

SÉMINAIRE N. BOURBAKI

ROGER GODEMENT

Domaines fondamentaux des groupes arithmétiques

Séminaire N. Bourbaki, 1964, exp. n° 257, p. 201-225

<http://www.numdam.org/item?id=SB_1962-1964__8__201_0>

© Association des collaborateurs de Nicolas Bourbaki, 1964, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (<http://www.bourbaki.ens.fr/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

DOMAINES FONDAMENTAUX DES GROUPES ARITHMÉTIQUES

par Roger GODEMENT

Le fait qu'on peut construire, à l'aide d'inégalités simples, un domaine fondamental de mesure finie pour le groupe $SL(n, \mathbb{Z})$ dans $SL(n, \mathbb{R})$ a été étendu récemment par BOREL et HARISH-CHANDRA à tous les groupes linéaires algébriques définis sur le corps des rationnels (le volume fini, et la compacité quand il y a lieu, sont obtenus dans [2], mais les résultats les plus précis, et qui sont nouveaux même pour la plupart des groupes classiques, se trouvent dans [1], recueil d'énoncés dont les démonstrations n'ont pas encore paru). Le critère de compacité pour $G_{\mathbb{R}}/G_{\mathbb{Z}}$ a d'autre part été démontré directement par MOSTOW et TAMAGAWA [4] à l'aide de méthodes tout à fait différentes de celles de BOREL et HARISH-CHANDRA, nettement plus simples, mais qui, jusqu'à présent, n'avaient pas été étendues au cas général.

Le but de cet exposé est de montrer qu'en fait on peut étendre la méthode de MOSTOW et TAMAGAWA de façon à obtenir, dans le cas général, les inégalités à la Minkowski annoncées par BOREL dans [1], et obtenir ainsi une démonstration fort simple de celles-ci, plus simple même, on l'espère, que celle de BOREL... Cette nouvelle démonstration a été obtenue récemment par A. WEIL et le conférencier.

On ne suppose connus du lecteur, outre bien entendu le matériel de la théorie des groupes algébriques qu'on peut trouver dans le Séminaire Chevalley, dans [3], et dans les articles passés, présents et à venir de BOREL, que les notions les plus simples sur les groupes adéliques, qu'on trouvera dans les premières pages de [6]. Si G désigne un groupe linéaire algébrique défini sur le corps $k = \mathbb{Q}$ des nombres rationnels, on note $G_{\mathbb{A}}$ le groupe adélique correspondant, et $G_{\mathbb{A}}^0$ le sous-groupe fermé de $G_{\mathbb{A}}$ ensemble des g tels que $|\chi(g)| = 1$ pour tout caractère rationnel χ de G défini sur k ; on a évidemment $G_k \subset G_{\mathbb{A}}^0$ en vertu de la formule du produit.

1. La réduction de Minkowski dans $GL(n)$.

1.1. - Hauteurs.

Soit V un espace vectoriel de dimension finie défini sur k comme variété algébrique (en sorte que, pour toute extension k' de k , l'ensemble $V_{k'}$ se déduit du vectoriel V_k par extension à k' des scalaires). Il est clair

que V_A est le A -module déduit de V_k par extension à A de l'anneau de base k , et que $GL(V)_A$ s'identifie canoniquement à $GL(V_A)$. On dira qu'un $x \in V_A$ est primitif s'il existe un $g \in GL(V_A)$ tel que $g(x)$ soit un élément non nul de V_k . Si l'on a choisi une base (a_i) de V_k sur k , cela veut dire que $x_p \neq 0$ pour tout p et que, pour presque tout p fini, les coordonnées de x_p par rapport à cette base sont des entiers p -adiques premiers entre eux.

Sur l'ensemble des éléments primitifs de V_A , on appelle hauteur toute fonction $\|x\|$, à valeurs strictement positives, obtenue de la façon suivante : pour chaque p (fini ou non) on choisit sur $V_p = V_{k_p}$ une norme $\|\cdot\|_p$ compatible avec la valeur absolue définie sur k_p , et cela de telle sorte que, pour presque tout p fini, et pour tout $x \in V_p$, le nombre $\|x\|_p$ soit le maximum des valeurs absolues des coordonnées de x par rapport à une base de V_k choisie une fois pour toutes. Ceci fait, on pose

$$\|x\| = \prod \|x_p\|_p$$

pour tout $x \in V_A$ primitif. On vérifie aussitôt les propriétés suivantes :

- (i) si $\|x\|'$ et $\|x\|''$ sont deux hauteurs, le rapport $\|x\|'/\|x\|''$ reste dans un compact fixe de $\mathbb{R}_+^*$ quand x varie
- (ii) si des $x_n \in V_A$ primitifs tendent vers 0 dans V_A alors $\|x_n\|$ tend vers 0
- (iii) inversement, si $\|x_n\|$ tend vers 0, il existe des rationnels non nuls λ_n tels que $\lambda_n x_n$ tende vers 0 dans V_A
- (iv) pour tout $g \in GL(V_A)$ l'ensemble des $\xi \in V_k$ non nuls tels que $\|g(\xi)\| < c$ est fini modulo k^* (et en particulier il y a un $\xi \neq 0$ tel que $\|g(\xi)\|$ soit minimum)
- (v) on a $\|tx\| = |t| \cdot \|x\|$ pour tout $t \in A^*$ et tout $x \in V_A$ primitif
- (vi) si M est une partie compacte de $GL(V_A)$, il y a des constantes $c', c'' > 0$ telles que l'on ait

$$c' \|x\| \leq \|m(x)\| \leq c'' \|x\|$$

pour tout $m \in M$ et tout $x \in V_A$ primitif.

1.2. - Réduction de Minkowski.

Prenons dans ce qui précède pour V l'espace vectoriel canonique de dimension n , en sorte que $V_k = k^n$, $V_A = A^n$ et $GL(V) = GL(n)$. On utilise dans ce qui suit sur l'ensemble des éléments primitifs de A^n la hauteur canonique, qui

s'obtient comme suit : pour p fini, et $x \in V_p$, on pose $\|x\|_p = \text{maximum des valeurs absolues des coordonnées de } x \text{ par rapport à la base canonique}$; pour p infini, et $x \in V_p = \mathbb{R}^n$, on prend $\|x\|_p = \text{racine carrée de la somme des carrés des coordonnées de } x$. Posant $G = GL(n)$, on désignera par K le sous-groupe compact de $G_A = GL(n, A)$ défini comme suit : on pose $K = \prod_p K_p$ où $K_\infty = O(n)$, groupe orthogonal, et où, pour p fini, $K_p = GL(n, \mathbb{Z}_p)$. Enfin on note $(e_i)_{1 \leq i \leq n}$ la base canonique de k^n .

Il est bien connu (et élémentaire) que toute matrice $g \in G_A = GL(n, A)$ peut se mettre sous la forme $g = kt$, où $k \in K$ et où t est triangulaire. On va montrer que, pour toute $g \in G_A$, il existe $\gamma \in G_k = GL(n, k)$ telle que $\gamma g = kt$, où $k \in K$ et où t est une matrice triangulaire dont les termes diagonaux $t_i \in A^*$ vérifient les inégalités

$$|t_i/t_{i+1}| \leq c = 2/\sqrt{3}.$$

En effet, d'après la propriété (iv) du n° 1.1 on peut, modulo G_k , supposer que $\|g(e_1)\| \leq \|g(\xi)\|$ pour tout $\xi \in V_k$ non nul ; posant $g = kt$ ($k \in K$, t triangulaire, en sorte que $\|g(e_1)\| = |t_1|$, vu que la hauteur canonique est invariante par K), et raisonnant par récurrence sur n en utilisant le sous-groupe de G qui laisse fixe e_1 et stabilise le sous-espace engendré par les autres vecteurs de base, on peut supposer déjà réalisées les conditions $|t_i/t_{i+1}| \leq c$ pour $i \geq 2$. Expriment que $\|g(e_1)\| \leq \|g(\xi)\|$ lorsque ξ est combinaison linéaire de e_1 et e_2 , il vient

$$|t_1| \leq \|(\lambda + \mu u) t_1 e_1 + \mu t_2 e_2\|$$

quels que soient $\lambda, \mu \in k$ non tous deux nuls, u étant un certain coefficient de la matrice t ; posant $x = t_1/t_2$ il vient donc $|x| \leq \|(u + v) x e_1 + e_2\|$ pour tout $v \in k$; comme on ne change pas les deux membres de cette inégalité en multipliant x par un idèle dont chaque composante est de valeur absolue 1, on voit qu'on peut se ramener au cas où x est produit d'un élément non nul de k par un élément de $k_\infty = \mathbb{R}$, puis (en modifiant u et v) au cas où $x_p = 1$ pour tout p fini ; ceci fait, on observe que, pour tout $u \in A$, il existe $v \in k$ tel que $u_p + v_p$ soit entier pour tout p fini et que $|u_\infty + v_\infty| \leq \frac{1}{2}$ (miracle dont le rédacteur ne se sent pas responsable) ; il vient alors, pour cette valeur de v , l'inégalité $|x| \leq \sqrt{1 + |x|^2/4}$, ce qui montre comme annoncé que $|t_1/t_2| \leq c$.

[Il serait instructif d'étendre si possible la méthode précédente à la caractéristique p , i. e. en prenant pour corps de base $k = \mathbb{F}_p(X)$ au lieu du corps des rationnels.]

