v_c, b_c' \in L_\theta \cap U_k\,;\ z_c \in Z(S)_k). \tag{5}$$

Quitte à agrandir $\mathfrak{S}$, on peut admettre que $\mathfrak{S}'$ est le produit de ses projections sur $Z(S_\theta)$ et V_θ, la deuxième étant compacte, donc :

$$h_c \in (\mathfrak{S}' \cap Z(S_\theta))^{-1}.(\mathfrak{S}' \cap Z(S_\theta)) \qquad (c \in C'). \tag{6}$$

Nous montrerons tout d'abord que h_c est borné. Soient π_1, π_2, π_3 les projections canoniques de $Z(S_\theta)$ sur ses quotients Q_1, Q_2, Q_3 par $M_\theta.S_\theta$, $L_\theta.M_\theta$ et $L_\theta.S_\theta$ respectivement. La restriction à $Z(S_\theta)_{\mathbf{R}}$ de l'application :

$$\pi = \pi_1 \times \pi_2 \times \pi_3 : Z(S_\theta) \to Q = Q_1 \times Q_2 \times Q_3$$

est de noyau fini, et son image est fermée, car elle contient la composante connexe de e dans Q, pour la topologie ordinaire. C'est donc une application propre, et il suffit de montrer que $\pi_i(h_c)$ est borné $(i = 1, 2, 3)$.

Soit $i = 2, 3$. D'après (5), on a $\pi_i(h_c) = \pi_i(z_c)$, d'où notre assertion dans ces cas, puisque z_c est borné, vu (i).

Soit $\mathfrak{T} = \pi_1(\mathfrak{S}' \cap Z(S_\theta))$. On vérifie immédiatement à partir des définitions que $\mathfrak{T}$ est un ensemble de Siegel de $Q_{1\mathbf{R}}$ (par rapport aux projections K_1', P_1, S_1, de $K \cap L_\theta$, $P \cap L_\theta$ et $S \cap L_\theta$). Vu (6), on a :

$$\pi_1(h_c) \in \mathfrak{T}^{-1}.\mathfrak{T}. \tag{7}$$

Comme π_1 est un k-morphisme, on a $\pi_1(h_c) \in Q_{1,k}$, et l'égalité $C' = C'^{-1}$ de (3) implique immédiatement que l'ensemble des h_c est aussi symétrique. π_1 est une k-isogénie de L_θ sur Q_1. L'homomorphisme $\pi_1^* : X(P_1) \to X(Z(S_\theta))$ induit par π_1

transforme un poids dominant en un poids dominant. Si l'on applique π_1 à la relation $h_c = u_c.w.z_c.b'_c$, on voit que l'on obtient la décomposition de Bruhat de $\pi_1(h_c)$ par rapport à P_1, S_1. En particulier, $\pi_1(z_c)$ est la composante relative à $Z(S_1)$ de $\pi_1(h_c)$. Il s'ensuit que l'ensemble des $\pi_1(h_c)$ vérifie toutes nos hypothèses. Comme $\mathrm{rg}_k(Q_1) = \mathrm{rg}_k(L_\theta) < \mathrm{rg}_k(G)$, on peut appliquer l'hypothèse d'induction, donc $\pi_1(h_c)$ est borné.

Il reste encore à faire voir que b_c est borné. Or l'égalité $x.c = y$ peut s'écrire :

$$k_x.m_x.s_x.n'_x.n''_x.h_c.b_c = k_y.m''_y.s_y.n'_y.n''_y \qquad (n'_x, n'_y \in U \cap L_\theta;\quad n''_x, n''_y \in V_\theta),$$

d'où :

$$n''_y = h_c^{-1}.n''_x.h_c.b_c.$$

On vient de montrer que h_c est borné. Quant à n''_x, n''_y, ils le sont aussi puisque $x, y \in \mathfrak{S}$, donc b_c est borné.

(iii) Cela termine la démonstration lorsque $X(G)_k = \{1\}$. Dans le cas général, G s'écrit comme produit presque direct $G = G_1.Z$ où Z est un tore décomposé sur k et $X(G_1)_k = \{1\}$. Soit $\pi : G \to G' = G/Z$ la projection canonique. π définit une k-isogénie de G_1 sur G', donc $X(G')_k = \{1\}$. D'autre part, $\pi(P)$ et $\pi(S)$ sont respectivement un k-sous-groupe parabolique minimal et un tore décomposé sur k maximal de G', et il résulte immédiatement des définitions que $\pi(\mathfrak{S}) = \mathfrak{S}'$ est un ensemble de Siegel de $G'_{\mathbf{R}}$. Ce qui a déjà été démontré montre alors que $\pi(C_{\mathfrak{S}})$ est relativement compact. Comme Z est un tore décomposé sur k, l'homomorphisme π applique $G_{k'}$ sur $G'_{k'}$, pour toute extension k' de k, d'où l'existence d'un compact $Q \subset G_{\mathbf{R}}$ tel que $C_{\mathfrak{S}} \subset Q.Z_{\mathbf{R}}$. Écrivons $c \in C_{\mathfrak{S}}$ sous la forme $c = q_c.r_c (q_c \in Q, r_c \in Z_{\mathbf{R}})$ où q_c et r_c sont déterminés au produit par un élément du compact $Q.Q \cap Z_{\mathbf{R}}$ près. On a, vu (14.10), $c^\chi \succ 1$, d'où $r_c^\chi \succ 1$, pour tout poids dominant χ. Mais l'ensemble des restrictions à Z des poids dominants de G contient un sous-groupe d'indice fini de X(Z), donc r_c est borné, ce qui termine la démonstration.

15.3. COROLLAIRE. *Supposons* $k = \mathbf{Q}$. *Soit* E *une partie symétrique de* $G_{\mathbf{Q}}$ *formée d'éléments à dénominateurs bornés. Alors* $E_{\mathfrak{S}} = E \cap \mathfrak{S}^{-1}.\mathfrak{S}$ *est fini.*

(Dans cet énoncé, on a identifié G à un $\mathbf{Q}$-sous-groupe de $\mathbf{GL}_n$. Remarquons que pour une partie *symétrique* M de $G_{\mathbf{Q}}$, la condition d'être « à dénominateurs bornés » est indépendante de la représentation matricielle choisie, car (7.1, 7.2) si $\varphi : G \to \mathbf{GL}_m$ est un $\mathbf{Q}$-morphisme, les coefficients de $\varphi(g)$ sont des polynômes à coefficients rationnels en les coefficients g_{ij} de g et en $(\det g)^{-1}$.)

Les éléments de E ayant des coefficients rationnels à dénominateurs bornés, on a $|\det x| \succ 1$ sur E, d'où aussi, puisque E est symétrique, $|\det x| \prec 1$ et :

$$|\det x| \asymp 1 \qquad (x \in E). \tag{1}$$

Étant donné $w \in {}_{\mathbf{Q}}W$, posons $G_w = U'_w.w.P$ et $E_w = E \cap G_w$. On a :

$$w^{-1}.G_w \subset U^-.P = U^-.Z(S).U.$$

Notons z'_y la composante en Z(S) d'un élément de $U^-.Z(S).U$. On a alors :

$$z'_{w^{-1}.x} = z_x \qquad (x \in G_w).$$

D'autre part, $w^{-1}.E_w$ est formé d'éléments de $G_{\mathbf{Q}}$ à dénominateurs bornés, dont le déterminant est, vu (1), comparable à un en valeur absolue. On est donc ramené à prouver que si $F \subset U_{\mathbf{Q}}^{-}.P_{\mathbf{Q}}$ est formé d'éléments à dénominateurs bornés, vérifiant

$$|\det x| \asymp 1 \qquad (x \in F) \tag{2}$$

alors :

$$|z_x'^{\chi}| > 1 \qquad (x \in F;\ \chi \text{ poids dominant}). \tag{3}$$

On peut se borner à un ensemble de poids dominants contenant une base de $\mathbf{X}(S) \otimes \mathbf{Q}$. Étant donné χ, soient, comme dans (14.4), $\pi : G \to GL(V)$ une représentation irréductible, définie sur $\mathbf{Q}$, et D_π une droite stable par P, sur laquelle P agit par l'intermédiaire de χ. Il existe une base (e_i) de $V_{\mathbf{Q}}$ formée des vecteurs propres de S, dont le premier sous-tend D_π. Si $x = u.z_x'.v$ $(u \in U^-, v \in U)$, alors :

$$\pi(x).e_1 = \pi(u).z_x'^{\chi}.e_1 = z_x'^{\chi}(e_1 + \sum_{i \geqq 2} c_i(u).e_i),$$

donc :

$$z_x'^{\chi} = \pi(x)_{11}. \tag{4}$$

Mais $\pi(x)_{11}$ est une fonction régulière sur G, définie sur $\mathbf{Q}$. C'est donc un polynôme à coefficients rationnels en les coefficients x_{ij} de x et en $(\det x)^{-1}$. En multipliant par une puissance convenable de $\det x$, et en tenant compte de (2), on voit qu'il suffit de prouver que si R est un polynôme à coefficients rationnels en les coefficients de x, qui ne s'annule pas sur F, alors $|R(x)| > 1$ sur F. Or, si m est un multiple des dénominateurs des coefficients de R et des éléments de F, on a évidemment $m|R(x)| \geqq 1$ $(x \in F)$, d'où notre assertion.

15.4. THÉORÈME. *Soient $k = \mathbf{Q}$ et $\mathfrak{S}$ un ensemble de Siegel de $G_{\mathbf{R}}$ (par rapport à K, P, S). Soient A une partie finie de $G_{\mathbf{Q}}$ et Γ un groupe arithmétique de G. Alors $\mathfrak{S}.A$ a la propriété de Siegel pour Γ.*

Il s'agit donc de montrer que, étant donné $q \in G_{\mathbf{Q}}$:

$$M = \{\gamma \in \Gamma \mid \mathfrak{S}.A.q \cap \mathfrak{S}.A.\gamma \neq \emptyset\}$$

est fini.

On peut supposer $\Gamma \subset G_{\mathbf{Z}}$; ses éléments sont de déterminant égal à ± 1, donc :

$$E = A.\Gamma.q^{-1}.A^{-1} \cup A.q.\Gamma.A^{-1}$$

est une partie symétrique de $G_{\mathbf{Q}}$, formée d'éléments à dénominateurs bornés, et l'on est ramené à 15.3 lorsque G est connexe.

Supposons maintenant G non connexe. Quitte à agrandir A, on peut se borner au cas où $\Gamma \subset G^0$. Les $\mathbf{Q}$-sous-groupes paraboliques minimaux de G^0 étant conjugués sur $\mathbf{Q}$, on a $G_{\mathbf{Q}} = N_G(P)_{\mathbf{Q}}.(G^0)_{\mathbf{Q}}$. On peut donc trouver des parties finies A', B' de $N_G(P)_{\mathbf{Q}}$ et A'', B'' de $(G^0)_{\mathbf{Q}}$ telles que $A \subset A'.A''$, $A.q \subset B'.B''$. D'autre part (12.7), il existe un ensemble de Siegel $\mathfrak{S}'$ contenant $\mathfrak{S}.(A' \cup B')$. Soit $C = A'' \cup B''$. Il suffit de montrer la finitude de :

$$M = \Gamma \cap (\mathfrak{S}'.C)^{-1}.\mathfrak{S}'.C.$$

Comme $G_{\mathbf{R}} = K.(G^0)_{\mathbf{R}}$, $K.\mathfrak{S}' = \mathfrak{S}'$, et $\Gamma \subset G^0$, on a aussi :

$$M = \Gamma \cap (\mathfrak{S}''.C)^{-1}.(\mathfrak{S}''.C), \qquad (\mathfrak{S}'' = \mathfrak{S}' \cap G^0),$$

et l'on est ainsi ramené au cas, déjà traité, du groupe connexe.
En combinant 12.5, 13.1 et 15.4, on obtient le théorème suivant, qui est le principal résultat de la théorie de la réduction pour les groupes arithmétiques.

15.5. THÉORÈME. *Soit $k = \mathbf{Q}$ et soit Γ un groupe arithmétique de G. Il existe un ensemble de Siegel $\mathfrak{S}$ sur $\mathbf{Q}$ de G et une partie finie C de $G_{\mathbf{Q}}$ tels que $\Omega = \mathfrak{S}.C$ soit un ensemble fondamental pour Γ dans $G_{\mathbf{R}}$. Cet ensemble est compact si $\mathrm{rg}_{\mathbf{Q}}(G) = 0$ et est de mesure de Haar finie si $X(G^0)_{\mathbf{Q}} = \{1\}$. Pour toute partie finie A de $G_{\mathbf{Q}}$, l'ensemble $\Gamma \cap (\Omega A)^{-1}.\Omega A$ est fini.*

Nous terminerons ce paragraphe en donnant une interprétation de C.

