Sous-groupes arithmétiques et réseaux

Ce cours est un "préliminaire" pour le dernier cours, concernant la croissance et la finitude des formes automorphes. On étudie les sous-groupes arithmétiques des groupes réductifs, sujet délicat, très technique et qui a fait (et fait toujours) couler beaucoup d'encre... La référence fondamentale est le (difficile) livre de Borel "Introduction aux groupes arithmétiques". Le livre de Platonov et Rapinchuk "Algebraic groups and number theory" est aussi une merveille. Enfin, l'article de Borel et Harish-Chandra "Arithmetic subgroups of algebraic groups" est très bien écrit (mais très technique). Nous allons illustrer les résultats principaux, sans faire des démonstrations complètes, qui sont souvent fort pénibles.

1 Un théorème de Borel et Harish-Chandra

Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ un $\mathbf{Q}$-groupe algébrique. Contrairement à $G(\mathbf{Q})$, le groupe $G(\mathbf{Z}) := G \cap \mathbf{GL}_n(\mathbf{Z})$ dépend vraiment du choix du plongement de G dans $\mathbf{GL}_n(\mathbf{C})$, mais le résultat suivant montre qu'il est bien défini à commensurabilité près. Rappelons que deux sous-groupes H_1, H_2 d'un groupe H sont dits commensurables si leur intersection est d'indice fini dans chacun d'entre eux. Cela définit une relation d'équivalence sur les sous-groupes de H.

Proposition 1.1. *Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ et $\rho : G \to \mathbf{GL}_m(\mathbf{C})$ un $\mathbf{Q}$-morphisme de $\mathbf{Q}$-groupes algébriques. Alors:*

a) Il existe un sous-groupe d'indice fini Γ de $G(\mathbf{Z})$ tel que $\rho(\Gamma) \subset \mathbf{GL}_m(\mathbf{Z})$.

b) Si ρ est injectif, alors $\rho(G(\mathbf{Z}))$ est commensurable avec $\rho(G)(\mathbf{Z}) := \rho(G) \cap \mathbf{GL}_m(\mathbf{Z})$.

Proof. a) Ecrivons $\rho(g) = (f_{ij}(g))_{i,j}$, avec $f_{i,j} \in \mathbf{Q}[\mathbf{GL}_n(\mathbf{C})]$. Si $N \geq 1$ est un entier, alors $\Gamma(N) = \{g \in \mathbf{GL}_n(\mathbf{Z}) | g \equiv 1 \pmod N\}$ est un sous-groupe distingué d'indice fini de $\mathbf{GL}_n(\mathbf{Z})$, donc $\Gamma(N, G) := \Gamma(N) \cap G$ est distingué d'indice fini dans $G(\mathbf{Z})$. Il suffit de montrer que pour N convenable on a $\rho(\Gamma(N, G)) \subset \mathbf{GL}_m(\mathbf{Z})$, ou encore que $\rho(\gamma) \in M_m(\mathbf{Z})$ pour $\gamma \in \Gamma(N, G)$. Cela découle immédiatement du fait que les $f_{i,j}$ sont à coefficients rationnels et $f_{i,j}(I_n) = \delta_{ij}$ (car $\rho(I_n) = I_m$).

b) Le morphisme bijectif $\rho : G \to H := \rho(G)$ est un isomorphisme de $\mathbf{Q}$-groupes algébriques[1]. Notons $\rho^{-1} : H \to G$ son inverse, un $\mathbf{Q}$-morphisme auquel on peut appliquer a). On obtient l'existence d'un sous-groupe Γ_1 d'indice fini dans $H(\mathbf{Z}) = H \cap \mathbf{GL}_m(\mathbf{Z})$ tel que $\rho^{-1}(\Gamma_1) \subset \mathbf{GL}_n(\mathbf{Z})$, autrement dit $\Gamma_1 \subset \rho(G(\mathbf{Z}))$. D'autre part le point a) montre que $H(\mathbf{Z})$ contient un sous-groupe d'indice fini dans $\rho(G(\mathbf{Z}))$, donc $H(\mathbf{Z})$ et $\rho(G(\mathbf{Z}))$ sont commensurables. □

[1] Rappelons que tout morphisme bijectif de groupes algébriques est un isomorphisme.