2. Critère de Mahler.2.1. - Une propriété de propreté.

Soient G un groupe linéaire algébrique défini sur k et H un sous-groupe fermé et défini sur k de G . On a évidemment une injection continue de H_A/H_k dans G_A/G_k ; on va montrer que celle-ci est propre lorsqu'on la restreint à H_A^0/H_k , autrement dit (c'est la même chose car il s'agit d'espaces localement compacts dénombrables à l'infini) que cette application induit un homéomorphisme de H_A^0/H_k sur un sous-espace fermé de G_A/G_k . On va faire la démonstration pour G connexe, le cas général s'y ramenant immédiatement.

Dans ce cas, il existe en effet un vectoriel V défini sur k , une représentation ρ de G dans V , définie sur k , et un $a \in V_k$ non nul tels que H soit le sous-groupe stabilisant la droite engendrée par a . Pour tout $h \in H_A$ on a alors évidemment $\rho(h)a = ta$ où $t \in A^*$; inversement, si $h \in G_A$ possède cette propriété, chaque composante h_p de h laisse stable la droite engendrée par a , donc appartient à H_p , et $h \in H_A$.

Soient λ le caractère de H donné par $\rho(h)a = \lambda(h)a$ et H_A^λ le sous-groupe $|\lambda(h)| = 1$ de H_A ; on va montrer que l'image de H_A^λ/H_k dans G_A/G_k est fermée, autrement dit que $H_A^\lambda G_k$ est fermé dans G_A . Soit $I^0(k)$ le groupe des idèles de valeur absolue 1 de k ; d'après ce qui précède, $H_A^\lambda G_k$ est l'image réciproque de $I^0(k) \cdot \rho(G_k)a$ par l'application continue $g \rightarrow \rho(g)a$ de G_A dans V_A ; il suffit donc de montrer que $I^0(k) \cdot \rho(G_k)a$ est fermé dans V_A ; or $I^0(k)$ est produit d'un compact par k^* , et $k^* \cdot \rho(G_k)a \subset V_k$ est fermé, car discret.

On a ainsi une injection continue de H_A^λ/H_k sur un sous-espace fermé de G_A/G_k ; comme il s'agit d'espaces localement compacts dénombrables à l'infini, cette injection est un homéomorphisme. Comme H_A^0/H_k est évidemment un fermé de H_A^λ/H_k , la démonstration est achevée.

2.2. - Le critère de Mahler.

Le voici :

THÉOREME 1. - Soient V un espace vectoriel défini sur k et G un sous-groupe fermé et défini sur k de $GL(V)$. Pour qu'une partie M de G_A^0 soit relativement compacte modulo G_k , il faut et il suffit que la propriété suivante soit vérifiée : étant donnés des $m_n \in M$ et des $\xi_n \in V_k$ tels que $m_n(\xi_n)$ tende vers 0 dans V_A , on a $\xi_n = 0$ pour n grand.

Tout d'abord le résultat de 2.1 permet immédiatement de se borner au cas où $G = GL(V)$; on suppose dans ce qui suit que V est l'espace canonique de dimension n , donc que $G = GL(n)$.

Supposons M compact modulo G_K ; si $m_n(\xi_n)$ tend vers 0 , on peut poser $m = k_n \gamma_n$ où les k_n restent dans un compact de G_A et où $\gamma_n \in G_K$; alors il est clair que $\gamma_n(\xi_n) \in V_K$ tend vers 0 , donc est nul pour n grand par dis-
crétion ...

Supposons inversement la condition vérifiée. La propriété (iii) de 1.1 montre aussitôt qu'il existe $c > 0$ tel que $\|m(\xi)\| \geq c$ pour tout $m \in M$ et tout $\xi \in k^n$ non nul ; comme on raisonne modulo G_K , on peut supposer $m \equiv kt$ avec $k \in K$ et t triangulaire telle que $|t_i/t_{i+1}| \leq c'$ (cf. 1.2), on a $|t_1| = \|m(e_1)\| \geq c$, et d'autre part $|t_1 \dots t_n| = 1$ vu que $M \subset G_A^0$; d'où des majorations

$$0 < c_1 \leq |t_i| \leq c_2 < +\infty$$

en sorte que les t_i restent dans un compact de A^* modulo k^* , et comme les matrices triangulaires vérifiant ces conditions forment évidemment un compact modulo les matrices triangulaires rationnelles, la démonstration est terminée.

3. Où l'on se débarrasse des groupes résolubles.

THÉOREME 2 (ONO). - Soit G un groupe linéaire algébrique résoluble défini sur k ; l'espace G_A^0/G_K est compact.

Soit ρ une représentation linéaire de G dans un vectoriel V , le tout défini sur k ; tout revient à montrer que, si des $g_n \in G_A^0$ et des $\xi_n \in V_K$ sont tels que $\rho(g_n) \xi_n$ converge vers 0 dans V_A , alors $\xi_n = 0$ pour n grand (en effet, une fois ce point établi, il reste à appliquer le critère de Mahler en prenant ρ fidèle). On va raisonner par récurrence sur $\dim(V)$, le cas où $\dim(V) = 0$ ne présentant pas de difficulté.

Considérons sur V un polynôme P homogène et semi-invariant par G , i. e. tel que

$$P[\rho(g) x] = \chi(g) P(x)$$

où χ est un caractère rationnel de G , et supposons P défini sur k (auquel cas χ l'est aussi). L'application de V_A dans A définie par P est continue,

donc $P[\rho(g_n) \xi_n]$ converge vers 0 dans A , de sorte qu'il en est de même, vu (ii) de 1.1, de

$$|P[\rho(g_n) \xi_n]| = |\chi(g_n)| \cdot |P(\xi_n)| = |P(\xi_n)| \quad ;$$

or $P(\xi_n)$ est rationnel, donc nul ou bien de valeur absolue 1 ; par suite, on a $P(\xi_n) = 0$ pour tout n assez grand.

Pour achever la démonstration, notons que, puisque G est résoluble, on peut trouver un semi-invariant F homogène et de degré 1 défini sur la clôture algébrique $\bar{K}$ de k (prendre un vecteur propre de G dans le dual de V). Appliquons le résultat déjà obtenu au polynôme $P = \prod F^\sigma$, où σ décrit le groupe de Galois de $\bar{K}$ sur k modulo le sous-groupe laissant F fixe ; on voit alors, que, pour n assez grand, ξ_n appartient au sous-espace $W = \bigcap \text{Ker}(F^\sigma)$ de V , et l'hypothèse de récurrence montre alors que $\xi_n = 0$ pour n grand, ce qui termine la démonstration.

4. Une remarque sur le passage au groupe adjoint.

THEOREME 3. - Soient G un groupe linéaire algébrique défini sur k et G^* son groupe adjoint. Alors l'application canonique $G_A^O/G_k \rightarrow G_A^*/G_k^*$ est propre.

Supposons d'abord G réductif et connexe. G étant réalisé comme sous-groupe fermé de $GL(V)$ où V est un vectoriel défini sur k , désignons par M l'algèbre associative formée des combinaisons linéaires d'éléments de G , et par Z le groupe multiplicatif des éléments inversibles du centre de M . Evidemment Z est un groupe linéaire algébrique défini sur k , qui commute à G , et l'on peut donc former $H = G.Z$, sous-groupe fermé de $GL(V)$ défini sur k . Il est clair que $G \cap Z$ est le centre de G , i. e. le noyau de la représentation adjointe puisque G est connexe, et par suite on a des isomorphismes canoniques $G^* = G/G \cap Z = H/Z$. Pour montrer que l'application $G_A^O/G_k \rightarrow G_A^*/G_k^*$ est propre il suffit donc, puisque la composée de deux applications propres est propre, de montrer qu'il en est ainsi des applications $G_A^O/G_k \rightarrow H_A^O/H_k$ et $H_A^O/H_k \rightarrow G_A^*/G_k^*$. Pour la première, cela résulte du n° 2.1. Pour la seconde, notons que, G étant réductif, son algèbre enveloppante M est semi-simple, donc aussi le centre de M . Le théorème 90 montre donc que, si k' est une extension galoisienne de k , de groupe de Galois Σ , on a $H^1(\Sigma, Z_{k'}) = 0$. Comme les points rationnels sont denses dans H/Z (on est en caractéristique 0) on déduit de là, par un argument connu [6], que la fibration de H par Z est localement triviale, et par suite que H_A^O/H_k est un fibré principal de base G_A^*/G_k^* et de groupe structural

$Z_A^\wedge/Z_k$ compact vu le théorème 2, d'où la propriété. [N. B. - Ce raisonnement utilise le fait que $Z_A^O = Z_A \cap H_A^O$, lequel provient de ce que les restrictions à Z des caractères rationnels définis sur k de H forment un sous-groupe d'indice fini du groupe des caractères de Z rationnels et définis sur k , résultat valable pour tout groupe réductif.]

Le théorème étant établi pour G réductif connexe, il reste à examiner le cas général. Pour cela, on se ramène au cas réductif en passant au quotient par le radical unipotent (opération inoffensive puisque la fibration par un sous-groupe unipotent est toujours localement triviale), et le cas réductif se ramène au cas réductif connexe en observant que, si H est la composante connexe de G , le quotient G_A/H_A est compact (mais non fini...).