15.6. PROPOSITION. *Soit $k = \mathbf{Q}$. Soient Γ un groupe arithmétique de G, et P' un $\mathbf{Q}$-groupe parabolique. Alors $G_{\mathbf{Q}}$ est réunion d'un nombre fini de doubles classes $P'_{\mathbf{Q}}.c.\Gamma$.*
Soit C une partie finie de $G_{\mathbf{Q}}$. On a $P_{\mathbf{Q}}.C.\Gamma = G_{\mathbf{Q}}$ si, et seulement si, il existe un ensemble de Siegel $\mathfrak{S}$, par rapport à K, P, S, tel que $\mathfrak{S}.C.\Gamma = G_{\mathbf{R}}$.

Il suffit de prouver la première assertion pour $P' = P$. Tenant compte de 15.5, on voit alors qu'il suffit d'établir la deuxième.
Supposons tout d'abord que l'on ait $\mathfrak{S}.C.\Gamma = G_{\mathbf{R}}$. Soit $g \in G_{\mathbf{Q}}$. Alors $\mathfrak{S}.g$ ne rencontre qu'un nombre fini de translatés $\mathfrak{S}.c.\gamma$ ($c \in C$, $\gamma \in \Gamma$) d'après 15.4. Comme $\mathfrak{S}.C.\Gamma = G_{\mathbf{R}}$, il existe un nombre fini d'éléments $c_i \in C$, $\gamma_i \in \Gamma$ ($1 \leqq i \leqq m$) tels que :

$$\mathfrak{S}.g \subset \bigcup_i \mathfrak{S}.c_i.\gamma_i.$$

Puisque C est fini, il existe une suite d'éléments $x_j \in \mathfrak{S}$, et un indice i tels que :

$$(s_{x_j})^{\alpha} \to 0 \quad (j \to \infty), \qquad x_j.g \in \mathfrak{S}.c_i.\gamma_i \qquad (\alpha \in {}_{\mathbf{Q}}\Delta).$$

Il résulte alors de 12.5 que $c_i.\gamma_i.g^{-1} \in P_{\mathbf{Q}}$, d'où $g \in P_{\mathbf{Q}}.C.\Gamma$.
Réciproquement, supposons que $G_{\mathbf{Q}} = P_{\mathbf{Q}}.C.\Gamma$. D'après 15.5, il existe une partie finie C' de $G_{\mathbf{Q}}$ et un ensemble de Siegel $\mathfrak{S}$ tels que $\mathfrak{S}.C'.\Gamma = G_{\mathbf{R}}$. Il existe une partie finie F de $P_{\mathbf{Q}}$ telle que $C' \subset F.C.\Gamma$, d'où $G_{\mathbf{R}} = \mathfrak{S}.F.C.\Gamma$. Il suffit alors de remarquer (12.7) que $\mathfrak{S}.F$ est contenu dans un ensemble de Siegel relatif à K, P, S.

15.7. COROLLAIRE. *Soient H un $\mathbf{Q}$-groupe, et P' le normalisateur d'un $\mathbf{Q}$-sous-groupe parabolique minimal P de H^0. Soit Γ un sous-groupe arithmétique de H. Il existe une partie finie C de $H^0_{\mathbf{Q}}$ contenue dans l'intersection des noyaux des éléments de $X(H^0)_{\mathbf{Q}}$, telle que $H_{\mathbf{Q}} = \Gamma.C.P'_{\mathbf{Q}}$.*

Il résulte immédiatement de (11.8) que $H_{\mathbf{Q}} = H^0_{\mathbf{Q}}.P'_{\mathbf{Q}}$. On peut donc supposer H connexe. Soit U le radical unipotent de H. Alors $H = L.U$ est le produit semi-direct d'un $\mathbf{Q}$-groupe réductif L par U (7.15) et $X(H)_{\mathbf{Q}}$ s'identifie, par restriction, à $X(L)_{\mathbf{Q}}$. Soit M la composante neutre du noyau des éléments de $X(L)_{\mathbf{Q}}$ et soit S

le plus grand tore décomposé sur $\mathbf{Q}$ central de L. Alors $L = M.S$, et $M \cap S$ est fini (10.7). Évidemment $S.U \subset P$, et $P \cap M$ (resp. $P \cap L$) est un $\mathbf{Q}$-sous-groupe parabolique minimal de M (resp. L). Les espaces $M/(P \cap M)$, $L/(L \cap P)$ et H/P sont $\mathbf{Q}$-isomorphes. Tenant compte de (10.9) et (11.8), on voit que :

$$M_{\mathbf{Q}}/(P \cap M)_{\mathbf{Q}} = H_{\mathbf{Q}}/P_{\mathbf{Q}}.$$

Par conséquent, si C est une partie finie de $M_{\mathbf{Q}}$ telle que :

$$(M \cap \Gamma).C.(P \cap M)_{\mathbf{Q}} = M_{\mathbf{Q}},$$

on a aussi $\Gamma.C.P_{\mathbf{Q}} = H_{\mathbf{Q}}$.

Enfin, pour la commodité des références, mentionnons encore une simple conséquence de la propriété de Siegel.

15.8. PROPOSITION. *Soient* $k = \mathbf{Q}$ *et* $\mathfrak{S}$ *un ensemble de Siegel de* $G_{\mathbf{R}}$. *Soit* A *une partie finie de* $G_{\mathbf{Q}}$. *Alors, pour tout* $g \in G_{\mathbf{R}}$, *l'ensemble* $\mathfrak{S} \cap g.\Gamma.A$ *est fini.*

Soit $V = \{\gamma \in \Gamma \mid \mathfrak{S}.A^{-1}\gamma \cap \mathfrak{S}.A^{-1} \neq \emptyset\}$. L'ensemble V est fini vu (15.4), et il est immédiat que si $x = g.\sigma.b$ $(\sigma \in \Gamma,\ b \in A)$ fait partie de $\mathfrak{S} \cap g.\Gamma.A$, alors tout autre élément de cet ensemble est de la forme $g.\sigma.v.a$ $(v \in V,\ a \in A)$.

Appendice : Groupe de commensurabilité et propriété de Siegel.

La condition (F_2) fait intervenir, outre $G_{\mathbf{R}}$ et Γ, le groupe $G_{\mathbf{Q}}$, qui n'est pas directement associé à $G_{\mathbf{R}}$ et Γ. Nous voulons faire voir ici qu'en fait on peut remplacer $G_{\mathbf{Q}}$ par un groupe qui lui est intimement lié, mais peut être plus grand, et qui est défini à partir de $G_{\mathbf{R}}$ et Γ. Cela mène à une formulation plus forte de (F_2), qui peut être imposée à un groupe et un sous-groupe quelconques (15.13), et est aussi vérifiée par les groupes arithmétiques (15.15).

15.9. DÉFINITION. Soient H un groupe et L un sous-groupe. On appelle *groupe de commensurabilité de* L *dans* H, et on note C(L), l'ensemble des $h \in H$, tels que ${}^hL$ soit commensurable à L.

Comme la notion « être commensurables » est une relation d'équivalence entre sous-groupes de H, il est immédiat que C(L) est bien un groupe, qui ne dépend que de la classe de commensurabilité de L.

15.10. LEMME. *Soient* H, H' *des groupes,* $\pi : H \to H'$ *un homomorphisme surjectif de noyau* N *fini, et* L *un sous-groupe de* H. *Alors* $C(L) = \pi^{-1}(C(\pi(L)))$.

Il est clair que $C(L) \subset \pi^{-1}(C(\pi(L)))$. Soit réciproquement $x \in \pi^{-1}(C(\pi(L)))$. Comme N est fini, $\pi^{-1}(\pi(L)) = L.N$ et $\pi^{-1}(\pi({}^xL)) = {}^xL.N$ sont commensurables. Mais ces groupes sont respectivement commensurables à L et ${}^xL$, donc $x \in C(L)$.

15.11. LEMME. *Supposons* G *connexe, presque simple sur* $\mathbf{Q}$, *et soit* L *un sous-groupe de* $G_{\mathbf{Q}}$.

(i) *Si* L *est infini, et* C(L) *Zariski-dense, alors* L *est Zariski-dense.*

(ii) *Si* G *est simple sur* $\mathbf{Q}$, *et* L *est Zariski-dense, alors* $C(L) \subset G_{\mathbf{Q}}$.

(Un $\mathbf{Q}$-groupe connexe est *simple* (resp. *presque simple*) sur $\mathbf{Q}$ s'il ne contient pas de $\mathbf{Q}$-sous-groupe distingué propre $\neq \{e\}$ (resp. de dimension > 0).)

Étant donné un sous-groupe M de G, on note $\mathscr{A}(M)$ le plus petit sous-groupe algébrique de G contenant M. C'est aussi l'adhérence de M en topologie de Zariski. Si $M \subset G_{\mathbf{Q}}$, alors $\mathscr{A}(M)$ est défini sur $\mathbf{Q}$. Si M' est d'indice fini dans M, il est immédiat que $\mathscr{A}(M')$ est d'indice fini dans $\mathscr{A}(M)$, donc $\mathscr{A}(M')^0 = \mathscr{A}(M)^0$. Il s'ensuit que si M'' est commensurable à M, alors $\mathscr{A}(M)^0 = \mathscr{A}(M'')^0$.

(i) Comme L est infini, $\mathscr{A}(L)^0$ est de dimension > 0. Vu ce qui précède, c'est un groupe défini sur $\mathbf{Q}$, qui est normalisé par C(L). Mais, C(L) étant dense dans G, cela entraîne que $\mathscr{A}(L)^0$ est distingué dans G. On a donc $\mathscr{A}(L)^0 = G$, d'où (i).
(ii) On identifie G à un sous-groupe de $\mathbf{SL}_n$. Alors $\mathbf{C}[G]$ est l'algèbre engendrée par 1 et les coefficients g_{ij} des éléments de G. On fait opérer g sur $\mathbf{C}[G]$ par $f \mapsto {}^g f$, où :

$$ {}^g f(x) = f(g^{-1}.x.g) \qquad (g, x \in G). $$

On obtient une représentation rationnelle σ, définie sur $\mathbf{Q}$, de G dans l'espace vectoriel engendré dans $\mathbf{C}[G]$ par les g_{ij}. Comme G est simple sur $\mathbf{Q}$, et en particulier est de centre réduit à $\{e\}$, σ est un $\mathbf{Q}$-isomorphisme de G sur $\sigma(G)$. Par suite, $g \in G$ appartient à $G_{\mathbf{Q}}$ si, et seulement si, l'application $f \mapsto {}^g f$ envoie $\mathbf{Q}[G]$ dans $\mathbf{Q}[G]$. Soient $g \in C(L)$ et $f \in \mathbf{Q}[G]$. On peut écrire :

$$ {}^g f = f_0 + c_1 f_1 + \ldots + c_m f_m \qquad (f_i \in \mathbf{Q}[G];\ 0 \leqq i \leqq m) $$

avec $(1, c_1, \ldots, c_m)$ linéairement indépendants sur $\mathbf{Q}$. Soit $x \in L$ tel que $g^{-1}.x.g \in L$. Alors :

$$ f_0(x) + c_1 f_1(x) + \ldots + c_m f_m(x) = f(g^{-1}.x.g) \in \mathbf{Q}, $$

donc $f_i(x) = 0$, $(1 \leqq i \leqq m)$. Comme $L \cap g^{-1}.L.g$ est d'indice fini dans L, il est aussi Zariski-dense dans G, donc $f_i = 0$ $(1 \leqq i \leqq m)$, et ${}^g f = f_0 \in \mathbf{Q}[G]$.

Remarques. (i) vaut si $\mathbf{Q}$ est remplacé par un corps k quelconque. Le raisonnement précédent montre que $\mathscr{A}(L)^0$ est distingué dans G. Vu sa définition, il est k-fermé. Mais dans un k-groupe réductif connexe, tout sous-groupe distingué connexe est défini sur une extension séparable de k, donc $\mathscr{A}(L)^0$ est défini sur k, et l'on a de nouveau $\mathscr{A}(L)^0 = G$.
(ii) et sa démonstration restent aussi valables sur un corps quelconque si l'hypothèse « G simple sur k » est remplacée par « G est simple sur k et isomorphe à son groupe adjoint ».

15.12. PROPOSITION. *Supposons* G *connexe, semi-simple. Soient* N *le plus grand* $\mathbf{Q}$*-sous-groupe distingué de* G *dont l'ensemble des points réels est compact,* $\pi : G \to G' = G/N$ *la projection canonique, et* Γ *un sous-groupe arithmétique de* G.

(i) *Si* N *est fini,* Γ *est Zariski-dense dans* G.
(ii) *On a* $C(\Gamma) = \pi^{-1}(G'_{\mathbf{Q}})$.