Définition 1.1. Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ un $\mathbf{Q}$-groupe algébrique. Un sous-groupe $\Gamma \subset G(\mathbf{Q})$ est dit **arithmétique** si Γ est commensurable avec $G(\mathbf{Z})$.

Exercice 1.1. Soit G un $\mathbf{Q}$-groupe algébrique, $\rho : G \to \mathbf{GL}_m(\mathbf{C})$ un morphisme défini sur $\mathbf{Q}$, $\Gamma \subset G(\mathbf{Q})$ un sous-groupe arithmétique et $v \in \mathbf{Q}^m$. Il existe un réseau[2] $R \subset \mathbf{Q}^m$ contenant v et stable par $\rho(\Gamma)$.

La proposition 1.1 montre que si $\rho : G \to G'$ est un isomorphisme de $\mathbf{Q}$-groupes algébriques, alors $\rho(\Gamma)$ est arithmétique dans G' dès que Γ est arithmétique dans G. Un théorème beaucoup plus profond est le suivant:

Théorème 1.2. *(Borel, Harish-Chandra) a) Soit $f : G \to G'$ un morphisme surjectif de $\mathbf{Q}$-groupes algébriques. Si Γ est arithmétique dans G, alors $f(\Gamma)$ est arithmétique dans G'.*

b) Tout sous-groupe arithmétique d'un $\mathbf{Q}$-groupe algébrique est de présentation finie, en particulier de type fini.

L'étude des formes automorphes fait naturellement intervenir l'analyse sur des espaces du type $\Gamma\backslash G(\mathbf{R})$, en particulier il sera très important de savoir quand ce genre de quotient est compact ou de mesure (de Haar) finie.

Si G est un groupe localement compact, un sous-groupe Γ de G est appelé un **réseau de** G si Γ est discret dans G et si G/Γ possède une mesure G-invariante finie. Un tel groupe est forcément unimodulaire (exercice) et $\Gamma\backslash G$ possède aussi une mesure G-invariante finie. Par exemple, un réseau de $\mathbf{R}^n$ est précisément un sous-groupe libre de rang n dans $\mathbf{R}^n$ (ce n'est pas vraiment évident, mais assez classique tout de même).

Soit G un $\mathbf{Q}$-groupe et $\Gamma \subset G(\mathbf{Q})$ un sous-groupe arithmétique. Alors Γ est un sous-groupe discret de $G(\mathbf{R})$, ce dernier étant un groupe localement compact. On peut naturellement se demander sous quelles conditions Γ est un réseau de $G(\mathbf{R})$. Ce n'est pas toujours le cas, prendre par exemple $G = \mathbf{C}^*$ (tout sous-groupe arithmétique de $G(\mathbf{Q})$ est fini, et le quotient de $\mathbf{R}^*$ par un groupe fini n'est pas de mesure invariante finie). En général, on dispose du théorème très difficile suivant (rappelons que $X(H)_k = \mathrm{Hom}_{k-gr.alg}(H, \mathbf{C}^*)$).

Théorème 1.3. *(Borel, Harish-Chandra) Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ un $\mathbf{Q}$-groupe algébrique. Alors $G(\mathbf{Z})$ est un réseau dans $G(\mathbf{R})$ si et seulement si $X(G^0)_{\mathbf{Q}} = 1$.*

Remarque 1.4. a) Bien sûr, $G(\mathbf{Z})$ est un réseau de $G(\mathbf{R})$ si et seulement si Γ est un réseau de $G(\mathbf{R})$ pour tout groupe arithmétique $\Gamma \subset G(\mathbf{Q})$.

b) En particulier $G(\mathbf{R})$ est unimodulaire quand $X(G^0)_{\mathbf{Q}} = 1$. Par des arguments généraux, cela revient à dire que $|\det(\mathrm{Ad}(g))| = 1$ pour $g \in G(\mathbf{R})$, qui découle à son tour du fait que la composée de $\mathrm{Ad} : G \to \mathbf{GL}(\mathfrak{g})$ et de $\det : \mathbf{GL}(\mathfrak{g}) \to \mathbf{C}^*$ est un morphisme de groupes défini sur $\mathbf{Q}$, donc d'ordre fini (car trivial sur G^0 par hypothèse).