5. Groupes réductifs anisotropes.

Un groupe réductif G défini sur k est dit anisotrope si tout $g \in G_k$ est semi-simple, i. e. si aucun élément de G_k n'est unipotent (la décomposition en semi-simple et unipotent est valable sur k) ; il revient au même d'exiger que tout élément rationnel sur k de l'algèbre dérivée de l'algèbre de Lie de G soit semi-simple, i. e. que la dite algèbre dérivée ne contienne aucun élément rationnel sur k et nilpotent. Ainsi, dire que G est anisotrope revient à dire que le groupe adjoint est anisotrope.

THÉOREME 4 (BOREL-HARISH-CHANDRA). - Soit G un groupe réductif connexe défini sur k . Pour que G_A^O/G_k soit compact, il faut et il suffit que G soit anisotrope

Vu le théorème 3 on peut passer au groupe adjoint, i. e. supposer que G est le groupe des automorphismes d'une algèbre de Lie semi-simple g définie sur k , auquel cas on va prouver que G_A/G_k est compact. D'après le théorème 1 il suffit de montrer que si l'on a des $g_n \in G_A$ et des $\xi_n \in g_k$ tels que $g_n(\xi_n)$ tende vers 0 dans g_A , alors $\xi_n = 0$ pour n grand. Or désignons par P l'un quelconque des coefficients du polynôme caractéristique de $\text{Ad}(X)$, où X est un élément générique de g . Alors P est un polynôme sur g , à coefficients dans k , et invariant par G ; et $P(g_n(\xi_n)) = P(\xi_n)$ tend vers $P(0)$, en sorte que $P(\xi_n) = P(0)$ pour n grand. Autrement dit, l'opérateur $\text{Ad}(\xi_n)$ est nilpotent pour n grand, et comme g_k ne contient pas d'éléments nilpotents non nuls, on en conclut que $\xi_n = 0$, ce qui termine une belle démonstration due à MOSTOW et TAMAGAWA [4].

Quant au fait que G est anisotrope si G_A/G_k est compact, on observe d'abord que la seconde propriété entraîne que, pour tout $\xi \in g_k$, l'orbite $G_A(\xi)$ est

fermé dans G_A ; mais si G n'était pas anisotrope, on pourrait prendre ξ nilpotente et alors il existerait dans G un sous-groupe (fermé et défini sur k) stabilisant la droite engendrée par ξ sans stabiliser le vecteur ξ lui-même (cf. [2], p. 21) ; ainsi, $G_A(\xi)$ contiendrait la "droite" $A^* \cdot \xi$, en sorte que 0 serait adhérent à $G_A(\xi)$, ce qui est absurde.

[Le raisonnement du théorème 4 s'applique directement, i. e. sans passage au groupe adjoint, lorsque G est plongé dans un $GL(V)$ de telle sorte que l'orbite $G(\xi)$ de tout $\xi \in V_k$ soit fermé au sens de la géométrie algébrique. Cette hypothèse permet en effet immédiatement de "séparer" 0 des $\xi \neq 0$ à l'aide des invariants de G à coefficients dans k , et on raisonne alors comme MOSTOW-TAMAGAWA. Il serait intéressant de savoir si tout groupe anisotrope admet une représentation fidèle de ce type, y compris en caractéristique p . D'une manière générale, on n'a pas l'air de savoir grand'chose sur ces questions d'orbites, qui devraient pourtant présenter un grand intérêt à tous points de vue.]

6. Groupes réductifs généraux : racines simples.

Ce paragraphe a pour but d'apporter (sans démonstrations) certains compléments indispensables à un exposé antérieur [3]. Voir [1].

A. - Soit G un groupe réductif connexe défini sur k , et non anisotrope, de sorte que G_k contient des éléments unipotents autres que e . D'après [3], théorème 9, il existe dans G des tores définis et décomposés sur k et non contenus dans le centre de G ; on désignera par T un tore défini et décomposé sur k , et maximal relativement à ces conditions ; T est unique modulo conjugaison par un élément de G_k ([3], corollaire 1 du théorème 6). Soit $\mathfrak{g}$ l'algèbre de Lie de G (on s'excuse de ce recours à la caractéristique $0 \dots$) et, pour tout caractère α de T , soit $\mathfrak{g}(\alpha)$ le sous-espace des $X \in \mathfrak{g}$ tels que $\text{Ad}(t)X = \alpha(t)X$ pour tout $t \in T$; alors chaque $\mathfrak{g}(\alpha)$ est défini sur k , et $\mathfrak{g}$ est somme directe des $\mathfrak{g}(\alpha)$ non nuls. Les α tels que $\mathfrak{g}(\alpha)$ ne soit pas nul sont les racines de G par rapport à T (on inclut le caractère unité parmi les racines), ce sont évidemment les restrictions à T des racines de G par rapport à un tore maximal contenant T .

Soit $r = \dim(T/T \cap Z)$ où Z est le centre de G - on dira que r est le rang de G sur k . Alors il existe r racines linéairement indépendantes $\alpha_1, \dots, \alpha_r$ telles que toute racine de G par rapport à T soit une combinaison linéaire à coefficients entiers tous de même signe des α_i ; une fois choisi un tel système de racines simples, on peut parler de racines "positives"

(et réciproquement, pour construire un système de racines simples on ordonne totalement les racines et on considère les racines positives indécomposables). On désignera par U le sous-groupe de G dont l'algèbre de Lie est la somme des $g(\alpha)$ avec $\alpha > 0$, par $Z(T)$ - c'est évidemment le centralisateur de T - le sous-groupe correspondant à $g(0)$, et par P le sous-groupe engendré par $Z(T)$ et U ; on montre facilement que P est un sous-groupe parabolique minimal de G au sens de [3], que U est son radical unipotent et est un sous-groupe unipotent défini sur k et maximal de G , enfin que P est produit semi-direct de U et de $Z(T)$. Le groupe $Z(T)$ est réductif, a pour centre T , et est anisotrope puisque T , qui en est un sous-tore décomposé maximal, est dans son centre.

B. - Pour tout i tel que $1 \leq i \leq r$, considérons les racines $\alpha = \sum n_j(\alpha) \alpha_j$ pour lesquelles on a $n_i(\alpha) \geq 0$; la somme des $g(\alpha)$ correspondant à ces racines est l'algèbre de Lie d'un sous-groupe $P(i)$ de G , défini sur k et contenant P . On a $P(i) = Z(i) U(i)$ (produit semi-direct sur k) où $Z(i)$ est le groupe réductif engendré par les racines telles que $n_i(\alpha) = 0$, et $U(i) \subset U$ le groupe unipotent engendré par les racines telles que $n_i(\alpha) \geq 1$. Il est clair que $Z(i)$ est de rang $r - 1$: il admet T pour tore décomposé maximal, $P \cap Z(i)$ pour sous-groupe parabolique minimal, et les racines simples de $Z(i)$ relativement à T et $Z(i) \cap P$ sont les α_j ($j \neq i$). Le rôle joué par les $Z(j)$ dans G est joué dans $Z(i)$ par les $Z(i) \cap Z(j)$.

Pour chaque i , on désignera par $V(i)$ un vectoriel défini sur k , par ρ_i une représentation définie sur k de G dans $V(i)$, et par a_i un vecteur rationnel non nul dans $V(i)$, choisis de telle sorte que $P(i)$ soit le stabilisateur de la droite engendrée par a_i ; on a alors $\rho_i(p) a_i = \Delta_i(p) a_i$ où Δ_i est un caractère de $P(i)$ défini sur k ("poids dominant" de ρ_i); on dira que les ρ_i forment un système de représentations fondamentales de G par rapport à P (terminologie non orthodoxe: les représentations fondamentales sont habituellement assujetties à avoir des poids dominants Δ_i aussi bas que possible, condition qu'on n'impose pas ici). Il est clair que, pour tout i , les restrictions des ρ_j ($j \neq i$) à $Z(i)$ forment un système de représentations fondamentales de $Z(i)$ relativement à $Z(i) \cap P$.

Si G est de rang 1 sur k , il y a une seule représentation fondamentale ρ_1 , et il existe deux entiers strictement positifs a et b , ainsi qu'un caractère χ de G , défini sur k , tels que l'on ait sur T la relation

$$\Delta_1(t)^a = \chi(t) \cdot \alpha_1(t)^b \quad ;$$

on en déduit alors que

$$|\Delta_1(t)| = |\alpha_1(t)|^s \quad \text{pour tout } t \in T_A \cap G_A^\circ$$

où s est un nombre rationnel strictement positif.

Enfin, le "théorème de Bruhat" a été étendu par BOREL et TITS au cas étudié ici de la façon suivante : soit $N(T)$ le normalisateur de T dans G et $W(T) = N(T)/Z(T)$, groupe fini évidemment ; alors tout élément de $W(T)$ est représenté par un élément de $N(T)_k$, et G_k est réunion des classes bilatères $U_k \nu P_k$ où ν décrit $N(T)_k$ modulo $Z(T)_k$. Nous n'aurons pas besoin ici de ce résultat.

7. Finitude du nombre de classes.

Les résultats des § 5 et § 6 permettent déjà d'établir en toute généralité le théorème du "nombre de classes fini". Soit G un sous-groupe fermé et défini sur k de $GL(V)$, où V est un vectoriel défini sur k . Choisissons une base de V_k sur k , et pour tout p fini soit K_p le sous-groupe ouvert compact de G_p qui laisse fixe le réseau p -adique engendré par la dite base. Désignant par α le sous-groupe de V_k engendré par celle-ci, on a alors dans le groupe adélique G_A un sous-groupe ouvert

$$W(\alpha) = G_\infty \times \prod_{p \text{ fini}} K_p.$$

Le résultat qu'on a en vue dans ce paragraphe est le suivant :

THÉOREME 5. - L'ensemble $W(\alpha) \backslash G_A / G_k$ est fini.