(i) On suppose évidemment $G \neq \{e\}$. Alors $G \neq N$, et $G_{\mathbf{R}}$ n'est pas compact. Comme $G_{\mathbf{R}}/\Gamma$ est de volume invariant fini (13.2), Γ est *infini*. D'autre part, vu (7.13), $C(\Gamma) \supset G_{\mathbf{Q}}$. Or, d'après un théorème de Rosenlicht (cf. [1]), $G_{\mathbf{Q}}$ est dense dans G. On applique alors (15.11 (i)) à chaque $\mathbf{Q}$-facteur de G, et (8.10).
(ii) Vu (15.10), et le fait que $\pi(\Gamma)$ est arithmétique (8.11), il suffit de considérer le cas où $N = \{e\}$, et de montrer qu'alors $C(\Gamma) = G_{\mathbf{Q}}$. Le groupe G est produit

direct de groupes $\mathbf{Q}$-simples G_i. De plus, vu (8.10), Γ est commensurable au produit des groupes $\Gamma \cap G_i$, et $\Gamma \cap G_i$ est arithmétique dans G_i. On est donc ramené au cas où G est simple sur $\mathbf{Q}$, et où $G_{\mathbf{R}}$ est non compact. Alors Γ est Zariski-dense par (i), et $C(\Gamma) \subset G_{\mathbf{Q}}$ d'après (15.11 (ii)). Comme l'inclusion inverse résulte de (7.13), cela termine la démonstration.

15.13. Étant donné un groupe H, un sous-groupe L et une partie Ω de H, nous considérerons les conditions suivantes :

$(F_2)^-$: pour tout $c \in L$, l'ensemble des $x \in L$ tels que $\Omega c \cap \Omega x \neq \emptyset$ est fini;

$(F_2)^+$: étant donné $c \in C(L)$, l'ensemble des $x \in L$ tels que $\Omega c \cap \Omega x \neq \emptyset$ est fini.

Il est immédiat que si Ω vérifie $(F_2)^+$ pour L, il vérifie aussi cette condition pour *tout* sous-groupe L' commensurable à L. Si Ω est un « ensemble fondamental », i.e. vérifie en plus (F_1) : $\Omega.L = H$, alors il existe aussi un ensemble fondamental Ω' pour L'; il suffit de prendre $\Omega' = \Omega.D$, où D est un système de représentants pour $L/(L \cap L')$. Par contre il ne semble pas clair que si Ω vérifie (F_1) et $(F_2)^-$ pour L, on puisse trouver un Ω' vérifiant (F_1) et $(F_2)^-$ pour L'.
Si $H = G_{\mathbf{R}}$ et L est arithmétique, alors $C(L) \supset G_{\mathbf{Q}}$, vu (7.13), donc (F_2) est intermédiaire entre $(F_2)^-$ et $(F_2)^+$.

15.14. PROPOSITION. *Supposons* G *connexe, semi-simple et soit* Γ *un sous-groupe arithmétique de* G. *Alors tout ensemble de Siegel* (12.3) $\mathfrak{S}$ *de* $G_{\mathbf{R}}$ *vérifie la condition* $(F_2)^+$ *pour* Γ.

Soit N le plus grand $\mathbf{Q}$-sous-groupe distingué de G dont l'ensemble des points réels est compact et soit $\pi : G \to G' = G/N$ la projection canonique. On a déjà remarqué que $\pi(\mathfrak{S}) = \mathfrak{S}'$ est contenu dans un ensemble de Siegel de $G'_{\mathbf{R}}$ (12.3). D'autre part (8.11), $\Gamma' = \pi(\Gamma)$ est arithmétique dans G'. Soit $c \in C(\Gamma)$. D'après 15.12, on a $\pi(c) \in G'_{\mathbf{Q}}$. Comme $\mathfrak{S}'$ est contenu dans un ensemble de Siegel, l'ensemble des $x' \in \Gamma'$ tels que $\mathfrak{S}'.c' \cap \mathfrak{S}'.x' \neq o$ est fini. Par conséquent :

$$\{x \in \Gamma \mid \mathfrak{S}.c \cap \mathfrak{S}.x \neq \emptyset\}$$

est formé d'un nombre fini de classes modulo $N \cap \Gamma$. Mais $N_{\mathbf{R}}$ est compact, donc $N \cap \Gamma$ est fini.

15.15. THÉORÈME. *Supposons* G *connexe, semi-simple. Soit* Γ *un sous-groupe de* $G_{\mathbf{R}}$ *commensurable à un sous-groupe arithmétique de* G. *Il existe un ensemble de Siegel* $\mathfrak{S}$, *relatif à* $\mathbf{Q}$, *de* $G_{\mathbf{R}}$, *et une partie finie* C *du groupe de commensurabilité* $C(\Gamma)$ *de* Γ, *tels que* $G_{\mathbf{R}} = \mathfrak{S}.C.\Gamma$. *L'ensemble* $\mathfrak{S}.C$ *vérifie la condition* $(F_2)^+$ *de* (15.13).

Si Γ est arithmétique, cela résulte de (15.7) et (15.14). On passe de là à un sous-groupe de $G_{\mathbf{R}}$ commensurable à un groupe arithmétique en utilisant les remarques faites dans (15.13).
Nous nous sommes bornés au cas où G est connexe, semi-simple pour éviter quelques complications techniques, mais l'énoncé se généralise au cas d'un $\mathbf{Q}$-groupe réductif. Nous laissons au lecteur le soin de s'en convaincre à titre d'exercice.

§ 16. Ensembles fondamentaux et minima.

Dans ce paragraphe, G *est un* **Q***-groupe réductif connexe,* P *un* **Q***-sous-groupe parabolique propre, supposé minimal à partir de* 16.5, S *un tore décomposé sur* **Q** *maximal de* P,

$$P = M.S.U$$

la décomposition canonique de P *suivant* S, *et* K *un sous-groupe compact maximal de* $G_{\mathbf{R}}$ *dont l'algèbre de Lie est orthogonale à celle de* $S_{\mathbf{R}}$. *Enfin,* Γ *est un sous-groupe arithmétique de* G *et* C *une partie finie de* $G_{\mathbf{Q}}$ *telle que* $G_{\mathbf{Q}} = \Gamma.C.P_{\mathbf{Q}}$ (cf. 15.6).

16.1. Le but de ce paragraphe est de lier les ensembles fondamentaux du deuxième type à des conditions de minimum portant sur des fonctions de type (P, χ). La méthode utilisée est l'analogue « à l'infini », i.e. pour $G_{\mathbf{R}}$, de celle utilisée par Godement-Weil dans le cas des groupes adéliques [12]. Elle est cependant techniquement plus compliquée car, contrairement à ce qui se passe pour les groupes adéliques, il est nécessaire de considérer des ensembles à plus d'une « pointe », ce qui revient à dire que l'on ne peut supposer en général C réduit à $\{e\}$.
Des paragraphes précédents, on utilisera essentiellement :

(a) Le critère de Mahler (1.9, 8.2);
(b) Le critère de compacité (§ 8);
(c) La finitude de $P_{\mathbf{Q}}\backslash G_{\mathbf{Q}}/\Gamma$ (15.6).

Dans la présentation suivie ici, ce dernier point est lui-même obtenu comme conséquence de l'existence d'ensembles fondamentaux de la forme $\mathfrak{S}.C$, donc ce paragraphe n'en fournit pas une démonstration indépendante. Cependant, on peut démontrer *(c)* directement à partir du critère de compacité pour les groupes adéliques [12]. A part cela, ce paragraphe n'utilise pas de résultat démontré dans les §§ 9 et 13.

16.2. LEMME. *Soit* A *une partie finie de* $G_{\mathbf{Q}}$. *Soient* $\chi \in X(P)_{\mathbf{Q}}$ *dominant* (14.4), $\Phi > 0$ *de type* (P, χ) *et* Φ' *une fonction continue strictement positive comparable à* Φ. *Alors :*

$$\inf_{u \in \Gamma.A} \Phi'(u) > 0.$$

Si $\Phi = \Phi_\pi$ *est standard* (14.4), *alors* Φ *a un minimum* > 0 *sur* $\Gamma.A$.

Vu la dernière remarque de 14.2, il suffit de prouver la deuxième assertion. Soit donc $\Phi(g) = \| (\pi(g).e_0) \|$, où $\pi : G \to GL(V)$ est un **Q**-morphisme et $e_0 \in V$ un élément sous-tendant une droite stable par P. Il existe alors un réseau L de $V_{\mathbf{Q}}$ stable par Γ. Comme A est fini, il existe $q \in \mathbf{Q}^*$ tel que $\pi(A).L \subset q.L$. Par suite, $\pi(\Gamma.A).e_0$ est contenu dans l'ensemble $q.L - \{0\}$, qui est discret dans $V_{\mathbf{R}}$, d'où notre assertion.

16.3. Rappelons que si deux **Q**-sous-groupes paraboliques R, R' de G sont conjugués, on a un isomorphisme canonique entre $X(R)_{\mathbf{Q}}$ et $X(R')_{\mathbf{Q}}$ (11.9). Nous identifierons ces deux groupes par cet isomorphisme.

Soient $c \in G$ et f une fonction sur G. On notera $r_c f$ la transformée de f par translation à droite : $r_c f(x) = f(x.c)$ $(x \in G)$. Si $g \in G_R$ et f est de type (R, χ), alors $r_c f$ est évidemment de type $({}^cR, \chi)$.

16.4. LEMME. *On suppose* $X(G)_Q = \{1\}$ *et* $\mathrm{rg}_Q G = 1$. *Soit* Φ *une fonction continue* > 0 *comparable à une fonction de type* (P, χ) *strictement positive, où* χ *est dominant, non nul. Soit* $\Psi(g) = \inf_{u \in \Gamma . C} \Phi(g.u)$, $(g \in G_R)$. *Alors* Ψ *est une fonction bornée supérieurement sur* G_R.

Il suffit de faire la démonstration pour Φ de type (P, χ). Pour tout $d > 0$ soit :

$$E_d = \{x \in G_R \mid \Psi(x) \geqq d\}. \tag{1}$$

Évidemment, E_d est fermé, fonction décroissante de d, et le lemme équivaut à l'existence d'une constante $d_0 > 0$ telle que $E_d = \varnothing$ si $d > d_0$.
Par définition, Ψ est invariante à droite par Γ, donc :

$$E_d . \Gamma = E_d \qquad (d > 0). \tag{2}$$

D'autre part, 16.2 montre que $\bigcap_{d>0} E_d = \varnothing$. Il suffit donc de prouver que E_d/Γ est compact dans G_R/Γ. On peut se borner à le faire pour Φ standard. Soit μ la projection de G sur son groupe adjoint Ad G. Alors $\mu(\Gamma)$ est arithmétique (8.11) et l'application canonique $G_R/\Gamma \to \mathrm{Aut}\, \mathfrak{g}_R/\mu(\Gamma)$ est propre (8.5). Il suffit donc de considérer le cas où G est de centre réduit à $\{e\}$. On peut ainsi supposer G semi-simple, isomorphe à son groupe adjoint. Comme E_d est fermé, stable par Γ, son image E_d/Γ dans G_R/Γ est fermée. D'autre part $X(G) = \{1\}$, puisque G est semi-simple connexe. Tenant compte du critère de Mahler, sous la forme de 8.2 (iv), appliqué à la représentation adjointe, on voit que la compacité de E_d/Γ résultera de l'assertion suivante :

(*) *Soient* L *un réseau de* $\mathfrak{g}_Q$ *et* $d > 0$. *Soient* $z_j \in L$, $g_j \in E_d$ $(j = 1, 2, \ldots)$ *tels que* $\lim_{j \to \infty} \mathrm{Ad}\, g_j(z_j) = 0$. *Alors il existe* j_0 *tel que* $z_j = 0$ *pour* $j \geqq j_0$.