Il est hors de question de discuter la preuve, très difficile, de ce théorème, mais nous allons discuter un certain nombre de cas particuliers, qui font intervenir pas mal de techniques très utiles.

Dans un premier temps, nous allons expliquer pourquoi $\mathbf{SL}_n(\mathbf{Z})$ est un réseau de $\mathbf{SL}_n(\mathbf{R})$ (ce n'est déjà pas trivial!). Cela repose sur l'énoncé assez technique ci-dessous, qui sera crucial pour la suite. Notons $K = O(n)$, le sous-groupe compact

[2] i.e. un groupe abélien libre de rang m contenu dans $\mathbf{Q}^m$.

maximal standard de $\mathbf{GL}_n(\mathbf{R})$, $A = \{\mathrm{diag}(a_1, ..., a_n) | a_i > 0, i = 1, ..., n\}$ et N groupe des matrices triangulaires supérieures unipotentes. Un argument standard, conséquence du procédé d'orthogonalisation de Gram-Schmidt permet de montrer que l'application produit $K \times A \times N \to G$ est un homéomorphisme (qu'on appelle **décomposition d'Iwasawa**), ainsi tout élément de $\mathbf{GL}_n(\mathbf{R})$ s'écrit de manière unique $g = kan$ et aussi $g = n'a'k'$, avec des notations évidentes.

Si $t, u > 0$ on pose

$$A_t = \{a = \mathrm{diag}(a_1, ..., a_n) \in A | a_1 \leq ta_2 \leq t^2 a_3 \leq ... \leq t^{n-1} a_n\},$$

ainsi que

$$N_u = \{n \in N | |n_{ij}| \leq u, i < j\},\ \mathscr{S}_{t,u} = KA_t N_u.$$

Les $\mathscr{S}_{t,u}$ sont des cas particuliers d'ensembles de Siegel, et ils forment des approximations raisonnables d'un domaine fondamental de $\mathbf{GL}_n(\mathbf{Z})$ dans $\mathbf{GL}_n(\mathbf{R})$. Nous aurons besoin seulement de la version plus faible suivante:

Théorème 1.5. *On a* $\mathbf{GL}_n(\mathbf{R}) = \mathscr{S}_{t,u}\mathbf{GL}_n(\mathbf{Z})$ *pour* $t \geq 2/\sqrt{3}$ *et* $u \geq 1/2$.

Proof. Notons simplement $G_n = \mathrm{GL}_n(\mathbf{R})$, $\Gamma_n = \mathrm{GL}_n(\mathbf{Z})$ et $\mathscr{S}^n = \mathscr{S}_{2/\sqrt{3},1/2}$. En notant $e_1, ..., e_n$ la base canonique de $\mathbf{R}^n$, on va montrer par récurrence sur n que pour tout $g \in G_n$ $\min_{x \in g\Gamma_n} ||xe_1||$ (qui est bien atteint sur $g\Gamma_n$ car $g\Gamma_n(e_1)$ est discret) est atteint en un point de $\mathscr{S}^n$. Cela montrera que $g\Gamma_n \cap \mathscr{S}^n \neq \emptyset$ et permettra de conclure. L'ingrédient essentiel est le:

Lemme 1.1. *Si* $g = kan$ *vérifie* $||ge_1|| = \min_{x \in g\Gamma_n} ||xe_1||$, *alors il existe* $\bar{n} \in N_{1/2}$ *tel que* $h = ka\bar{n} \in g\Gamma_n$ *et* $||ge_1|| = ||he_1||$. *De plus* $a_1/a_2 \leq 2/\sqrt{3}$.

Proof. Une récurrence facile montre que $N = N_{1/2}(N \cap \Gamma_n)$. Prenons $\bar{n} \in N_{1/2}$ tel que $n \in \bar{n}(N \cap \Gamma_n)$ et notons $h = ka\bar{n}$. Alors $||ge_1|| = ||ae_1|| = a_1$, d'où la première partie. Pour la seconde, considérons la matrice Z qui permute e_1 and e_2 et fixe $e_3, ..., e_n$. Alors

$$a_1 = ||he_1|| \leq ||hZe_1|| = ||he_2|| = ||k(a_1\bar{n}_{12}e_1 + a_2e_2)|| = \sqrt{a_1^2\bar{n}_{12}^2 + a_2^2}$$