C'est évident si G_A / G_k est compact (BOREL-LEBESGUE...), en sorte qu'en passant au quotient par le radical unipotent on se ramène immédiatement au cas où G est réductif. Utilisant le § 6, on voit tout d'abord que G_A / P_A est compact, car la fibration de G par P est localement triviale ([3], théorème 7), en sorte que $G_A / P_A \cong (G/P)_A$ est la variété des adèles d'une variété complète et même projective, donc est bien compacte. Puisque $W(\alpha)$ est ouvert, il y a donc un nombre fini d'éléments x_i de G_A tels que

$$G_A = \bigcup W(\alpha) x_i P_A.$$

Désignant par α_1 le réseau transformé de α par x_i , en sorte que $x_i W(\alpha_1) = W(\alpha) x_i$ on est visiblement ramené à montrer que P_A est réunion finie de classes bilatères modulo $W(\alpha_1) \cap P_A$ à gauche et P_k à droite. Mais $W(\alpha_1) \cap P_A$ joue le même rôle pour P_A que $W(\alpha)$ pour G_A , en sorte qu'on est ramené à établir le théorème 5 pour P , i. e. pour P modulo son radical unipotent, i. e. pour un groupe réductif anisotrope, et alors le résultat cherché est une conséquence du théorème 4 et du fait évident que

$$G_A = G_\infty G_A^O \quad .$$

On notera qu'on a en fait démontré que G_A est réunion finie de classes $W(\alpha)xP_k$. On va en déduire le résultat suivant :

THÉOREME 6. - Soient V un espace vectoriel défini sur k , α un réseau dans V_k , G un sous-groupe fermé, connexe et défini sur k de $GL(V)$, et P un sous-groupe parabolique minimal de G . Soit Γ le sous-groupe de G_k qui laisse fixe le réseau α . Alors $\Gamma \backslash G_k / P_k$ est fini.

On a évidemment $\Gamma = G_k \cap W(\alpha)$. Ecrivons $G_A = \bigcup W(\alpha)x_i P_k$ avec des x_i en nombre fini, et en particulier $G_k \subset \bigcup W(\alpha)x_i P_k$; il est clair que G_k est contenu dans la réunion de celles des classes $W(\alpha)x_i P_k$ qui rencontrent effectivement G_k , et pour une telle classe on peut supposer $x_i = \xi_i \in G_k$; il vient alors trivialement $G_k = \bigcup \Gamma \xi_i P_k$, d'où le théorème.

On déduit immédiatement du théorème 6 les résultats suivants :

(i) les sous-groupes paraboliques minimaux de G sont en nombre fini modulo conjugaison par les éléments de Γ ;

(ii) si U est un sous-groupe unipotent de G , défini sur k , et maximal, les sous-groupes $\Gamma \cap \xi U \xi^{-1}$ ($\xi \in G_k$) de Γ sont en nombre fini modulo conjugaison par les éléments de Γ (on notera que les $\xi U \xi^{-1}$ sont les divers sous-groupes unipotents définis sur k et maximaux de G).

8. Inégalités de Minkowski (énoncés).

A partir de maintenant G est un groupe réductif connexe de rang $r \geq 1$ sur k , et on utilise les notations du § 6. On se propose de construire dans G_A des ouverts Ω définis par des inégalités analogues à celles du n° 1.2 et tels que $G_A = \Omega \cdot G_k$, ce qui mettra en évidence notamment le fait que G_A^O / G_k est de volume fini.

Choisissons pour cela une fois pour toutes un compact M dans G_A tel que $G_A = M \cdot P_A$ et un ouvert relativement compact F dans P_A^O tel que $P_A^O = F \cdot P_k$ (ceci est possible en vertu du fait que $P_A^O = Z(T)_A^O \cdot U_A$ et que $Z(T)$ est anisotrope); enfin, pour tout $c > 0$, notons $T_A(c)$ la partie de T_A définie par les inégalités $|\alpha_i(t)| < c$; on posera alors

$$\Omega(c) = M \cdot T_A(c) \cdot F \quad .$$

Le premier résultat qu'on a en vue est le suivant :

THÉOREME 7 (BOREL). - Il existe un $c > 0$ tel que l'on ait $G_A = \Omega(c) \cdot G_k$.

(Ce résultat implique aussitôt que G_A^O/G_K est de volume fini ; en effet reprenons les K_p du § 7 et soit K_∞ un sous-groupe compact maximal de G , en sorte qu'on a $G_\infty = K_\infty P_\infty$ comme on le voit aussitôt ; le théorème 5 montre alors qu'on peut prendre pour M une réunion d'un nombre fini de classes Kx où K est le produit des K_p pour p fini ou non ; on est donc ramené à faire voir que $KxT_A(c) \cap G_A^{Op}$ est de mesure finie ; or sur la classe ouverte KxP_A la mesure de Haar de G_A est, à un facteur près, le produit de celle de K par la mesure invariante à droite de P_A , et celle-ci est le produit des mesures invariantes de $Z(T)_A$, de U_A et d'un facteur qui est le déterminant de la représentation adjointe (adélique!) de $Z(T)_A$ dans l'algèbre de Lie de U_A , déterminant qui est un monôme à exposants entiers strictement positifs en les racines simples α_i ; la finitude du volume résulte aussitôt de là.)

La "réduction" indiquée par le théorème 7 s'obtient en outre par une méthode analogue à celle du n° 1.2. Considérons les représentations ρ_i du § 6, et choisissons sur chaque $V(i)$ une hauteur (n° 1.1). Pour tout $c > 0$, notons $R(c)$ l'ensemble des $g \in G_A$ qui vérifient les conditions suivantes :

$$\begin{aligned} \|\rho_1(g)a_1\| &\leq c\|\rho_1(g\gamma)a_1\| \quad \text{pour tout } \gamma \in G_K \\ \|\rho_2(g)a_2\| &\leq c\|\rho_2(g\gamma)a_2\| \quad \text{pour tout } \gamma \in P(1)_K \\ \|\rho_3(g)a_3\| &\leq c\|\rho_3(g\gamma)a_3\| \quad \text{pour tout } \gamma \in P(1)_K \cap P(2)_K \end{aligned}$$

et ainsi de suite (les γ qu'on autorise dans chaque inégalité sont évidemment ceux qui ne détruisent pas les inégalités précédentes...). D'après le n° 1.1, (iv), on a évidemment $G_A = R(1) \cdot G_K$; ceci dit, on va établir aussi le résultat suivant (qui implique le théorème 7 trivialement, comme on vient de le voir - mais on ne pourra pas démontrer directement le théorème 8 sans passer d'abord par une démonstration, au moins partielle, du théorème 7) :

THÉOREME 8. - Pour tout $c > 0$, il existe un $c' > 0$ tel que l'on ait
 $R(c) \subset R(c') \cdot P_K$ (il est évident que $R(c)$ est invariant à droite par P_K).

9. Démonstrations des théorèmes 7 et 8.

9.1. - Démonstration du théorème 7 (rang 1).

On suppose G de rang 1 dans ce numéro. Tenant compte du fait qu'on a

$$P_A = T_A P_A^O ; \quad T_A \cap P_A^O = T_A^O ,$$

(se ramener à $Z(T)$ et observer que les caractères de $Z(T)$ définis sur k sont déterminés, à un nombre fini d'ambiguïtés près, par leurs restrictions au tore décomposé maximal T), on voit qu'il existe sur G_A une fonction $d(g)$ continue, strictement positive, et vérifiant

$$d(gtp) = d(g) |\alpha_1(t)| \quad \text{pour } t \in T_A \text{ et } p \in P_A^O.$$

Considérant le compact M tel que $G_A = M \cdot P_A$ choisi pour définir les $\Omega(c)$, il est clair que $d(M)$ est un compact dans $\mathbb{R}_+^*$ et par suite que, pour $g = mtp$ ($m \in M$, $t \in T_A$ et $p \in P_A^O = F \cdot P_k$) les nombres $d(g)$ et $|\alpha_1(t)|$ sont "équivalents". Par conséquent le théorème 7 équivaut à la relation

$$\sup_{g \in G_A} \inf_{\gamma \in G_k} d(g\gamma) < +\infty ;$$

il suffit du reste évidemment, dans ce qui précède, de faire varier g dans l'ensemble E des g tels que l'on ait $d(g\gamma) \geq 1$ pour tout $\gamma \in G_k$, et le résultat cherché va non moins évidemment résulter du fait que $E \cap G_A^O = E^O$ est compact modulo G_k .