Démonstration de (*). Nous pouvons supposer L stable par Γ (7.13). Montrons tout d'abord que z_j est nilpotent pour j assez grand. Il existe des polynômes P_i sur $\mathfrak{g}$, invariants par Ad G, tels que :

$$\det(\mathrm{Ad}\, x - t.\mathrm{I}) = (-t)^n + \sum_{i=1}^{i=n} P_i(x).t^{n-i}.$$

Les P_i ont des coefficients rationnels, si l'on prend des coordonnées par rapport à une base de L. Il existe donc une constante $a > 0$ telle que :

$$(P_i(z) \leqq a \qquad (z \in L)) \Rightarrow P_i(z) = 0 \qquad (1 \leqq i \leqq n).$$

On a $P_i(z_j) = P_i(\mathrm{Ad}\, g_j(z_j)) \to 0$, donc, pour j assez grand, $P_i(z_j) = 0$ $(1 \leqq i \leqq n)$, et z_j est nilpotent.
Il résulte de 11.10 que tout élément nilpotent de $\mathfrak{g}_Q$ est conjugué par G_Q à un élément de $\mathfrak{u}_Q$. Comme $G_Q = \Gamma . C . P_Q$, on peut trouver $\gamma_j \in \Gamma$, $c_j \in C$ et $y_j \in \mathfrak{u}_Q$ tels que $z_j = \mathrm{Ad}\,(\gamma_j . c_j).y$, $(j \geqq j_0)$. Soit :

$$M = \mathfrak{u}_Q \cap \Big(\bigcap_{c \in C} \mathrm{Ad}\, c^{-1}(L) \Big).$$

C'est un réseau de $\mathfrak{u}_{\mathbf{Q}}$, qui contient y_j quel que soit $j \geqq j_0$. Passant à une suite partielle, et remplaçant g_j par $g_j.\gamma_j$ (ce qui est licite vu (2)), et L par la réunion de L et des réseaux $\mathrm{Ad}\, c^{-1}(\mathrm{L})$, $(c \in \mathrm{C})$, on voit que l'on est ramené à prouver :

(**) *Soient* $g_j \in \mathrm{E}_d$, $z_j \in \mathfrak{u} \cap \mathrm{L}$, $(j = 1, 2, \ldots)$, *et* $c \in \mathrm{C}$ *tels que* $\mathrm{Ad}\, g_j.c(z_j) \to 0$. *Alors* $z_j = 0$ *pour* j *assez grand.*

Démonstration de (**). Le groupe $\Gamma' = {}^c\Gamma$ est arithmétique. Il existe donc (8.4) des compacts $\eta \subset \mathrm{M}_{\mathbf{R}}$ et $\omega \subset \mathrm{U}_{\mathbf{R}}$ tels que :

$$\mathrm{G}_{\mathbf{R}} = \mathrm{K}.\mathrm{P}_{\mathbf{R}} = \mathrm{K}.\eta.{}_{\mathbf{Q}}\mathrm{A}.\omega.(\Gamma' \cap \mathrm{P}).$$

On peut par conséquent trouver $\sigma_j \in \Gamma' \cap \mathrm{P}$ tels que :

$$g_j.c.\sigma_j^{-1} \in \mathrm{K}.\eta.{}_{\mathbf{Q}}\mathrm{A}.\omega.$$

Quitte à remplacer g_j par $g_j.c.\sigma_j^{-1}.c^{-1} \in g_j.\Gamma$, on voit qu'il suffit d'établir (**) en supposant $g_j.c \in \mathrm{K}.\eta.{}_{\mathbf{Q}}\mathrm{A}.\omega$. Posons :

$$g_j.c = k_j.m_j.a_j.u_j \qquad (k_j \in \mathrm{K};\ m_j \in \eta;\ a_j \in {}_{\mathbf{Q}}\mathrm{A};\ u_j \in \omega).$$

Comme $k_j.m_j$ varie dans un compact, l'hypothèse de (**) équivaut à :

$$\lim_{j \to \infty} \mathrm{Ad}\, a_j.u_j(z_j) = 0. \tag{3}$$

Par ailleurs, la condition $g_j \in \mathrm{E}_d$ entraîne $a_j^{\chi} > 1$. Soit α l'unique $\mathbf{Q}$-racine simple de G. De $(\chi, \alpha) > 0$, on tire que $\chi = m.\alpha$ $(m > 0)$, donc :

$$a_j^{\alpha} > 1 \qquad (j = 1, 2, \ldots). \tag{4}$$

L'ensemble des $\mathbf{Q}$-racines positives se réduit à $\{\alpha\}$ ou à $\{\alpha, 2\alpha\}$. On a :

$$\mathfrak{u} = \mathfrak{g}_{\alpha} + \mathfrak{g}_{2\alpha}, \qquad [\mathfrak{g}_{\alpha}, \mathfrak{g}_{\alpha}] \subset \mathfrak{g}_{2\alpha}, \qquad [\mathfrak{u}, \mathfrak{g}_{2\alpha}] = \{0\},$$

($\mathfrak{g}_{2\alpha}$ étant nul si 2α n'est pas une $\mathbf{Q}$-racine). Ces deux sous-espaces sont définis sur $\mathbf{Q}$. Il existe donc des réseaux $\mathrm{L}' \subset \mathfrak{g}_{\alpha,\mathbf{Q}}$ et $\mathrm{L}'' \subset \mathfrak{g}_{2\alpha,\mathbf{Q}}$ tel que $\mathrm{L} \cap \mathfrak{u}$ soit d'indice fini dans $\mathrm{L}' + \mathrm{L}''$ et que l'on ait :

$$z_j = z_j' + z_j'' \qquad (z_j' \in \mathrm{L}';\ z_j'' \in \mathrm{L}'';\ j = 1, 2, \ldots).$$

Comme U opère trivialement, par la représentation adjointe, sur $\mathfrak{u}/\mathfrak{g}_{2\alpha}$, on a :

$$\mathrm{Ad}\, u_j(z_j') \equiv z_j' \pmod{\mathfrak{g}_{2\alpha}}, \qquad (j = 1, 2, \ldots),$$

donc :

$$\mathrm{Ad}\, a_j.u_j(z_j') \equiv a_j^{\alpha}.z_j' \pmod{\mathfrak{g}_{2\alpha}}, \qquad (j = 1, 2, \ldots).$$

Vu (4), on a $z_j' \to 0$. Mais z_j' fait partie du réseau L', donc est nul pour j assez grand. On a alors :

$$\mathrm{Ad}\, a_j.u_j(z_j) = a_j^2.z_j'' \qquad (j \geqq j_0)$$

d'où également $z_j'' = 0$ si j est assez grand.

16.5. NOTATION. Soient $\theta \subset {}_{\mathbf{Q}}\Delta$ et $t > 0$. On pose :

$$\mathrm{P}(\theta, t) = \{p \in \mathrm{P}_{\mathbf{R}},\ |p^{\alpha}| \leqq t\ (\alpha \in \theta)\}. \tag{1}$$

On écrira aussi $\mathrm{P}(t)$ pour $\mathrm{P}({}_{\mathbf{Q}}\Delta, t)$.

Il est clair que :

$$P(\theta \cup \theta', t) = P(\theta, t) \cap P(\theta', t) \qquad (\theta, \theta' \subset {}_{\mathbf{Q}}\Delta). \tag{2}$$

16.6. LEMME. *Soient* $\theta \subset {}_{\mathbf{Q}}\Delta$ *et* $\chi \in X(P)_{\mathbf{Q}}$ *dominant tel que* $(\chi, \alpha) > 0$ *pour* $\alpha \in \theta$. *Soient* Φ *une fonction continue* > 0 *comparable à une fonction* > 0 *de type* (P, χ) *et* μ *un nombre réel* > 1. *Pour* $b \in C$, *posons :*

$$\Omega_{b,\mu}(\Phi) = \Omega_{b,\mu} = \{g \in G_{\mathbf{R}}, \Phi(g.b) \leqq \mu.\Phi(g.u),\ (u \in \Gamma.C)\}.$$

Alors il existe $t > 0$ *tel que* $\Omega_{b,\mu}.b \subset K.P(\theta, t)$ *et que* $G_{\mathbf{R}} = K.P(\theta, t).C^{-1}.\Gamma$.

Soit $\Phi' > 0$ de type (P, χ) comparable à Φ. Il existe donc des constantes $d, d' > 0$ telles que :

$$d.\Phi'(g) \leqq \Phi(g) \leqq d'.\Phi'(g) \qquad (g \in G_{\mathbf{R}}).$$

On en déduit immédiatement que :

$$\Omega_{b,\mu}(\Phi) \subset \Omega_{b,\mu'}(\Phi') \qquad (\mu' = \mu.d'.d^{-1}).$$

Il suffit donc de démontrer le lemme pour Φ standard. Tout caractère de P est évidemment $\asymp 1$ sur $K \cap P$. Vu (16.5 (2)), on peut donc se borner à démontrer la première assertion dans le cas où θ est formé d'un élément, soit α.

Nous avons la décomposition $P_\alpha = M_\alpha.S_\alpha.V_\alpha$ (11.8). Soit L_α le $\mathbf{Q}$-groupe connexe dont l'algèbre de Lie est sous-tendue par $\mathfrak{g}_\beta + [\mathfrak{g}_\beta, \mathfrak{g}_{-\beta}]$ $(\beta = \alpha, 2\alpha)$. Alors L_α est facteur presque direct de M_α, et l'on a :

$$M_\alpha = L_\alpha.Q_\alpha, \tag{1}$$

avec Q_α anisotrope sur $\mathbf{Q}$, et L_α de rang rationnel égal à un (11.7). De plus, $T_\alpha = (S \cap L_\alpha)^0$ est un tore décomposé sur $\mathbf{Q}$ maximal de L_α, dont l'algèbre de Lie est engendrée par un élément h_α vérifiant :

$$\nu(h_\alpha) = 2(\nu, \alpha).(\alpha.\alpha)^{-1}, \qquad (\nu \in \mathfrak{s}^*).$$

Le caractère χ s'écrit sous la forme $\chi = \sum d_\beta \Lambda_\beta$ $(d_\beta \geqq 0)$. Vu l'hypothèse, $d_\alpha > 0$. Comme la restriction de χ à T_α est égale à $d_\alpha.\Lambda_\alpha$, il s'ensuit que :

$$\chi\,|_{T_\alpha} = m\alpha\,|_{T_\alpha}, \qquad (m > 0). \tag{2}$$

Soit D une partie finie de $L_{\alpha,\mathbf{Q}}$ telle que :

$$L_{\alpha,\mathbf{Q}} = (L_\alpha \cap \Gamma).D.(P \cap L_\alpha)_{\mathbf{Q}}, \tag{3}$$

(dont l'existence est assurée par 15.4). Désignons par ζ la restriction de $r_b\,\Phi$ à ${}^bL_\alpha$. C'est, vu (2), une fonction > 0 de type $({}^b(P \cap L_\alpha), m.\alpha)$. On peut écrire :

$$g = k_g.q_g.l_g.s_g.v_g \quad (k_g \in K,\ q_g \in {}^bQ_\alpha,\ l_g \in {}^bL_\alpha,\ s_g \in {}^bS_\alpha,\ v_g \in {}^bV_\alpha). \tag{4}$$

Nous prouverons plus bas :

(*) *Il existe une constante* $\mu' > 0$ *telle que l'on ait* $\zeta(l_g) \leqslant \mu'.\zeta(l_g.z)$ $(z \in {}^b(\Gamma \cap L_\alpha).{}^bD)$, *quel que soit* $g \in \Omega_{b,\mu}$.

Admettons-le provisoirement. D'après 16.4, appliqué à ${}^bL_\alpha$, il existe alors $\delta > 0$ tel que :

$$\zeta(l_g) \leqq \delta < \infty \qquad (g \in \Omega_{b,\mu}). \tag{5}$$

Vu (2) et (5), on a alors :

$$a(l_g)^{m\alpha} \leqq \delta \qquad (g \in \Omega_{b,\mu}). \tag{6}$$

La composante a_g de g dans ${}^{b}_{\mathbf{Q}}\mathrm{A}$, par rapport à la décomposition :

$$\mathrm{G}_{\mathbf{R}} = \mathrm{K}.{}^{b}\mathrm{M}_{\mathbf{R}}.{}^{b}_{\mathbf{Q}}\mathrm{A}.{}^{b}\mathrm{U}_{\mathbf{R}}$$

est égale au produit de la composante $a(l_g)$ de l_g dans ${}^{b}\mathrm{T}_{\alpha}$ par l'élément s_g de (4), d'où, puisque α est trivial sur S_{α}, l'existence d'une constante $t' > 0$ telle que :

$$a_g^{\alpha} \leqq t', \qquad (g \in \Omega_{b,\mu}). \tag{7}$$

Cela signifie, par définition, que :

$$g \in \mathrm{K}.{}^{b}\mathrm{P}(\alpha, t').$$

Écrivons $b = k.p$ $(k \in \mathrm{K},\ p \in \mathrm{P}_{\mathbf{R}})$. Il existe $t > 0$ tel que $p.\mathrm{P}(\alpha, t') \subset \mathrm{P}(\alpha, t)$, d'où $g.b \subset \mathrm{K}.\mathrm{P}(\alpha, t)$, et la première assertion du lemme.
Nous démontrons maintenant (*). On a :

$$r_b\Phi(g) = r_b\Phi(k_g.l_g.s_g) = r_b.\Phi(l_g).r_b\Phi(s_g)$$

$$r_b\Phi(g) = \eta(g).\zeta(l_g) \qquad (g \in \Omega_{b,\mu};\ \eta(g) = r_b\Phi(s_g)). \tag{8}$$

Soit $z \in {}^{b}((\Gamma \cap \mathrm{L}_{\alpha}).\mathrm{D})$. Alors z normalise ${}^{b}\mathrm{V}_{\alpha}$, centralise ${}^{b}\mathbf{Q}_{\alpha}$ et ${}^{b}\mathrm{S}_{\alpha}$, donc :

$$g.z = k_g.l_g.z.s_g.q_g.v'_g \qquad (v'_g = z^{-1}.v_g.z \in {}^{b}\mathrm{V}_{\alpha}).$$

Par suite :

$$r_b\Phi(g.z) = r_b\Phi(l_g.z).\eta(g) = \zeta(l_g.z).\eta(g), \qquad (g \in \Omega_{b,\mu}). \tag{9}$$

Écrivons z sous la forme $z = \sigma.d$ $(\sigma \in {}^{b}(\mathrm{L}_{\alpha} \cap \Gamma),\ d \in {}^{b}\mathrm{D})$. Il existe :

$$\gamma(d, b) \in \Gamma, \qquad c(d, b) \in \mathrm{C}, \qquad p(d, b) \in \mathrm{P}_{\mathbf{Q}},$$

tels que :

$$d.b = \gamma(d, b).c(d, b).p(d, b),$$

d'ou :

$$r_b\Phi(g.z) = \Phi(g.\sigma.d.b) = \Phi(g.\sigma.\gamma(d, b).c(d, b).p(d, b)) = \\ = |\,p(d, b)^{\chi}\,|.\Phi(g.\sigma.\gamma(d, b).c(d, b)).$$

L'élément b est fixé, et d parcourt un ensemble fini, donc $p(d, b)$ a un nombre fini de valeurs. Il existe par conséquent $\delta > 0$ tel que :

$$\inf_{\sigma, d} r_b\Phi(g.\sigma.d) \geqq \delta \inf_{\gamma \in \Gamma;\ c \in \mathrm{C}} \Phi(g.\gamma.c), \qquad (\sigma \in {}^{b}(\mathrm{L}_{\alpha} \cap \Gamma),\quad d \in {}^{b}\mathrm{D}). \tag{10}$$

Mais, par hypothèse :

$$\mu . \inf_{\gamma, c} \Phi(g.\gamma.c) \geqq \Phi(g.b). \tag{11}$$

En utilisant alors (8), (9), (10), (11), on voit qu'il existe une constante $\mu' > 0$ telle que :

$$\zeta(l_g).\eta(g) = \Phi(g.b) \leqq \mu' . \inf_{\sigma, d} r_b\Phi(g.\sigma.d) \leqq \mu'\,\eta(g) . \inf_{\sigma, d} \zeta(l_g.\sigma.d), \tag{12}$$

quel que soit $g \in \Omega_{b,\mu}$. En divisant les deux membres extrêmes de (13) par $\eta(g)$, on obtient (*), ce qui termine la démonstration de la première assertion.