et on conclut en utilisant l'inégalité $\bar{n}_{12}^2 \leq 1/4$. □

Pour $n = 2$ le résultat suit directement du lemme. Supposons qu'il est vrai pour $n-1$ et montrons le pour n. Soit $g = kan$ tel que $||ge_1|| = \min_{x \in g\Gamma_n} ||xe_1||$. Ecrivons $n = \left(\begin{smallmatrix} 1 & * \\ 0 & n' \end{smallmatrix}\right)$, $a = \left(\begin{smallmatrix} a_1 & 0 \\ 0 & a' \end{smallmatrix}\right)$ avec a', n' des matrices de taille $(n-1) \times (n-1)$. Par hypothèse de récurrence on peut écrire $a'n'c' = k''a''n''$ avec $c' \in \Gamma_{n-1}$, $k'' \in O_{n-1}(\mathbf{R})$, $a_i''/a_{i+1}'' \leq 2/\sqrt{3}$ et $|n_{ij}''| \leq 1/2$. Alors

$$g\left(\begin{smallmatrix} 1 & 0 \\ 0 & c' \end{smallmatrix}\right) = k\left(\begin{smallmatrix} 1 & 0 \\ 0 & k'' \end{smallmatrix}\right)\left(\begin{smallmatrix} a_1 & 0 \\ 0 & a'' \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & * \\ 0 & n'' \end{smallmatrix}\right)$$

autrement dit on peut écrire $g\tilde{c} = \tilde{k}\tilde{a}\tilde{n}$ avec des notations évidentes. Puisque $\tilde{c}e_1 = e_1$, on a $||g\tilde{c}e_1|| = ||ge_1||$, donc $||g\tilde{c}e_1|| = \min_{x \in g\tilde{c}\Gamma_n} ||xe_1||$. Le lemme montre que $a_1/a_1'' \leq 2/\sqrt{3}$. Cela permet de conclure, en utilisant encore l'égalité $N = N_{1/2}(N \cap \Gamma_n)$ pour modifier $\tilde{n}$. □

Remarque 1.6. Un résultat beaucoup plus délicat, dû à Siegel, est que les ensembles de Siegel $\mathscr{S}_{t,u}$ ci-dessus ne se rencontrent pas trop, au sens où pour tout $b \in \mathbf{GL}_n(\mathbf{Q})$ il n'existe qu'un nombre fini de $\gamma \in \mathbf{GL}_n(\mathbf{Z})$ tels que $\mathscr{S}_{t,u}\gamma \cap \mathscr{S}_{t,u}b \neq \emptyset$. La preuve de ce résultat est fort technique, cf. le chapitre 1 du livre de Borel.

Proposition 1.2. $\mathbf{SL}_n(\mathbf{Z})$ *est un réseau dans* $\mathbf{SL}_n(\mathbf{R})$.

Proof. Soit $G = \mathbf{SL}_n$ et notons $\mathscr{S}^1_{t,u} = \mathscr{S}_{t,u} \cap G(\mathbf{R})$. Le théorème 1.5 entraîne directement l'égalité $G(\mathbf{R}) = \mathscr{S}^1_{t,u} G(\mathbf{Z})$. Relativement à la décomposition d'Iwasawa $G = K_0 A_0 N$ (avec $K_0 = \mathrm{SO}_n(\mathbf{R})$, $A_0 = A \cap G$) la mesure de Haar de $G(\mathbf{R})$ se décompose

$$dg = \rho(a) dk \cdot da \cdot dn, \quad \rho(a) = \prod_{i<j} \frac{a_i}{a_j},$$

donc

$$\mathrm{vol}(\mathscr{S}^1_{t,u}) = \int_{K_0} dk \int_{A_t \cap G} \rho(a) da \int_{N_u} dn.$$

Par compacité de K et N_u il suffit de vérifier que $\int_{A_t \cap G} \rho(a) da < \infty$. L'identification de A_0 avec $(\mathbf{R}^*_+)^{n-1}$ via $a \to (a_1/a_2, a_2/a_3, ..., a_{n-1}/a_n)$ permet d'identifier $A_t \cap G$ avec les $x \in (\mathbf{R}^*_+)^{n-1}$ tels que $x_i \leq t$. De plus, à travers cette identification on peut écrire $\rho(a) = \prod_{i=1}^{n-1} x_i^{r_i}$ avec des entiers $r_i > 0$. On a alors

$$\int_{A_t \cap G} \rho(a) da = \int_{[0,t]^{n-1}} x_1^{r_1} ... x_{n-1}^{r_{n-1}} \frac{dx_1}{x_1} ... \frac{dx_{n-1}}{x_{n-1}} < \infty.$$