Il reste à établir ce dernier point, et pour cela on peut remplacer E^O par son image dans le groupe adjoint (théorème 3) ; donc (théorème 1) il reste à montrer que si des $g_n \in E^O$ et des ξ_n rationnels dans l'algèbre de Lie $\mathfrak{g}$ de G sont tels que $\text{Ad}(g_n)\xi_n$ tende vers 0 dans $\mathfrak{g}_A$, alors $\xi_n = 0$ pour n grand. On voit d'abord, en raisonnant comme dans la démonstration du théorème 4, que l'on a $P(\xi_n) = P(0)$ pour tout invariant P de la représentation adjointe, en particulier pour les coefficients du polynôme caractéristique de $\text{Ad}(?)$; donc les $\text{Ad}(\xi_n)$ sont nilpotents pour n grand ; écrivant g comme somme directe de son centre et de l'algèbre dérivée $\mathfrak{g}'$, et remarquant que la composante centrale de ξ_n est nulle (car $\text{Ad}(g_n)$ opère trivialement sur le centre de $\mathfrak{g}$) on voit qu'on a en outre $\xi_n \in \mathfrak{g}'_k$ pour n grand ; donc les ξ_n engendrent dans G des sous-groupes unipotents à un paramètre définis sur k , donc transformables par G_k en sous-groupes de U , et on voit donc qu'au besoin en remplaçant g_n par $g_n \gamma_n$ avec des $\gamma_n \in G_k$ on peut supposer les ξ_n dans l'algèbre de Lie de U , i. e. écrire

$$\xi_n = \xi'_n + \xi''_n \quad \text{avec } \xi'_n \in \mathfrak{g}(\alpha_1) \text{ et } \xi''_n \in \mathfrak{g}(2\alpha_1).$$

Ecrivons maintenant $g_n = k_n t_n z_n u_n$ où les k_n restent dans un compact fixe, et où $t_n \in T_A$, $z_n \in Z(T)_A^O$, $u_n \in U_A$; comme les k_n restent dans un compact, les $\text{Ad}(t_n z_n u_n)\xi_n$ tendent vers 0 ; mais il est clair, en vertu de la relation $[g(\lambda), g(\mu)] \subset g(\lambda + \mu)$, que l'on a

$$\text{Ad}(t_n z_n u_n) \xi_n \equiv \alpha_1(t_n) \text{Ad}(z_n) \xi'_n \pmod{g(2\alpha_1)},$$

en sorte que $\alpha_1(t_n) \text{Ad}(z_n) \xi'_n$ tend vers 0 ; comme par hypothèse $\alpha_1(t_n)$ reste supérieur à 1 , on voit que $\text{Ad}(z_n) \xi'_n$ tend vers 0 , mais comme $\hat{Z}(T)$ est anisotrope le théorème 4 montre qu'on peut supposer que les z_n restent dans un compact fixe - et alors ξ'_n tend vers 0 , donc est nul pour n grand. Ceci fait, il reste à tuer la seconde composante ξ''_n , ce qu'on fait en observant que

$$\text{Ad}(t_n z_n u_n) \xi''_n = \alpha_1(t_n)^2 \text{Ad}(z_n) \xi''_n$$

et en raisonnant comme ci-dessus.

9.2. - Démonstration du théorème 8 (rang 1).

On suppose toujours G de rang 1 , et on pose $d'(g) = \|\rho_1(g) a_1\|$. Comme on l'a vu au § 6, il existe des entiers positifs r et s et un caractère χ de G , défini sur k , tels que l'on ait

$$\Delta_1(t)^r = \chi(t) \cdot \alpha_1(t)^s ;$$

la fonction $d'(g)^r / |\chi(g)| \cdot d(g)^s$ est donc invariante à droite par P_A , et comme G_A/P_A est compact on en déduit qu'il existe des constantes c' , $c'' > 0$ telles que l'on ait

$$c' |\chi(g)| \cdot d(g)^s \leq d'(g)^r \leq c'' |\chi(g)| \cdot d(g)^s$$

pour tout $g \in G_A$. Supposons alors $g \in \mathcal{R}(c)$, i. e. $d'(g) \leq c \cdot d'(gy)$ pour tout y ; on a alors évidemment

$$c' |\chi(g)| d(g)^s \leq \inf_Y |\chi(gY)| d(gY)^s ;$$

or on a $|\chi(gY)| = |\chi(g) \chi(Y)| = |\chi(g)|$ vu la formule du produit, et d'autre part le théorème 7, déjà établi, montre que $\inf d(gY)$ est inférieur à une constante fixe ; on en déduit aussitôt que la fonction $d(g)$ est bornée supérieurement sur $\mathcal{R}(c)$, ce qui établit évidemment le théorème 8.

9.3. - Démonstration des théorèmes 7 et 8 (cas général).

Comme le théorème 7 résulte évidemment du théorème 8, on va se borner à établir celui-ci, en raisonnant par récurrence sur le rang r de G .

Considérons le compact M du § 8, tel que $G_A = M \cdot P_A$, et pour tout $g \in \mathcal{R}(c)$ écrivons $g = mp$ avec $m \in M$ et $p \in P_A$; d'après la propriété (v) du n° 1.1 les rapports $\|\rho_1(gy)a_1\|/\|\rho_1(py)a_1\|$ restent dans un compact fixe de $\mathbb{R}_+^*$, et par suite il y a un c' tel que $p \in \mathcal{R}(c')$. Posant $p = tp'$ avec $t \in T_A$ et $p' \in P_A^0 = \mathbb{R}P_K$ on voit donc qu'il reste à prouver l'existence d'un c'' tel que l'on ait $|\alpha_i(t)| < c''$ pour tout i .

Considérons le sous-groupe réductif $Z(1)$ de rang $r - 1$ défini au § 6, et posons $p = zu$ avec $z \in Z(1)_A$ et $u \in U(1)_A$; l'hypothèse que $p \in \mathcal{R}(c)$ implique, puisque $U(1)$ est invariant par $Z(1)$ et laisse fixes les a_i , les inégalités

$$\|\rho_2(z)a_2\| \leq c\|\rho_2(z\zeta)a_2\| \quad \text{pour tout } \zeta \in Z(1)_k$$

$$\|\rho_3(z)a_3\| \leq c\|\rho_3(z\zeta)a_3\| \quad \text{pour tout } \zeta \in Z(1)_k \cap P(2)_k$$

etc., et par suite z reste dans un $\mathcal{R}(c)$ du sous-groupe $Z(1)$; l'hypothèse de récurrence montre alors que les $|\alpha_i(t)|$ restent bornés supérieurement pour $i \geq 2$.

Il reste à majorer $|\alpha_1(t)|$. Pour cela, on utilise dans G le sous-groupe H (réductif de rang 1) engendré par les racines proportionnelles à α_1 , et le sous-groupe unipotent V engendré par les $\alpha > 0$ non proportionnelles à α_1 ; il est clair que H normalise V , contient $Z(T)$, et que P est produit semi-direct de V et du sous-groupe parabolique minimal $H \cap P$ de H ; enfin, ρ_1 est évidemment une représentation fondamentale de H . Cela dit, si l'on écrit $p = thv$ avec $v \in V_A$ et $h \in (H \cap P)_A^0$, l'hypothèse que $p \in \mathcal{R}(c)$ implique une majoration de la forme

$$\|\rho_1(th)a_1\| \leq c\|\rho_1(th\gamma)a_1\| \quad \text{pour tout } \gamma \in H_k;$$

comme H est de rang 1, on en conclut que $|\alpha_1(t)| \leq c'$, et ceci achève la démonstration.

10. Construction d'ouverts fondamentaux.

Le théorème 7 montre que, pour c assez grand, G_A est réunion des ouverts $\Omega(c)\gamma$ lorsque γ décrit G_k ; on se propose maintenant de construire dans G_A des ouverts fondamentaux pour G_k , i. e. des ouverts $\mathcal{G}$ tels que l'on ait

$$G_A = \mathcal{G} \cdot G_k,$$

et tels que, de plus, les $\gamma \in G_k$ pour lesquels l'intersedtion $\mathcal{G}\gamma \cap \mathcal{G}$ n'est pas vide soient en nombre fini, propriété qui n'est généralement pas vérifiée par les $\Omega(c)$ du § 8.

Pour cela, nous appellerons ouvert de Siegel dans G_A tout ouvert

$$\mathcal{G} = M \cdot T_\infty^+(c) \cdot F$$

construit comme suit : $T_{\infty}^{+}(c)$ est l'ensemble des $t \in T_{\infty}^{+}$ (composante connexe de l'unité dans le groupe de Lie T_{∞}) tels que l'on ait $\alpha_i(t) < c$ pour $1 \leq i \leq r$; F est un ouvert relativement compact dans P_A^0 , tel que l'on ait $P_A^0 = F \cdot P_k$; enfin, M est un compact tel que $G_A = M \cdot P_A$, et choisi de telle sorte que l'image M_{∞} de M par l'application canonique de G_A sur G_{∞} soit un sous-groupe compact maximal de G_{∞} adapté à T_{∞} (i. e. tel que les algèbres de Lie de M_{∞} et T_{∞} soient orthogonales relativement à la forme de Killing de $\mathfrak{g}$, ou encore tel que la symétrie par rapport à M_{∞} se réduise à $t \rightarrow t^{-1}$ sur T_{∞}). L'existence d'un compact M vérifiant ces conditions est à peu près évidente si l'on tient compte d'une part de la compacité de G_A/F_A et, d'autre part, du fait que pour tout sous-groupe compact maximal M_{∞} de G_{∞} on a $G_{\infty} = M_{\infty} P_{\infty}$ en vertu des théorèmes classiques d'Iwasawa.

L'hypothèse faite sur M_{∞} n'interviendra que dans les dernières lignes de la démonstration (et en particulier n'intervient pas dans les lemmes 1 à 4 ci-dessous).