La constante μ étant > 1, on peut, étant donné $g \in G_{\mathbf{R}}$, trouver $\sigma \in \Gamma$, $b \in C$ tels que :

$$\Phi(g.\sigma.b) \leqq \mu.\Phi(g.u) \qquad (u \in \Gamma.C).$$

On a alors $g.\sigma \in \Omega_{\mu,b}$ donc $g.\sigma.b \in K.P(\theta, t)$ pour t convenable, ne dépendant que de b. Comme C est fini, il existe t tel que cela soit valable pour tout $b \in C$, ce qui prouve la deuxième assertion du lemme.

16.7. THÉORÈME. *Soit* $\chi \in X(P)_{\mathbf{Q}}$ *un caractère dominant tel que* $(\chi, \alpha) > 0$ *pour tout* $\alpha \in {}_{\mathbf{Q}}\Delta$, *et soit* Φ *une fonction* > 0 *de type* (P, χ). *Alors il existe un ensemble de Siegel* $\mathfrak{S}$, *par rapport à* P, S, *tel que pour tout* $g \in G_{\mathbf{R}}$, *la fonction* $\Phi_g : u \mapsto \Phi(g.u)$ $(u \in \Gamma.C)$ *atteigne son minimum en un point de* $\mathfrak{S} \cap g.\Gamma.C$. *En particulier,* $G_{\mathbf{R}} = \mathfrak{S}.C^{-1}.\Gamma$.

Soit μ une constante > 1. Étant donné $g \in G_{\mathbf{R}}$, on peut trouver $\sigma \in \Gamma$, $b \in C$ tels que :

$$\Phi(g.\sigma.b) \leqq \mu\Phi(g.\gamma.c) \qquad (\gamma \in \Gamma, \quad c \in C).$$

D'après 16.6, il existe $t > 0$, indépendant de $b \in C$, tel que :

$$g.\sigma.b \in K.P(t).$$

Soit :

$$\Gamma' = \Gamma \cap \Big(\bigcap_{c \in C} . c^{-1}.\Gamma.c \Big).$$

C'est un groupe arithmétique (7.13), qui vérifie :

$$c.\Gamma' \subset \Gamma.c, \qquad (c \in C). \tag{1}$$

Vu le critère de compacité (8.4), il existe un compact $\omega \subset (M.U)_{\mathbf{R}}$ tel que :

$$(M.U)_{\mathbf{R}} = \omega(\Gamma' \cap M.U). \tag{2}$$

Nous voulons montrer que l'ensemble de Siegel $\mathfrak{S} = K._{\mathbf{Q}}A_t.\omega$ vérifie 16.7. D'après (2), il existe $\tau \in \Gamma' \cap P$ tel que $g.\sigma.b.\tau \in \mathfrak{S}$. Mais vu (1), on peut écrire :

$$g.\sigma.b.\tau = g.\gamma_1.b \qquad (\gamma_1 \in \Gamma) \tag{3}$$

ce qui montre que :

$$g \in \mathfrak{S}.C^{-1}.\Gamma.$$

Comme Φ est invariante à droite par $\Gamma \cap P$, on a $\Phi(g.\gamma_1.b) = \Phi(g.\sigma.b)$, donc :

$$\Phi(g.\gamma_1.b) \leqq \mu.\Phi(g.u) \qquad (u \in \Gamma.C).$$

Cela montre que, étant donné $\mu > 1$, on peut, quel que soit $g \in G_{\mathbf{R}}$, trouver $x \in g.\Gamma.C \cap \mathfrak{S}$ tel que $\Phi(x) \leqq \mu.\Phi(y)$ pour tout $y \in g.\Gamma.C$. Comme μ est un nombre arbitraire > 1, la première assertion résulte alors du fait que $g.\Gamma.C \cap \mathfrak{S}$ est un ensemble *fini* (15.8).

16.8. Dans l'énoncé suivant, on ne suppose plus $(\chi, \alpha) > 0$ pour tout $\alpha \in {}_{\mathbf{Q}}\Delta$. De plus, il se trouve que dans au moins une application, il y a lieu d'affaiblir légèrement les hypothèses faites sur Φ. Remarquons que si $\Phi > 0$ est de type (P, χ), $(\chi \in X(P))$, et si $\Phi' > 0$ est comparable à Φ, alors :

$$\Phi'(x.p) \asymp \Phi'(x).\Phi'(p) \asymp \Phi'(x)\,|p^{\chi}| \qquad (x \in G_{\mathbf{R}},\ p \in P_{\mathbf{R}}).$$

En effet :

$$\Phi'(x.p) \asymp \Phi(x.p) = \Phi(x).\Phi(p) = \Phi(x).|p^{\chi}| \asymp \Phi'(x).|p^{\chi}|.$$

16.9. THÉORÈME. *Soient* $\chi \in \mathbf{X}(\mathrm{P})_{\mathbf{Q}}$ *un caractère dominant,* $\theta = \{\alpha \in {}_{\mathbf{Q}}\Delta \mid (\chi, \alpha) > 0\}$, *et* $\theta' = {}_{\mathbf{Q}}\Delta - \theta$. *Soit* Φ *une fonction continue* > 0 *sur* $\mathrm{G}_{\mathbf{R}}$, *comparable à une fonction* > 0 *de type* (P, χ), *et invariante à droite par* $\Gamma \cap \mathrm{P}$ *et* $\mathrm{L}_{\theta'}$ (cf. 11.7). *Alors il existe une partie finie* C′ *de* $\mathrm{G}_{\mathbf{Q}}$ *contenant* C, *et un ensemble de Siegel* $\mathfrak{S}$, *par rapport à* K, P, S, *tels que pour tout* $g \in \mathrm{G}_{\mathbf{R}}$, *la fonction* $\Phi_g : u \mapsto \Phi(g.u)$, $(u \in \Gamma.\mathrm{C}')$ *atteigne son minimum en un point de* $g.\Gamma.\mathrm{C}' \cap \mathfrak{S}$.

Soit, comme plus haut :

$$\Gamma' = \Gamma \cap \Big(\bigcap_{c \in \mathrm{C}} c^{-1}.\Gamma.c \Big).$$

C'est un groupe arithmétique vérifiant $c.\Gamma' \subset \Gamma.c$, $(c \in \mathrm{C})$. D'après 15.4, on peut trouver une partie finie D de $\mathrm{L}_{\theta',\mathbf{Q}}$ telle que :

$$\mathrm{L}_{\theta',\mathbf{Q}} = (\Gamma' \cap \mathrm{L}_{\theta'}).\mathrm{D}.(\mathrm{P} \cap \mathrm{L}_{\theta'})_{\mathbf{Q}}.$$

Le théorème précédent implique l'existence d'une constante $t' > 0$ telle que

$$\mathrm{L}_{\theta',\mathbf{R}} = (\mathrm{K} \cap \mathrm{L}_{\theta'}).((\mathrm{P} \cap \mathrm{L}_{\theta'})(t')).\mathrm{D}^{-1}.(\Gamma' \cap \mathrm{L}_{\theta'}). \tag{1}$$

Soit $\mu > 1$, et soient $\sigma \in \Gamma$, $b \in \mathrm{C}$ tels que :

$$\Phi(g.\sigma.b) \leqq \mu.\Phi(g.\gamma.c) \qquad (\gamma \in \Gamma, \quad c \in \mathrm{C}).$$

Nous montrerons tout d'abord :

(*) *Il existe* $y \in g.\Gamma.\mathrm{C}.\mathrm{D} \cap \mathrm{K}.\mathrm{P}(\theta', t')$ *tel que* $\Phi(y) = \Phi(g.\sigma.b)$. On a la décomposition $\mathbf{G}_{\mathbf{R}} = \mathrm{K}.\mathrm{M}_{\theta',\mathbf{R}}\mathrm{L}_{\theta',\mathbf{R}}\mathrm{S}_{\theta',\mathbf{R}}\mathrm{V}_{\theta',\mathbf{R}}$ (11.8), ce qui permet d'écrire :

$$x = g.\sigma.b = k_x.m_x.l_x.s_x.v_x \qquad (k_x \in \mathrm{K},\ m_x \in \mathrm{M}_{\theta'},\ l_x \in \mathrm{L}_{\theta'},\ s_x \in \mathrm{S}_{\theta'},\ v_x \in \mathrm{V}_{\theta'}).$$

Soit $a(l_x)$ la composante dans $\mathrm{S} \cap \mathrm{L}_{\theta'}$, de $l_x \in \mathrm{L}_{\theta',\mathbf{R}}$ suivant la décomposition induite par la décomposition précédente. Vu (1), on peut trouver $\tau \in (\Gamma' \cap \mathrm{L}_{\theta'})$, $d \in \mathrm{D}$ tels que :

$$a(l_x.\tau.d)^{\alpha} \leqq t' \qquad (\alpha \in \theta').$$

Soit $y = x.\tau.d$. Comme $\mathrm{L}_{\theta'}$ centralise $\mathrm{S}_{\theta'}$ et normalise $\mathrm{V}_{\theta'}$, on a

$$a(l_y)^{\alpha} = a(l_x.\tau.d)^{\alpha} \leqq t' \qquad (\alpha \in \theta')$$

donc :

$$y \in \mathrm{K}.\mathrm{P}(\theta', t').$$

D'autre part, Φ étant invariante à droite par $\mathrm{L}_{\theta',\mathbf{R}}$, on a $\Phi(y) = \Phi(x)$. Enfin, vu la relation $c.\Gamma' \subset \Gamma.c$, on a $y = g.\sigma.b.\tau.d \in g.\Gamma.b.d$, ce qui prouve (*). Nous avons $\Phi(y) \leqq \mu.\Phi(g.u)$ pour $u \in \Gamma.\mathrm{C}$, donc aussi pour $u \in \Gamma.\mathrm{C}.\mathrm{D}$ puisque Φ est invariante à droite par D. Le lemme 16.6 montre alors l'existence d'une constante $t'' > 0$, indépendante de g, telle que $y \in \mathrm{K}.\mathrm{P}(\theta, t'')$, d'où, pour $t > 0$ convenable :

$$y \in \mathrm{K}.\mathrm{P}(t).$$

Soit :

$$\Gamma'' = \Gamma \cap \Big(\bigcap_{u \in \mathrm{CD}} u^{-1}.\Gamma.u \Big).$$

C'est un groupe arithmétique vérifiant $u.\Gamma'' \subset \Gamma.u$ $(u \in C.D)$. Soit ω un compact de $(M.U)_R$ tel que $(M.U)_R = \omega(\Gamma'' \cap MU)$ (cf. 8.4), et soit $\mathfrak{S} = K._Q A_t.\omega$. On peut donc trouver $\tau \in \Gamma'' \cap P$ tel que :

$$z = y.\tau = g.\sigma.b.d.\tau \in g.\Gamma.b.d \cap \mathfrak{S},$$

et l'on a :

$$\Phi(z) = \Phi(y) \leqq \mu\Phi(g.u) \qquad (u \in \Gamma.C.D).$$

Comme $\mathfrak{S} \cap g.\Gamma.C.D$ est fini (15.8) et que μ est un nombre quelconque > 1, cela démontre le théorème (avec $C' = C.D$).