Si l'on compare l'ouvert $\mathcal{G}$ précédent avec l'ouvert $\Omega(c) = M \cdot T_A(c) \cdot F$, on remarque tout d'abord que l'on a

$$T_A(c) = T_{\infty}^{+}(c) T_A^0 \subset T_{\infty}^{+}(c) P_A^0 = T_{\infty}^{+}(c) F P_k,$$

et par suite il vient $\Omega(c) \subset \mathcal{G} \cdot P_k$; le théorème 7 montre donc que l'on a

$$G_A = \mathcal{G} G_k$$

pour peu que c soit suffisamment grand. Pour exhiber des ouverts fondamentaux, il reste donc à établir le résultat que voici :

THÉORÈME 9 (BOREL). - Soient $\mathcal{G}'$ et $\mathcal{G}''$ deux ouverts de Siegel dans G_A ; alors l'ensemble des $\gamma \in G_k$ tels que $\mathcal{G}'\gamma$ rencontre $\mathcal{G}''$ est fini.

La démonstration consiste à examiner d'abord tous les triplets (g', g'', γ) tels que l'on ait

$$g' \in \mathcal{G}', \quad g'' \in \mathcal{G}'', \quad \gamma \in G_k \text{ et } g'\gamma = g''$$

et pour lesquels γ appartient à une classe bilatère donnée modulo P_k , autrement dit (théorème de Bruhat-Borel-Tits) pour lesquels

$$\gamma = \pi' w \pi''$$

avec $w \in N(T)_k$ donné, $\pi', \pi'' \in P_k$ variables.

On posera dans ce qui suit

$$g' = m' t' p', \quad g'' = m'' t'' p''$$

avec $m', m'' \in M$, $t', t'' \in T_{\infty}^+(c)$, et $p', p'' \in F$.

LEMME 1. - Pour tout $c > 0$ et tout compact F de P_A l'ensemble des tpt^{-1} ($t \in T_{\infty}^+(c)$, $p \in F$) est relativement compact dans P_A .

Puisque p et tpt^{-1} sont évidemment égaux en toute place finie, il suffit de se placer dans G_{∞} . Alors $p = zu$ où z reste dans un compact de $Z(T)_{\infty}$ et u dans un compact de U_{∞} , et comme $tpt^{-1} = z.tut^{-1}$ il suffit d'examiner tut^{-1} . Posant $u = \exp(X)$, où X appartient à la somme directe des $g(\alpha)_{\infty}$ pour toutes les racines $\alpha > 0$, tout revient évidemment à montrer que lorsque X reste dans un compact fixe, il en est de même de $\text{Ad}(t) X$. Pour cela, on se ramène au cas où $X \in g(\alpha)_{\infty}$, et alors $\text{Ad}(t) X = \alpha(t) X$; mais $\alpha(t)$ est un monôme à exposants entiers positifs en les $\alpha_i(t)$, donc reste borné sur $T^+(c)$, d'où le lemme.

LEMME 2. - L'élément $w^{-1} t'wt''^{-1}$ reste dans un compact fixe de T_{∞}^+ .

La relation $g'\gamma = g''$ s'écrit en effet

$$m't'p't'^{-1}.t'\gamma = m''t''p''t''^{-1}.t''$$

et montre, compte-tenu du lemme 1, que

$$t'\gamma t''^{-1} = t'\pi'w\pi''t''^{-1}$$

reste dans un compact fixe.

Considérons alors un vectoriel V défini sur k , une représentation linéaire ρ de G dans V , définie sur k , et un vecteur non nul $a \in V_k$ tels que l'on ait

$$\rho(p)a = \Delta(p).a$$

où Δ est un caractère de P , défini sur k . Choissant une hauteur sur V_A , la propriété (vi) du n° 1.1 montre que l'on a (*)

$$\|\rho(t'\pi'w\pi''t''^{-1})a\| \asymp 1,$$

ce qui s'écrit encore, puisque $|\Delta(\pi'')| = 1$, sous la forme

$$\Delta(t''^{-1}) \|\rho(t'\pi'w)a\| \asymp 1;$$

écrivant $t'\pi'w = t'\pi't'^{-1}.w.w^{-1}t'w$, il vient donc

$$\Delta(t''^{-1}) \Delta(w^{-1}t'w) \|\rho(t'\pi't'^{-1})\rho(w)a\| \asymp 1$$

(*) La relation $x \asymp y$ signifie que le rapport x/y reste dans un compact de $\mathbb{R}_{>0}^*$, et la relation $x < y$ qu'il reste borné supérieurement.

i. e.

$$(1) \quad \Delta(w^{-1} t' w t''^{-1}) \|\rho(t' \pi' t'^{-1}) \rho(w) a\| \asymp 1 \quad .$$

Or $t' \pi' t'^{-1}$ reste dans $P_A^0 = F.P_k$ avec F relativement compact; en appliquant à nouveau la propriété (vi) du n° 1.1 et en tenant compte du fait que les hauteurs des éléments rationnels non nuls de V restent au large de 0 (propriété (iv) du n° 1.1) on voit que $\|\rho(t' \pi' t'^{-1}) \rho(w) a\| > 1$, et par suite (1) conduit à la relation

$$(2) \quad \Delta(w^{-1} t' w t''^{-1}) < 1 \quad .$$

On va montrer qu'en fait on a aussi l'évaluation opposée

$$(3) \quad \Delta(w^{-1} t' w t''^{-1}) > 1 \quad ,$$

autrement dit, en vertu de (1), que l'on a aussi

$$(4) \quad \|\rho(t' \pi' t'^{-1}) \rho(w) a\| < 1 \quad .$$

En effet, il est tout d'abord clair que le vecteur $\xi = \rho(w) a$ appartient au poids $\Delta(w^{-1} t' w)$, en sorte que (4) équivaut à la relation

$$\Delta(w^{-1} t' w)^{-1} \|\rho(t' \pi') \xi\| < 1 \quad ;$$

mais puisque $\pi' \in P_k$, et comme P est engendré par les racines $\alpha \geq 0$, il est clair qu'on a une relation de la forme

$$\rho(\pi') \xi = \sum \xi_\lambda$$

où

$$\rho(t') \xi_\lambda = \Delta(w^{-1} t' w) \lambda(t') \xi_\lambda$$

et où chaque λ est un monôme à exposants entiers positifs en les α_1 ; la relation (3) ou (4) à établir s'écrit donc

$$\|\sum \lambda(t') \xi_\lambda\| < 1 \quad ,$$

et résulte facilement du fait que, comme t' reste dans $T^+(c')$, les $\lambda(t')$ restent bornés supérieurement.

Ceci fait, on voit donc en comparant (2) et (3) qu'on a $\Delta(w^{-1} t' w t''^{-1}) \asymp 1$ toutes les fois que Δ est un "poids dominant" de G par rapport à P ; or on sait que les restrictions à T de ces poids dominants engendrent un sous-groupe d'indice fini du groupe de tous les caractères rationnels de T ; il s'ensuit aussitôt qu'on a

$$\chi(w^{-1} t' w t''^{-1}) \asymp 1$$

pour tout caractère rationnel χ de T , et ceci démontre évidemment le lemme 2.

LEMME 3. - Pour tout j tel que $1 \leq j \leq r$, on a soit $\alpha_j(t') > 1$, soit $w \in P(j)$.

Comme le groupe de Weyl permute les racines, on a en effet pour tout i une relation de la forme

$$\alpha_i(w^{-1} t' w) = \prod \alpha_j(t')^{n_{ij}(w)}$$

avec des entiers $n_{ij}(w)$ tous positifs ou tous négatifs. Or on a les relations

$$\alpha_j(t') < 1, \quad \alpha_i(w^{-1} t' w) < 1$$

(la première parce que t' reste dans $T_\infty^+(c')$, la seconde en vertu du lemme 2 et du fait que t'' reste dans $T^+(c'')$); il est donc clair que, si $\alpha_j(t')$ ne reste pas au large de zéro, on a $n_{ij}(w) \geq 0$ pour tout i , ce qui veut dire que la transformée de la racine α_i est dans $P(j)$ pour tout i , ou encore que $wUw^{-1} \subset P(j)$; mais alors wUw^{-1} est un sous-groupe unipotent défini sur k et maximal de $P(j)$, donc conjugué de U par un élément rationnel de $P(j)$, et par suite

$$w \in P(j)_k N(U)_k = P(j)_k P_k = P(j)_k, \quad ,$$

ce qui achève la démonstration.

LEMME 4. - Supposons que w n'appartienne à aucun sous-groupe parabolique Q de G tel que $P \subset Q$ et $Q \neq G$. Alors les $\gamma \in P_k w P_k$, tels que $\mathcal{G}'\gamma$ rencontre $\mathcal{G}''$, sont en nombre fini.

En effet le lemme 3 montre qu'alors $\alpha_j(t') > 1$ pour tout j , donc que

$$\alpha_j(t') \asymp 1$$

pour tout j , ce qui veut dire que $t'' = t'_1 z'$ où t'_1 reste dans un compact et où $z' \in T_\infty \cap Z_\infty$ (où Z est le centre de G); le lemme 2 montre alors que $t'' = t''_1 z'$ avec t''_1 dans un compact fixe. La relation $g'\gamma = g''$ s'écrit alors

$$m' t'_1 z' p' \gamma = m'' t''_1 z' p''$$

i. e. $m' t'_1 p' \gamma = m'' t''_1 p''$ puisque z' est dans le centre de G_A , et on voit que γ reste dans un compact fixe, d'où le lemme.

Le lemme 4 montre que, parmi les $\gamma \in G_k$, tels que $\mathcal{G}'\gamma$ rencontre $\mathcal{G}''$, ceux qui n'appartiennent à aucun sous-groupe parabolique Q contenant P et distinct de G sont en nombre fini. Pour achever la démonstration, il reste donc à faire

voir que, pour tout sous-groupe parabolique Q contenant P , les $\gamma \in Q_k$ tels que $\delta'\gamma$ rencontre δ'' , et qui n'appartiennent à aucun sous-groupe parabolique contenant P et strictement contenu dans Q , sont en nombre fini.

Or Q est produit semi-direct d'un groupe réductif $H \supset Z(T)$ et de son radical unipotent $V \subset U$. Désignant d'une manière générale par q_H et q_V les composantes d'un $q \in Q_A$ dans la décomposition $Q_A = H_A V_A$, la relation $g'\gamma = g''$, i. e. $m't'p'\gamma = m''t''p''$ ou encore

$$m''^{-1} m't'p'\gamma = t''p''$$

implique $m''^{-1} m' \in Q_A \cap M^{-1}.M$ et se décompose en les relations

$$(5) \quad (m''^{-1} m')_H t'p'_H \gamma_H = t''p''_H$$

$$(6) \quad \gamma_H^{-1} p_H'^{-1} t'^{-1} (m''^{-1} m')_V t'p'\gamma = p'' \quad ;$$

pour montrer que les γ en question sont en nombre fini, il suffit donc de faire voir d'une part que les composantes γ_H possibles sont en nombre fini, et d'autre part que $t'^{-1} (m''^{-1} m')_V t'$ reste dans un compact fixe.

Pour établir le premier point, distinguons deux cas. Si $H = Z(T)$, i. e. si $Q = P$, le lemme 2 s'applique avec $w = e$ et montre que $t'^{-1} t''$ reste dans un compact fixe ; mais comme t' commute à $(m''^{-1} m')_H$ puisqu'on suppose $H = Z(T)$, la relation (5) s'écrit $(m''^{-1} m')_H p_H' \gamma_H = t'^{-1} t'' p_H''$, et montre que γ_H reste dans un compact fixe, d'où le résultat. Si maintenant $H \neq Z(T)$, le lemme 4 s'applique à H (relativement à T et $H \cap P$), et pour en déduire que γ_H ne peut prendre qu'un nombre fini de valeurs il suffit, puisqu'on est dans une situation telle que γ_H n'appartient à aucun sous-groupe parabolique de H contenant $P \cap H$ et distinct de H , de montrer que $(m''^{-1} m')_H t'p'_H$ et $t''p''_H$ restent dans une partie de H_A qui est le produit d'un compact par l'ensemble des $t \in T_\infty^+$ où les racines simples de H par rapport à T et $P \cap H$ sont inférieures à un nombre fixe et par un compact de $(H \cap P)_A^0 = H_A \cap P_A^0$; ce qui est clair puisque les racines simples de H sont évidemment certaines des α_i . On a ainsi établi que γ_H ne peut prendre qu'un nombre fini de valeurs (et sans avoir eu besoin de l'hypothèse faite sur M_∞ au début de ce paragraphe ; mais elle va servir maintenant).

Il reste en effet à vérifier que $t'^{-1} (m''^{-1} m')_V t''$ reste dans un ensemble compact, ce qu'on va faire en montrant beaucoup plus, à savoir que

$$t'^{-1} (m''^{-1} m')_V t' = (m''^{-1} m')_V \quad .$$

Comme t' est égal à 1 en toute place finie, il suffit pour cela de faire voir que $(m_{\infty}^{-1} m'_{\infty})_V = 1$, autrement dit que

$$M_{\infty}^{-1} \cdot M_{\infty} \cap Q_{\infty} \subset H_{\infty} \quad ;$$

mais cela résulte précisément de l'hypothèse que M_{∞} est un sous-groupe compact maximal de G_{∞} adapté à T . En effet, la symétrie par rapport à M_{∞} transforme chaque $t \in T_{\infty}^+$ en t^{-1} , donc chaque racine α en son opposée $-\alpha$, et par suite applique Q_{∞} sur le sous-groupe "symétrique" Q'_{∞} engendré par les opposées des racines appartenant à Q_{∞} ; donc $M_{\infty}^{-1} \cdot M_{\infty} \cap Q_{\infty} = M_{\infty} \cap Q'_{\infty}$ est contenu dans

$$Q_{\infty} \cap Q'_{\infty} = H_{\infty} \quad ,$$

et ceci termine la démonstration.

11. Points rationnels dans les orbites fermées.

On va montrer comment le théorème 7 permet de retrouver le résultat suivant :

THÉORÈME 10 (BOREL-HARISH-CHANDRA). - Soient V un espace vectoriel défini sur k , G un sous-groupe algébrique réductif et défini sur k de $GL(V)$, et ξ un point de V_k dont l'orbite $G(\xi)$ soit fermée (en tant que variété algébrique dans V). Alors les points de $G_A(\xi) \cap V_k$ sont en nombre fini modulo G_k .

(La démonstration qui suit est directement inspirée de [2], p. 504-505 ; on négligera, dans cette démonstration, les difficultés dues à la géométrie algébrique, pour ne retenir que l'aspect arithmétique du problème.)

On se ramène tout d'abord au cas où G est connexe, et on choisit alors T, P, M et G comme au début du n° 10. Désignant par H le stabilisateur de ξ dans G , l'orbite $G(\xi)$ est isomorphe à G/H comme variété algébrique sur k , donc G/H est affine, et l'on en déduit que H est réductif ([2], p. 499) ; pour cette raison, H_{∞} est stable par l'involution de G_{∞} par rapport à un conjugué convenable de M_{∞} , autrement dit il y a un $x \in G_{\infty}$ tel que l'on ait

$$(7) \quad \theta(x H_{\infty} x^{-1}) = x H_{\infty} x^{-1}$$

où θ désigne l'involution de G_{∞} par rapport à M_{∞} . Comme du reste M_{∞} est adapté à T on a aussi

$$(8) \quad \theta(t) = t^{-1}$$

pour $t \in T_{\infty}^+$.

Cela dit, et observant que, si G est bien choisi, on a

$$G_A = \mathcal{G}G_k = G_k \mathcal{G}^{-1} = G_k \mathcal{G}^{-1} x \quad ,$$

il suffit, pour établir le théorème, de montrer que l'ensemble

$$\mathcal{G}^{-1} x(\xi) \cap V_k$$

est fini, ce qu'on va faire.

Soit donc $g = mtp \in \mathcal{G}$ tel que $g^{-1} x(\xi) \in V_k$; on a

$$g^{-1} x(\xi) = \sum_{\lambda} \xi_{\lambda}(g)$$

où $\xi_{\lambda}(g)$ est un vecteur rationnel appartenant au poids λ de G par rapport à T , donc tel que

$$tg^{-1} x(\xi) = \sum \lambda(t) \xi_{\lambda}(g) \quad .$$

Or $tg^{-1} = tp^{-1} t^{-1} m^{-1}$ reste dans un compact fixe d'après le lemme 1 du § 10 ; il en est donc de même de $\sum \lambda(t) \xi_{\lambda}(g)$ et comme $\xi_{\lambda}(g)$, étant rationnel, est nul ou bien de hauteur supérieur à un $c > 0$ fixe, on déduit de là que, pour $\xi_{\lambda}(g) \neq 0$, on a à la fois

$$\|\lambda(t) \xi_{\lambda}(g)\| < 1 \quad \text{et} \quad |\lambda(t)| < 1 \quad ;$$

comme $t^2 g^{-1} x(\xi) = \sum \lambda(t)^2 \xi_{\lambda}(g)$, il s'ensuit que

$$\|t^2 g^{-1} x(\xi)\| < 1 \quad .$$

Mais puisque $t \in T_{\infty}^+$, la partie finie de $t^2 g^{-1}$ reste dans un compact fixe, et on voit donc que la composante à l'infini de $t^2 g^{-1} x(\xi)$ reste dans l'intersection d'un compact fixe de V_{∞} avec $G_{\infty}(\xi)$. Mais comme $G(\xi)$ est fermée dans V au point de vue de la géométrie algébrique, il est clair que $G(\xi)_{\infty}$ est une sous-variété fermée de V_{∞} au point de vue de la géométrie analytique réelle ; de plus, pour tout $x \in G(\xi)_{\infty}$, l'application $g \rightarrow g(x)$, qui est une submersion $G \rightarrow G(\xi)$ au point de vue de la géométrie algébrique, est une submersion $G_{\infty} \rightarrow G(\xi)_{\infty}$ au point de vue de la géométrie analytique réelle, en sorte que chaque orbite $G_{\infty}(x)$ est ouverte et donc fermée dans $G(\xi)_{\infty}$; ainsi, $G_{\infty}(\xi)$ est une sous-variété fermée de V_{∞} , évidemment isomorphe à G_{∞}/H_{∞} , et comme la composante à l'infini de $t^2 g^{-1} x(\xi)$ reste dans une partie compacte de V_{∞} , donc de $G_{\infty}(\xi) \cong G_{\infty}/H_{\infty}$, on voit que la composante à l'infini de $t^2 g^{-1} x$ reste dans le produit de H_{∞} par un compact fixe de G_{∞} , et finalement que $t^2 g^{-1} x \in C.H_A$ où C est un compact fixe dans G_A . Mais on a $t^2 g^{-1} = t^2 p^{-1} t^{-2}.tm^{-1}$, et en utilisant à nouveau le lemme 1 du § 10, on voit que $tm^{-1} x \in C'.H_A$ où C' est compact, donc que $tm^{-1} \in C''.xH_A x^{-1}$; utilisant (7) et (8) et appliquant θ on voit que $t^{-1} m^{-1} \in C'''.xH_A x^{-1}$, et comme

$$g^{-1} x(\xi) = p^{-1} t^{-1} m^{-1} x(\xi) \in C^{\infty} H_A(\xi) = C^{\infty}(\xi)$$

on voit que $g^{-1} x(\xi)$ reste dans l'intersection de V_k et d'un compact fixe de V_A , i. e. dans un ensemble fini fixe, ce qui termine la démonstration.