16.10. COROLLAIRE. *La fonction* $\Psi : g \mapsto \min_{u \in \Gamma.C'} \Phi(g.u)$ *est continue sur* G_R.

La fonction Ψ est invariante à droite par Γ. Il suffit donc de l'étudier lorsque g varie dans $\mathfrak{S}.C'$, où $\mathfrak{S}$ est un ensemble de Siegel convenable, que l'on peut supposer ouvert.

Soit $A = \{\gamma \in \Gamma,\ \mathfrak{S}.C'\gamma \cap \mathfrak{S}.C'^{-1} \neq \emptyset\}$. Vu 16.9, on a :

$$\Psi(g) = \min_{u \in A.C'} \Phi(g.u), \qquad (g \in \mathfrak{S}.C').$$

Comme A est fini (15.4), on voit que si g varie dans l'ouvert $\mathfrak{S}.C'$, la fonction Ψ est le minimum d'un nombre fini de fonctions continues, donc Ψ est continue.

16.11. Nous terminerons par un théorème portant sur des minima successifs, qui généralise (1.13), (1.14). L'énoncé en est plus compliqué, cela étant dû essentiellement au fait que l'égalité $G_Q = \Gamma.P_Q$, qui est vraie dans le cas particulier où $\Gamma = \mathbf{GL}(n, \mathbf{Z})$ et où P est un sous-groupe parabolique standard de $\mathbf{GL}_n$, ne l'est pas nécessairement dans le cas général envisagé ici.

Soient :

$$_Q\Delta = \theta_1 \cup \ldots \cup \theta_s$$

une partition de $_Q\Delta$ et $\zeta_i = \theta_{i+1} \cup \ldots \cup \theta_s$ $(1 \leqq i \leqq s-1)$. On pose :

$$P_i = P_{\zeta_i}, \qquad L_i = L_{\zeta_i} \qquad (i = 1, \ldots, s-1),$$

$$P_0 = L_0 = G, \qquad L_s = P_s = \{e\}, \qquad C_0 = C, \qquad \Gamma_0 = \Gamma.$$

On définit par récurrence sur i, un sous-groupe arithmétique Γ_i de G et une partie finie C_i de P_{iQ} contenant e, sur laquelle tout $\chi \in X(P_i)_Q$ est trivial, vérifiant :

$$\Gamma_i = \bigcap_{c \in C.C_1 \ldots C_{i-1}} c^{-1}.\Gamma_{i-1}.c \qquad (1 \leqq i < s)$$

$$P_{i,Q} = (\Gamma_i \cap P_i).C_i.(P_i \cap P)_Q,$$

(cf. 15.7). On note χ_i un poids dominant tel que :

$$((\chi_i, \alpha) > 0, \qquad (\alpha \in {}_Q\Delta)) \Leftrightarrow \alpha \in \theta_i \qquad (i = 1, \ldots, s)$$

et Φ_i une fonction standard (14.4) de type (P, χ_i).

Enfin, on pose $D = C_0.C_1 \cdot \ldots \cdot C_{s-1}$.

16.12. THÉORÈME. *On conserve les notations de* 16.11.

(i) *Soit* $\mu \geqq 1$. *Il existe une constante* $t > 0$ *telle que si :*

$$g \in G_{\mathbf{R}} \quad et \quad \gamma_i \in \Gamma_i, \quad c_i \in C_i \quad (0 \leqq i \leqq s-1)$$

vérifient :

$$(1) \quad \Phi_i(g.\gamma_0.c_0 \cdots \gamma_{i-1}c_{i-1}) \leqq \mu.\Phi_i(g.\gamma_0.c_0 \cdots \gamma_{i-2}c_{i-2}.u_{i-1}), \quad (u_{i-1} \in (\Gamma_{i-1} \cap P_{i-1}).C_{i-1}), \quad (1 \leqq i \leqq s),$$

alors $g.\gamma_0.c_0 \cdots \gamma_{s-1}.c_{s-1} \in K.P(t)$.

(ii) *Il existe un ensemble de Siegel* $\mathfrak{S}$, *par rapport à* K, P, S, *tel que pour tout* $g \in G_{\mathbf{R}}$, *on puisse trouver* $\gamma_i \in \Gamma_i$, $c_i \in C_i$ $(0 \leqq i \leqq s-1)$ *vérifiant* (1) *avec* $\mu = 1$, *et* $g.\gamma_0.c_0 \cdots \gamma_{s-1}.c_{s-1} \in \mathfrak{S} \cap g.\Gamma.D$.

Le théorème étant contenu dans 16.7, 16.9 pour $s = 1$, nous procédons par récurrence sur s.

(i) Soient V_1 le radical unipotent de P_1 et $\pi : P_1 \to G' = P_1/V_1$ la projection canonique. La fonction Φ_i est invariante à gauche par K, à droite par V_1, donc définit une fonction Φ_i' sur G' qui vérifie :

$$\Phi_i(k.z) = \Phi_i'(\pi(z)) \qquad (k \in K \cap P_1, \quad z \in P_{1,\mathbf{R}}; \quad 1 \leqq i \leqq s).$$

Il est clair que Φ_i' est de type $(\pi(P), \chi_i)$ $(2 \leqq i \leqq s)$ et que ζ_1 s'identifie à l'ensemble des $\mathbf{Q}$-racines simples de G', par rapport à $\pi(S)$, et pour un ordre associé à $\pi(P)$. Écrivons $g.\gamma_0.c_0 = k.z$ $(k \in K, \ z \in P_{1,\mathbf{R}})$. Vu l'hypothèse de récurrence, il existe une constante t', ne dépendant pas de g, γ_i, c_i telle que l'on ait :

$$\pi(z.\gamma_1.c_1 \cdots \gamma_{s-1}.c_{s-1}) \in \pi(K \cap P_1).(\pi(P)\,(t')),$$

ce qui implique :

$$(2) \qquad g.\gamma_0.c_0 \cdots \gamma_{s-1}.c_{s-1} \in K.P(\zeta_1, t').$$

La fonction Φ_1 est invariante à droite par $\Gamma \cap P_1$ et par C_i $(i \geqq 1)$. Si l'on tient compte de la définition des groupes Γ_i, on voit que l'on peut écrire :

$$g.\gamma_0.c_0 \cdots \gamma_{s-1}c_{s-1} = g.\sigma.b \qquad (\sigma \in \Gamma, \ b = c_0 \ldots c_{s-1})$$

et que la condition :

$$\Phi_1(g.\gamma_0.c_0) \leqq \mu.\Phi_1(g.u) \qquad (u \in \Gamma.C)$$

entraîne :

$$\Phi_1(g.\sigma.b) \leqq \mu.\Phi_1(g.\gamma.d) \qquad (\gamma \in \Gamma, \ d \in C_0 \ldots C_{s-1}).$$

D'après (16.9), il existe donc une constante $t'' > 0$, indépendante de g, γ_i, c_i telle que l'on ait :

$$(3) \qquad g.\sigma.b \in K.P(\theta_1, t'').$$

Vu (16.5 (2)), l'assertion (i) résulte alors de (2) et (3).

(ii) La fonction $u \mapsto \Phi_1(g.u)$ $(u \in \Gamma.C)$ a un minimum (16.2). On peut donc trouver $\gamma_0' \in \Gamma$, $c_0 \in C$ tels que :

$$(4) \qquad \Phi_1(g.\gamma_0'.c_0) \leqq \Phi_1(g.u) \qquad (u \in \Gamma.C).$$

Considérant comme plus haut les fonctions Φ_i' sur G', on tire de l'hypothèse de récurrence l'existence de $c_i \in C_i$, $\gamma_i' \in \Gamma_i$ $(1 \leqq i \leqq s-1)$, tels que :

$$\Phi_i(g.\gamma_0'.c_0 \cdots \gamma_{i-1}'.c_{i-1}) \leqq \Phi_i(g.\gamma_0'.c_0 \cdots \gamma_{i-2}'.c_{i-2}.u_{i-1}) \quad (u_{i-1} \in (\Gamma_{i-1} \cap P_{i-1}).c_{i-1}) \qquad (1 \leqq i \leqq s). \tag{5}$$

Vu (i), il existe alors une constante $t > 0$, indépendante de g, γ_i', c_i, telle que :

$$g.\gamma_0'.c_0 \cdots \gamma_{s-1}'.c_{s-1} \in K.P(t). \tag{6}$$

La démonstration se termine alors comme celle de (16.7). Soient :

$$\Gamma'' = \bigcap_{d \in D} d^{-1}.\Gamma_{s-1}.d,$$

ω un compact de $(M.U)_R$ tel que $(M.U)_R = \omega(\Gamma'' \cap M.U)$, et $\mathfrak{S} = K.{}_Q A_t.\omega$. Il existe $\sigma \in \Gamma'' \cap M.U$ tel que :

$$g.\gamma_0'.c_0 \cdots \gamma_{s-1}'.c_{s-1}.\sigma \in \mathfrak{S}.$$

L'élément σ normalise $\Gamma_i \cap P_i$ $(0 \leqq i \leqq s-1)$ et l'on a $c_i.\sigma \in \Gamma_i.c_i$. Par conséquent, les éléments c_i $(0 \leqq i \leqq s-1)$ et :

$$\gamma_0 = \gamma_0'.\sigma, \qquad \gamma_i = \sigma^{-1}.\gamma_i'.\sigma \qquad (1 \leqq i \leqq s-1)$$

vérifient nos conditions.

17. Groupes de rang rationnel un

Dans ce paragraphe, on considère l'espace $X = K\backslash G_R/\Gamma$ des doubles classes de G modulo un sous-groupe compact maximal K et un groupe arithmétique Γ, lorsque G est de $\mathbf{Q}$-rang égal à un, et Γ est « net » au sens de (17.1). Cette dernière condition peut toujours être satisfaite en passant à un sous-groupe d'indice fini convenable (17.4). X est alors difféomorphe à l'intérieur d'une variété à bord compacte dont on décrira le bord explicitement (17.10).
(17.10) répond à une question posée par J.-P. Serre. Ce dernier a aussi influencé la rédaction de ce paragraphe, notamment en proposant la condition (17.1).

17.1. Soient k un corps commutatif, p la caractéristique de k, et Ω une clôture algébrique de k. Pour un élément $g \in \mathbf{GL}(n, k)$, on note $V(g)$ le groupe multiplicatif engendré dans Ω^* par les valeurs propres de g. On dit que g est *net* si $V(g)$ est sans torsion. Un sous-groupe de $\mathbf{GL}(n, k)$ est net si tous ses éléments le sont.
Il est clair que g est net si, et seulement si, sa partie semi-simple g_s l'est.

17.2. PROPOSITION. *Soit $g \in \mathbf{GL}(n, k)$ et soit $\mathscr{A}(g)$ le plus petit sous-groupe algébrique de $\mathbf{GL}(n, \Omega)$ contenant g. Alors g est net si, et seulement si, tout élément de $X(\mathscr{A}(g))$ dont la valeur en g est une racine de l'unité est égal à un sur g.*

Pour les propriétés de $\mathscr{A}(g)$ utilisées ci-dessous, *voir* par exemple [1].

On a $\mathscr{A}(g) = \mathscr{A}(g_s) \times \mathscr{A}(g_u)$, où $g = g_s . g_u$ est la décomposition de Jordan (7.3) de g. Comme $\mathscr{A}(g_u)$ est unipotent, il est dans le noyau de tout caractère, d'où un isomorphisme naturel $\mathrm{X}(\mathscr{A}(g)) \cong \mathrm{X}(\mathscr{A}(g_s))$, ce qui montre que l'on peut supposer g semi-simple. Alors $\mathscr{A}(g)$ est diagonalisable, donc $\mathscr{A}(g) = \mathrm{T} \times \mathrm{H}$ où T est un tore et H est fini, contenu dans un tore. Les caractères de H sont d'ordre fini, et séparent les points de H. Il s'ensuit immédiatement que chacune des deux conditions de la proposition entraîne que $g \in \mathrm{T}$, donc que $\mathrm{H} = \{e\}$. Après un changement de coordonnées convenable, on peut supposer que T est l'ensemble des matrices diagonales inversibles telles que $x_{i,i} = 1 \quad (i > d = \dim \mathrm{T})$. Les fonctions coordonnées $x_{j,j} \quad (j \leqq d)$ forment alors une base de $\mathrm{X}(\mathrm{T})$, et leurs valeurs en g engendrent $\mathrm{V}(g)$. Plus précisément, les éléments de $\mathrm{V}(g)$ sont les valeurs en g des éléments de $\mathrm{X}(\mathrm{T})$, d'où la proposition.

17.3. COROLLAIRE. *Soient* $\mathrm{G} \subset \mathbf{GL}(n, \Omega)$ *un groupe algébrique, et* $f : \mathrm{G} \to \mathbf{GL}(m, \Omega)$ *un morphisme. Si* $g \in \mathrm{G}$ *est net, alors* $f(g)$ *est net.*

On sait que $f(\mathscr{A}(g)) = \mathscr{A}(f(g))$, [1, § 2.1]. Si $a \in \mathrm{X}(\mathscr{A}(f(g)))$, alors $a \circ f \in \mathrm{X}(\mathscr{A}(g))$ et $(a \circ f)(g) = a(f(g))$. Il suffit donc d'appliquer 17.2.