(Pour compléter le théorème 10 et en faire un énoncé du type Hasse-Minkowski, il faut encore montrer - ce qui est facile mais non évident - que les éléments de $G_A(\xi) \cap V_k$ sont les $\eta \in G(\xi)_k$ qui sont "localement équivalents" à ξ , i. e. qui vérifient $\eta \in G_p(\xi)$ pour tout p fini ou non).

12. Traductions à l'infini.

Les théorèmes 7, 9 et 10 peuvent facilement se remplacer par des énoncés ne faisant intervenir que la situation à l'infini, et ce sont du reste de tels énoncés qu'on trouve dans [1] et [2].

Supposons $G \subset GL(V)$ où V est un vectoriel défini sur k , et choisissons un sous-groupe compact maximal M_{∞} de G_{∞} adapté au tore T , en sorte qu'on a, d'après Mostow-Iwasawa, la relation $G_{\infty} = M_{\infty} P_{\infty}^{+}$ (où P_{∞}^{+} est la composante connexe de P_{∞}). Il est clair d'autre part que $P_{\infty}^{+} = T_{\infty}^{+} P_{\infty}^0$, où l'on désigne par P_{∞}^0 le sous-groupe des $p \in P_{\infty}^{+}$ pour lesquels on a $\chi(p) = 1$ pour tout caractère χ rationnel et défini sur k de P (en notant $Z'(T)$ le groupe dérivé, semi-simple, de $Z(T)$, il est clair que $P_{\infty}^0 = Z'(T)_{\infty} U_{\infty}$). On appellera alors ouvert de Siegel dans G_{∞} tout ensemble de la forme

$$G = M_{\infty} T_{\infty}^{+}(c) D$$

où D est un ouvert relativement compact dans P_{∞}^0 .

Choisissons d'autre part pour chaque p fini un sous-groupe ouvert compact M_p de G_p , de telle sorte bien entendu que, pour presque tout p , M_p soit le sous-groupe des points de G_p qui conservent un réseau rationnel donné, et soit Γ le sous-groupe des $\gamma \in G_k$ tels que l'on ait $\gamma_p \in M_p$ pour tout p fini (en sorte que Γ est un sous-groupe discret "arithmétiquement défini" de G_{∞}); il est clair (théorème 6) que $P_k \backslash G_k / \Gamma$ est fini. Cela dit :

THÉORÈME 11 (BOREL). - Soit (ξ_{ν}) une famille finie d'éléments de G_k . Les propriétés suivantes sont équivalentes :

- il existe un ouvert de Siegel G dans G_{∞} tel que $G_{\infty} = \cup G \xi_{\nu} \Gamma$
- on a $G_k = \cup P_k \xi_{\nu} \Gamma$.

(Il faudrait naturellement ajouter, pour être complet, que si (a) est vérifié alors $\Omega = \bigcup \mathcal{G}_{\nu}^{\xi}$ est un ouvert fondamental pour Γ dans G_{∞} , i. e., Ω ne rencontre qu'un nombre fini de $\Omega\gamma$ - mais ce genre d'assertion résulte aussitôt du théorème 9 établi plus haut.)

Supposons d'abord $G_K = \bigcup P_K \xi_{\nu} \Gamma$, et choisissons dans G_A un ouvert de Siegel $\mathcal{G}_A$ tel que $G_A = \mathcal{G}_A G_K$; l'image $\mathcal{G}$ de $\mathcal{G}_A$ par la projection $G_A \rightarrow G_{\infty}$ est évidemment un ouvert de Siegel dans G_{∞} . On a

$$G_A = \bigcup \mathcal{G}_A P_K \xi_{\nu} \Gamma$$

et par suite tout $g \in G_{\infty}$ peut s'écrire $g = s\pi\xi_{\nu}\gamma$ avec un $s \in \mathcal{G}_A$, un $\pi \in P_K$, un $\gamma \in \Gamma$ et un ν convenablement choisis; si l'on désigne d'une manière générale, pour tout $x \in G_A$, par x_f l'élément de G_A déduit de x en remplaçant la composante x_{∞} de x par l'unité, la relation $g = s\pi\xi_{\nu}\gamma$ se décompose en

$$(9) \quad g = s_{\infty}(\pi\xi_{\nu}\gamma)_{\infty}, \quad 1 = s_f(\pi\xi_{\nu}\gamma)_f ;$$

comme la partie "finie" d'un ouvert de Siegel dans G_A est compacte, la seconde relation (9) montre que $(\pi\xi_{\nu}\gamma)_f$ reste dans un compact fixe de G_A , donc aussi $(\pi\xi_{\nu})_f$ puisque γ_f reste dans le produit des M_p , p fini; on en déduit que, pour chaque ν , les $\pi \in P_K$ qui apparaissent ici restent dans un nombre fini de classes modulo $P_K \cap \Gamma$, ou, ce qui revient au même, modulo $P_K \cap \xi_{\nu} \Gamma \xi_{\nu}^{-1}$; il y a donc des $\pi_{\nu\rho} \in P_K$ en nombre fini tels que (9) implique $\pi\xi_{\nu} \in \pi_{\nu\rho} \xi_{\nu} \Gamma$ pour un ρ au moins, et comme $s_{\infty} \in \mathcal{G}$ la première relation (9) montre que

$$G_{\infty} = \bigcup \mathcal{G}\pi_{\nu\rho} \xi_{\nu} \Gamma ;$$

comme la réunion des $\mathcal{G}\pi_{\nu\rho}$ est évidemment un ouvert de Siegel dans G_{∞} , nous avons démontré que (b) implique (a).

Supposons inversement $G_{\infty} = \bigcup \mathcal{G}_{\nu}^{\xi} \Gamma$, et montrons que $G_K = \bigcup P_K \xi_{\nu} \Gamma$. Soit $\xi \in G_K$; on a

$$\mathcal{G}\xi \subset \bigcup \mathcal{G}_{\nu}^{\xi} \gamma$$

et d'après le théorème 9 on peut donc trouver des $\gamma_{\lambda} \in \Gamma$ en nombre fini tels que l'on ait

$$\mathcal{G}\xi \subset \bigcup \mathcal{G}_{\nu}^{\xi} \gamma_{\lambda} .$$

Il s'ensuit immédiatement que, pour un choix convenable de ν et λ , il y a dans $T_{\infty}^+ \cap \mathcal{G}$ des t_n vérifiant $t_n \xi \in \mathcal{G}_{\nu} \gamma_{\lambda}$ pour tout n , et $\lim_{n \rightarrow \infty} \alpha_i(t_n) = 0$ pour tout i ; comme la première relation s'écrit encore $t_n \gamma \in \mathcal{G}$ où

$$\gamma = \xi \gamma_{\lambda}^{-1} \xi_{\nu}^{-1}$$

le lemme 3 du § 10 (qui s'applique ici puisque $\mathcal{G}$ est l'intersection de G_{∞} avec un ouvert de Siegel de G_A qui, on peut le supposer, contient la composante finie de γ) montre que pour chaque indice j on a soit $\alpha_j(t_n) > 1$, ce qui n'est justement pas le cas, soit $\gamma \in P(j)$. Ainsi on a, pour un choix convenable de ν et de λ , la relation

$$\xi \gamma_{\lambda}^{-1} \xi_{\nu}^{-1} \in \bigcap_{1 \leq j \leq r} P(j)_k = P_k$$

et ceci montre que $\xi \in P_k \xi_{\nu} \Gamma$, ce qui termine la démonstration.

BIBLIOGRAPHIE

- [1] BOREL (Armand). - Ensembles fondamentaux pour les groupes arithmétiques. Colloque sur la théorie des groupes algébriques [1962 Bruxelles], p. 23-40. - Gauthier-Villars, 1962 (Centre belge de Recherches mathématiques).
- [2] BOREL (A.) and HARISH-CHANDRA. - Arithmetic subgroups of algebraic groups, *Annals of Math.*, Series 2, t. 75, 1962, p. 485-535.
- [3] GODEMENT (Roger). - Groupes linéaires algébriques sur un corps parfait, *Séminaire Bourbaki*, t. 13, 1960/61, n° 206, 22 p.
- [4] MOSTOW (G. D.) and TAMAGAWA (T.). - On the compactness of arithmetically defined homogeneous spaces, *Annals of Math.*, Series 2, t. 76, 1962, p. 446-463.
- [5] ONO (T.). - Sur une propriété arithmétique des groupes commutatifs, *Bull. Soc. math.*, France, t. 85, 1957, p. 307-323.
- [6] WEIL (André). - Adeles and algebraic groups. - Princeton, Institute for advanced Study, 1961 (multigraphié).