Remarque. La condition équivalente à la netteté dans 17.2 peut être introduite dans un groupe affine, sans avoir recours à une réalisation linéaire. On peut donc parler d'éléments nets dans un groupe algébrique affine, et 17.3 reste vrai pour tout morphisme de groupes algébriques affines.

17.4. PROPOSITION. *Soient* G *un* $\mathbf{Q}$*-groupe et* Γ *un sous-groupe arithmétique de* G. *Alors* Γ *possède un sous-groupe de congruence qui est net.*

On peut supposer G identifié à un $\mathbf{Q}$-sous-groupe de $\mathbf{GL}(n, \mathbf{C})$ par un morphisme qui applique Γ dans $\mathbf{GL}(n, \mathbf{Z})$ (7.13). Il suffit donc de faire la démonstration pour $\mathbf{GL}(n, \mathbf{Z})$.

Soit M l'ensemble des polynômes cyclotomiques de degré $\leqq n$ et différents de $\mathrm{T} - 1$. Il est fini. Soit p un nombre premier ne divisant aucun des nombres $f(1)$, $(f \in \mathrm{M})$. Montrons que le groupe de congruence :

$$\mathrm{H} = \{g \in \mathbf{GL}(n, \mathbf{Z}), \quad g \equiv 1 \bmod p\}$$

est net.

Soient $g \in \mathrm{H}$, $(s_i)_{1 \leqq i \leqq n}$ les valeurs propres de g, et K le corps engendré sur $\mathbf{Q}$ par les s_i. Comme les s_i sont les racines du polynôme caractéristique de g, qui est de degré n, à coefficients rationnels, K est de degré $\leqq n$ sur $\mathbf{Q}$. Soit $s \in \mathrm{V}(g)$ une racine de l'unité. Nous devons montrer que $s = 1$. Supposons que ce ne soit pas le cas. Soit $\mathfrak{p}$ un idéal premier de K divisant p. Les s_i se réduisent mod $\mathfrak{p}$ en les valeurs propres de la réduction mod p de g, donc en un, et par suite $s \equiv 1 \bmod \mathfrak{p}$. Il existe $f \in \mathrm{M}$ tel que $f(s) = 0$. On a par conséquent $f(1) \equiv 0 \bmod \mathfrak{p}$, donc aussi mod p, d'où une contradiction.

La proposition précédente suffit pour les applications que nous avons en vue ici. Pour compléter, nous en donnons une version plus générale, dont la démons-

tration nous a été communiquée par Serre. Nous aurons besoin du lemme élémentaire suivant :

17.5. LEMME. *Soient* L *un anneau commutatif intègre et* $\mathfrak{m}$ *un idéal maximal de* L *tel que la caractéristique* p *de* $L/\mathfrak{m}$ *soit* $\neq 0$. *Soient* x *un élément inversible de* L, *d'ordre fini* n. *Si* $x \equiv 1 \bmod \mathfrak{m}$, *alors* n *est une puissance de* p.

Il suffit de faire voir que si $(n, p) = 1$, alors $x \not\equiv 1 \bmod \mathfrak{m}$. Si ce n'était pas le cas, on aurait $x = 1 + a$ $(a \in \mathfrak{m})$, d'où $x^n = 1 + a(n + b)$, $(b \in \mathfrak{m})$; puisque $x^n = 1$, cela entraîne $b + n = 0$, $n \in \mathfrak{m}$, donc n est divisible par p, contrairement à l'hypothèse.

17.6. PROPOSITION. *Soient* k *un corps de caractéristique zéro et* L *un sous-anneau de* k *qui est de type fini sur* $\mathbf{Z}$. *Soit* Γ *un sous-groupe de* $\mathbf{GL}(n, L)$. *Alors* Γ *possède un sous-groupe net d'indice fini.*

D'après Bourbaki, *Alg. Commutative*, Chap. V, § 3, n° 1, Corollaire 3, p. 62 on peut trouver un entier rationnel a tel que si p est un nombre premier ne divisant pas a, alors il existe un homomorphisme f_p de L dans un corps algébriquement clos de caractéristique p, qui applique 1 sur 1. Comme L est de type fini, $f_p(L)$ est un corps fini, donc $\mathfrak{m}_p = \ker f_p$ est un idéal maximal de L, à corps résiduel fini. Par suite $\Gamma_p = \{g \in \Gamma,\ g \equiv 1 \bmod \mathfrak{m}_p\}$ est d'indice fini. Il en est alors de même du groupe $\Gamma_{pq} = \Gamma_p \cap \Gamma_q$, si p et q sont premiers et premiers à a. Montrons que Γ_{pq} est net si, de plus $p \neq q$. Il suffit pour cela de faire voir que si $g \in \Gamma_p$ et si s est une racine de l'unité contenue dans le groupe $V(g)$ engendré par les valeurs propres s_i de g, alors s est une puissance de p. Les s_i sont entiers sur L. La L-algèbre L' engendrée par les s_i est donc entière sur L. Il existe par suite un idéal premier $\mathfrak{m}'_p$ de L' tel que $\mathfrak{m}'_p \cap L = \mathfrak{m}_p$. Comme $g \equiv 1 \bmod \mathfrak{m}_p$, on a $s_i \equiv 1 \bmod \mathfrak{m}'_p (1 \leqq i \leqq n)$ donc aussi $s \equiv 1 \bmod \mathfrak{m}'_p$. Notre assertion résulte alors de (17.5), appliqué à L' et $\mathfrak{m}'_p$.

17.7. COROLLAIRE. *Soit* H *un sous-groupe de type fini de* $\mathbf{GL}(n, k)$. *Alors* H *possède un sous-groupe net d'indice fini.*

Soit (h_j) $(j \in I)$ un système générateur fini de H. L'anneau L engendré par les coefficients des h_j et h_j^{-1} est de type fini sur $\mathbf{Z}$, et $H \subset \mathbf{GL}(n, L)$. On peut donc appliquer (17.6).

Remarque. (17.7) montre en particulier que H possède un sous-groupe d'indice fini sans torsion, ce qui est un résultat bien connu de Selberg.

17.8. Dans cette section, G est un $\mathbf{Q}$-groupe réductif connexe, de $\mathbf{Q}$-rang égal à un, Γ un sous-groupe arithmétique de G, K un sous-groupe compact maximal de $G_{\mathbf{R}}$, $D = K\backslash G_{\mathbf{R}}$ l'espace des classes à droite de $G_{\mathbf{R}}$ mod K. On note π la projection de $G_{\mathbf{R}}$ sur l'espace $D/\Gamma = K\backslash G_{\mathbf{R}}/\Gamma$ des doubles classes $K.x.\Gamma$ de $G_{\mathbf{R}}$. L'espace D est muni canoniquement d'une structure de variété C^∞, invariante par $G_{\mathbf{R}}$. Si Γ est

sans torsion, alors $\Gamma \cap x.K.x^{-1} = \{e\}$ pour tout $x \in G_{\mathbf{R}}$, donc Γ opère librement sur D, d'où aussi une structure naturelle de variété C^∞ sur $X = K\backslash G_{\mathbf{R}}/\Gamma$.
Soit $P = M.S.U$ un $\mathbf{Q}$-sous-groupe parabolique minimal de G, où M, S, U ont la signification usuelle (§ 12). On écrit P_0 pour $M_{\mathbf{R}}.U_{\mathbf{R}} = (M.U)_{\mathbf{R}}$ et A pour $S^0_{\mathbf{R}}$. On suppose $\mathfrak{S}$ normal (12.3), i.e. A stable par rapport à l'involution de Cartan de $G_{\mathbf{R}}$ associée à K (11.17), ce qui entraîne *(loc. cit)* que $K \cap M_{\mathbf{R}}$ est un sous-groupe compact maximal de $M_{\mathbf{R}}$, donc aussi de P_0. Soit C un système de représentants des doubles classes $P_{\mathbf{Q}}.x.\Gamma$ dans $G_{\mathbf{Q}}$. Vu (15.6), il est fini, et il existe un ensemble de Siegel $\mathfrak{S}$ par rapport à K, P, S (12.3), que nous prendrons ici *ouvert*, tel que :

$$G_{\mathbf{R}} = \Omega.\Gamma \qquad \text{avec} \qquad \Omega = \mathfrak{S}.C. \tag{1}$$

L'ensemble $\mathfrak{S}$ est de la forme $K.A_t.\omega$, où ω est relativement compact dans $P^0_0 = M^0_{\mathbf{R}}.U_{\mathbf{R}}$. Quitte à agrandir ω, on peut supposer que ω est un ensemble fondamental dans P^0_0 pour l'intersection des groupes $P^0_0 \cap c.\Gamma.c^{-1}$ $(c \in C)$. On a alors, en particulier :

$$P^0_0 = \omega.(P^0_0 \cap {}^c\Gamma) \qquad (c \in C) \tag{2}$$

$$P_0 = (K \cap M).\omega.(P^0_0 \cap {}^c\Gamma) \qquad (c \in C). \tag{3}$$

L'ensemble ${}_{\mathbf{Q}}\Delta$ des $\mathbf{Q}$-racines simples se compose ici d'un élément, soit α, et l'on a :

$$A_t = \{a \in A, \quad a^\alpha < t\}. \tag{4}$$

Étant donné s $(0 < s < t)$, on pose :

$$A_{s,t} = \{a \in A, \quad s \leqq a^\alpha < t\} \tag{5}$$

$$\mathfrak{S}_{s,t} = K.A_{s,t}.\omega, \qquad \mathfrak{S}_s = K.A_s.\omega. \tag{6}$$

Il est clair que $\mathfrak{S}_{s,t}$ est relativement compact et que :

$$\mathfrak{S} = \mathfrak{S}_{s,t} \cup \mathfrak{S}_s, \qquad \mathfrak{S}_{s,t} \cap \mathfrak{S}_s = \emptyset.$$

L'ensemble fondamental $\Omega = \mathfrak{S}.C$ est donc réunion d'un ensemble relativement compact $\mathfrak{S}_{s,t}.C$ et des ensembles $\mathfrak{S}_s.c$ $(c \in C)$. Pour s assez petit, ces derniers jouent un rôle analogue à celui des pointes du domaine fondamental polygonal classique d'un groupe fuchsien, et seront aussi appelés pointes de Ω.

17.9. PROPOSITION. *On conserve les hypothèses et notations de* (17.8). *Il existe* $s > 0$ *tel que* $X = K\backslash G_{\mathbf{R}}/\Gamma$ *soit réunion d'un ensemble relativement compact* $\pi(\mathfrak{S}_{s,t}.C)$ *et d'ouverts disjoints* $\pi(\mathfrak{S}_s.c)$ $(c \in C)$. *De plus, la relation :*

$$K.A_s.P_0.c.\gamma \cap K.A_s.P_0.c' \neq \emptyset \qquad (c, c' \in C; \quad \gamma \in \Gamma)$$

entraîne $c = c'$, $c.\gamma.c^{-1} \in P$.

D'après la propriété de Siegel (15.4), l'ensemble L des $\gamma \in \Gamma$ tels que $\Omega.\gamma \cap \Omega \neq \emptyset$ est fini. On peut donc trouver s assez petit pour que, quels que soient $c, c' \in C$ et $\gamma \in L$, l'intersection $\mathfrak{S}_s.c.\gamma \cap \mathfrak{S}_s.c'$ soit ou bien vide ou bien non relativement compacte. Dans le deuxième cas, on a alors, d'après (12.6), $c.\gamma \in P_{\mathbf{Q}}.c'$, ce qui, vu le choix de C, entraîne aussi $c = c'$, et démontre la première assertion.

Soient $c, c' \in C$, $x \in \Gamma$, $k, k' \in K$, $p, p' \in P_0$, $a, a' \in A_s$ tels que :

$$k.a.p.c.x = k'.a'.p'.c'.$$

Vu 17.8 (3), on peut écrire :

$$p = k_1.q_1.c.x_1.c^{-1}, \quad p' = k_1'.q_1'.c'.x_1'.c'^{-1}$$

avec $k_1, k_1' \in K \cap M$, $q_1, q_1' \in \omega$, $x_1 \in \Gamma \cap c^{-1}.P.c$, $x_1' \in \Gamma \cap c'^{-1}.P.c'$.
On a donc :

$$\mathfrak{S}_s.c.x_1.x.x_1'^{-1}.c'^{-1} \cap \mathfrak{S}_s \neq \varnothing$$

donc, vu ce qui a été dit plus haut, entraîne :

$$c = c' \qquad c.x_1.x.x_1'^{-1}.c^{-1} \in P$$

et par conséquent, $c.x.c^{-1} \in P$.

17.10. THÉORÈME. *On conserve les hypothèses et notations de* 17.9, *et on suppose de plus* Γ *net* (17.1). *Alors* ${}^x\Gamma \cap P \subset MU$ *pour tout* $x \in G_{\mathbf{Q}}$. *Pour tout* $c \in C$, *l'application* π *induit un difféomorphisme* ν_c *du produit* $(0, s) \times (K \cap M)\backslash(MU)_{\mathbf{R}}/({}^c\Gamma \cap P)$ *sur* $\pi(\mathfrak{S}_s.c)$. *L'espace* X, *muni de sa structure naturelle de variété* C^∞, *s'identifie à l'intérieur d'une variété à bord* $\overline{Y}$ *compacte* C^∞.
Il existe une bijection de C *sur l'ensemble des composantes connexes du bord* $\partial\overline{Y}$ *de* $\overline{Y}$ *qui envoie* $c \in C$ *sur une variété difféomorphe à* $E_c = (K \cap M)\backslash(M.U)_{\mathbf{R}}/({}^c\Gamma \cap P)$.

Le groupe ${}^x\Gamma \cap P$ est arithmétique dans P. Par suite, si $a \in X(P)_{\mathbf{Q}}$, alors le groupe $a({}^x\Gamma \cap P)$ est arithmétique dans $\mathbf{GL}_1$ (8.10), donc est contenu dans $\{\pm 1\}$. Si Γ est net, il s'ensuit que $a({}^x\Gamma \cap P) = \{e\}$. Comme M.U est l'intersection des noyaux des éléments de $X(P)_{\mathbf{Q}}$, cela prouve la première assertion.
Soit $c \in C$. Posons $\omega' = (K \cap M_{\mathbf{R}}).\omega$. On a :

$$\pi(\mathfrak{S}_s.c) = \pi(A_s.\omega'.c) = \pi(A_s.\omega'.c.(\Gamma \cap c^{-1}Pc)).$$

Vu la première assertion et 17.8 (3), cela donne :

$$\pi(\mathfrak{S}_s.c) = \pi(A_s.P_0.c).$$

Soient $m, m' \in M_{\mathbf{R}}$, $u, u' \in U_{\mathbf{R}}$, $a, a' \in A_s$ tels que :

$$\pi(a.m.u.c) = \pi(a'.m'.u'.c).$$

Il existe donc $k \in K$ et $x \in \Gamma$ tels que :

$$a.m.u.c.x = k.a'.m'.u'.c.$$

Il résulte alors de 17.9 que $c.x.c^{-1} \in P$, d'où aussi, compte tenu de la première assertion, $c.x.c^{-1} \in P_0$. On a alors $k \in P_0$, donc $k \in P_0 \cap K = MU \cap K = M \cap K$. Comme $A \cap P_0 = \{e\}$, il s'ensuit que l'on a :

$$a = a', \qquad m.u.c.x.c^{-1} = k'.m'.u'$$

ce qui établit la deuxième assertion.
Comme $Q = \pi(\mathfrak{S}_{s,t}.C)$ est relativement compact, on peut trouver r $(0 < r < s)$ tel que $\pi(\mathfrak{S}_r.C) \cap Q = \varnothing$. Soit encore q tel que $0 < q < r$ et fixons un difféomorphisme μ de $(0, s)$ sur (q, s) qui soit l'identité sur (r, s). Notons aussi μ le difféomorphisme $\mu \times \mathrm{Id}$ de $(0, s) \times E_c$ sur $(q, s) \times E_c$. Alors $\mu_c = \nu_c \circ \mu \circ \nu_c^{-1}$ est un

difféomorphisme de $\pi(\mathfrak{S}_s, c)$ sur un ouvert relativement compact U_c. Ce dernier est en fait $\pi(\mathfrak{S}_{(q),s}, C)$, où l'on pose :

$$\mathfrak{S}_{(q),s} = K.A_{(q),s}.\omega, \qquad A_{(q),s} = \{a \in A \mid q < a^\alpha < s\}.$$

La collection des μ_c, et l'identité sur Q, définissent alors un difféomorphisme de X sur un ouvert Y, relativement compact, réunion de Q et des U_c ($c \in C$). Le bord $\partial Y = \overline{Y} - Y$ de Y est la réunion des sous-ensembles disjoints $\nu_c(\{q\} \times E_c)$. Ce sont des sous-variétés compactes. La réunion des images des sous-espaces $\nu_c([q,r) \times E_c)$ est un voisinage ouvert de ∂Y difféomorphe au produit de ∂Y par un intervalle, d'où la dernière assertion.

Remarque. Raghunathan [25] a montré que si H est un **Q**-groupe réductif connexe, L un sous-groupe compact maximal de H_R et Γ un sous-groupe arithmétique sans torsion de H, alors le quotient $L\backslash H_R/\Gamma$ a même type d'homotopie que l'intérieur d'une variété à bord compacte.

17.11. *Une fibration de* E_c. Le groupe ${}^c\Gamma \cap P$ opère librement et proprement sur $(K \cap M)\backslash P_0$. Le groupe ${}^c\Gamma \cap U$ est normal dans ${}^c\Gamma \cap P$. Par conséquent, le quotient $L_c = ({}^c\Gamma \cap P)/({}^c\Gamma \cap U)$ opère librement et proprement dans :

$$(K \cap M)\backslash P_0/({}^c\Gamma \cap U).$$

De plus, comme P_0 est produit semi-direct de M_R et U_R, il est clair que :

$$(1) \qquad (K \cap M)\backslash P_0/({}^c\Gamma \cap U) \approx (K \cap M)\backslash M_R \times U/({}^c\Gamma \cap U)$$

où $\approx$ signifie « difféomorphe ».

Le groupe U_R est normal dans P_R, donc ${}^c\Gamma \cap P$ opère par automorphismes intérieurs sur U_R, d'où une représentation de L_c comme groupe de difféomorphismes de $F_c = U_R/({}^c\Gamma \cap U)$.

La projection $\sigma : P_0 \to P_0/U_R \cong M_R$ induit un isomorphisme de L_c sur :

$$L_c' = \sigma({}^c\Gamma \cap P).$$

En particulier, L_c' est sans torsion, discret. (En fait, comme σ est la restriction d'un **Q**-morphisme de groupes algébriques, L_c' est arithmétique, et net vu (17.3).) Donc L_c' opère librement et proprement sur $(K \cap M)\backslash M_R$ et $B_c = (K \cap M)\backslash M_R/L_c'$ est une variété C^∞. Il résulte alors de (1) que E_c est l'espace total d'une fibration différentiable de fibre type F_c, groupe structural L_c, base B_c, dont la projection σ_c est induite par σ.

Le groupe U est commutatif si, et seulement si, 2α n'est pas une **Q**-racine. Si U est commutatif, alors F_c est un tore compact (au sens de la théorie des groupes topologiques).

Remarquons encore que si le **R**-rang de G est aussi égal à un, alors M_R est compact, donc $E_c = F_c$. Si U est commutatif, le bord de $\overline{Y}$ est alors formé de tores.

Comme G est de rang rationnel un, X possède une seule compactification « de Satake », du type décrit dans [2]. On peut l'obtenir en prenant le quotient de l'espace $\overline{Y}$ de (17.10) par la relation d'équivalence qui est l'identité sur l'intérieur de $\overline{Y}$ et est définie par la projection σ_c sur la composante connexe du bord correspondant à $c \in C$. C'est donc la réunion de X et des bases B_c ($c \in C$) des fibrations mentionnées ci-dessus.

BIBLIOGRAPHIE

[1] A. BOREL, *Linear algebraic groups*, Notes by H. BASS, New York, Benjamin, 1969.

[2] —, *Ensembles fondamentaux pour les groupes arithmétiques*, coll. « Théorie des Groupes algébriques », Bruxelles, 1962.

[3] —, Arithmetic properties of linear algebraic groups, *Proc. I.C.M.*, Stockholm, 1962, 10-22.

[4] —, Density and maximality of arithmetic subgroups, *J. f. reine u. ang. Math.*, *224* (1966), 78-89.

[5] — and HARISH-CHANDRA, Arithmetic subgroups of algebraic groups, *Annals of Math.* (2), *75* (1962), 485-535.

[6] — et J.-P. SERRE, Théorèmes de finitude en cohomologie galoisienne, *Comm. Math. Helv.*, *39* (1964), 111-164.

[7] — et J. TITS, Groupes réductifs, *Publ. Math. I.H.E.S.*, *27* (1965), 55-150.

[8] N. BOURBAKI, Intégration, chap. 7, 8, *Act. Sci. Ind.*, 1306, Paris, Hermann éd., 1963.

[9] C. CHEVALLEY, *Théorie des groupes de Lie*, t. II : *Groupes algébriques*, Paris, 1951; t. III : *Groupes algébriques*, Paris, Hermann éd., 1955.

[10] —, *Séminaire sur la classification des groupes de Lie algébriques*. Notes polycopiées, Institut H.-Poincaré, Paris, 1956-1958.

[11] R. FRICKE-F. KLEIN, *Vorlesungen über die Theorie der automorphen Funktionen*, I, Leipzig, Teubner, 1897.

[12] R. GODEMENT, *Domaines fondamentaux des groupes arithmétiques*, Sém. Bourbaki, 15e année (1962-1963), Exp. 257.

[13] C. HERMITE, *Œuvres complètes*, vol. I, Paris, Gauthier-Villars, 1905.

[14] C. JORDAN, Mémoire sur l'équivalence des formes, *J. Éc. Polytech.*, XLVIII, 1880, 112-150; *Œuvres complètes*, t. III, 421-461.

[15] A. KORKINE et G. ZOLOTAREFF, Sur les formes quadratiques, *Math. Annalen*, *6* (1873), 366-389.

[16] K. MAHLER, *On lattice points in n-dimensional star bodies* : I. *Existence theorems*, Proc. Roy. Soc. London, A 187 (1946), 151-187.

[17] H. MINKOWSKI, Diskontinuitätsbereich für arithmetische Aequivalenz, *J. f. reine u. ang. Math.*, *129* (1905), 220-274; *Ges. Werke*, *2*, 53-100.

[18] L. J. MORDELL, *The arithmetically reduced indefinite quadratic form in n-variables*, Proc. Roy. Soc. London, A 131 (1931), 99-108.

[19] G. D. MOSTOW, Self-adjoint group, *Annals of Math.* (2), *62* (1955), 44-55.

[20] —, Fully reducible subgroups of algebraic groups, *Amer. J. Math.*, *78* (1956), 200-221.

[21] — and T. TAMAGAWA, On the compactness of arithmetically defined homogeneous spaces, *Annals of Math.* (2), *76* (1962), 446-463.

[22] D. MUMFORD, Geometric invariant theory, *Erg. d. Math. u. i. Grenzgeb. N. F.*, Springer-Verlag, *34* (1965).

[23] M. NAGATA, Note on orbit spaces, *Osaka M. J.*, *14* (1962), 21-31.

[24] H. POINCARÉ, Sur les formes cubiques ternaires et quaternaires, *J. Éc. Polytechn.*, *51* (1882), 45-91; *Œuvres complètes*, t. 5, 294-334.

[25] M. S. RAGHUNATHAN, A note on quotients of real algebraic groups by arithmetic subgroups, *Invent. Math.*, *4* (1968), 318-335.

[26] M. ROSENLICHT, Some basic theorems on algebraic groups, *Amer J. Math.*, *78* (1956), 401-443.

[27] —, On quotient varieties and the affine embedding of certain homogeneous spaces, *Trans. Amer. Math. Soc.*, *101* (1961), 211-233.

[28] J.-P. SERRE, Corps locaux, Publ. Inst. Math. Nancago VIII, *Act. Sci. Ind.*, 1296, Paris, Hermann éd., 1962.
[29] C. L. SIEGEL, Einheiten quadratischer Formen, *Abh. Math. Sem. Hamburg*, *13* (1940), 209-239; *Gesammelte Werke*, II, 138-168.
[30] —, Symplectic geometry, *Amer. J. Math.*, *65* (1943), 1-85; *Gesammelte Werke*, II, 274-359.
[31] X. STOUFF, Remarques sur quelques propositions dues à M. Hermite, *Annales E. N. S.* (3), *19* (1902), 89-118.
[32] A. WEIL, *Discontinuous subgroups of classical groups*, Notes by A. WALLACE, University of Chicago, 1958.
[33] —, *Adeles and algebraic groups*, Notes by M. DEMAZURE and T. ONO, Princeton, N. J., The Institute for Advanced Study, 1961.

INDEX

IMPRIMÉ EN FRANCE PRESSES UNIVERSITAIRES DE FRANCE
N° 21 362
DÉPÔT LÉGAL DEUXIÈME TRIMESTRE 1969
NUMÉRO D'ÉDITION 2263
HERMANN, ÉDITEURS DES SCIENCES ET DES ARTS

中華民國七十三年三月

六藝出版社

發行人：曾　蘭　英
社　址：新竹市東美路45號之24
電　話：０３５－７１４６３６
門　市：新竹市光復路1030號
電　話：０３５－７１６７５３
郵　撥：１６１４９６號數學園雜誌社
登　記：局版台業字１５９６號

定　價：＄110元