□

2 Groupe des caractères, groupes semi-simples

Nous allons essayer de comprendre la structure de $X(G)_{\mathbf{Q}}$ pour un $\mathbf{Q}$-groupe réductif G. Pour cela nous allons d'abord introduire une classe très importante de groupes réductifs et montrer que l'étude des groupes réductifs se ramène à l'étude ("facile") des tores et l'étude (difficile) des groupes dans cette classe.

Définition 2.1. Un groupe algébrique réductif G est dit **semi-simple** si le centre de G est fini.

Par exemple, $\mathbf{SL}_n(\mathbf{C})$ est semi-simple, mais $\mathbf{GL}_n(\mathbf{C})$ ne l'est pas. Le théorème 2.1 ci-dessous est très facile pour $G = \mathbf{GL}_n(\mathbf{C})$, mais pas du tout évident en général. Pour la preuve nous utiliserons le résultat délicat suivant (cf. livre de Borel): si G est un groupe algébrique et $\mathfrak{g} = \mathrm{Lie}(G)$, alors G' est un groupe algébrique (connexe si G l'est) et $\mathrm{Lie}(G') = [\mathfrak{g}, \mathfrak{g}]$.

Théorème 2.1. *Si G est réductif, alors G' est semi-simple. Si de plus G est connexe et $T = Z(G)^0$ (un tore), alors $(G')' = G'$, $G = TG'$ et $T \cap G'$ est fini.*

Proof. Soit $\mathfrak{g} = \mathrm{Lie}(G)$ et $\mathfrak{z}$ le centre de $\mathfrak{g}$. Nous allons montrer ci-dessous que $\mathfrak{g} = \mathfrak{z} \oplus \mathfrak{g}'$, avec $\mathfrak{g}' = [\mathfrak{g}, \mathfrak{g}]$, que $(\mathfrak{g}')' = \mathfrak{g}'$ et enfin $\mathfrak{z}(\mathfrak{g}') = 0$. Admettons cela pour l'instant. Alors G' est un sous-groupe fermé distingué de G, donc réductif, et $\mathrm{Lie}(Z(G')) = \mathfrak{z}(\mathrm{Lie}(G')) = \mathfrak{z}(\mathfrak{g}') = 0$, donc $Z(G')$ est fini et G' est semi-simple. Ensuite, si G est connexe alors G' et $(G')'$ le sont aussi et $\mathrm{Lie}(G')' = (\mathfrak{g}')' = \mathfrak{g}'$.

Comme $(G')' \subset G'$ et les deux sont connexes, avec la même algèbre de Lie, on a $(G')' = G'$. Ensuite $T \cap G'$ est contenu dans le centre de G' qui est fini. Enfin, le morphisme de groupes $T \times G' \to G, (t,x) \to tx$ induit un isomorphisme sur les algèbres de Lie, donc il est surjectif (car G est connexe).

Montrons maintenant les assertions concernant $\mathfrak{g}$, en commençant par l'égalité $\mathfrak{g} = \mathfrak{z} + \mathfrak{g}'$. Utilisons les notations standard introduites dans l'étude du système de racines d'un groupe réductif. Clairement $\mathfrak{g}_\alpha \subset \mathfrak{g}'$ pour $\alpha \in \Phi$, il suffit donc de voir que $\mathfrak{h} \subset \mathfrak{z} + \mathfrak{g}'$. Nous avons vu que $H_\alpha \in \mathfrak{g}'$ pour $\alpha \in \Phi$ et $\mathfrak{h} \cap \mathfrak{z} + \mathrm{Vect}_{\alpha\in\Phi} H_\alpha = \mathfrak{h}$, ce qui permet de conclure.

Montrons ensuite que $\mathfrak{z} \cap \mathfrak{g}' = 0$. Soit $X = \sum_{i=1}^d [Y_i, Z_i] \in \mathfrak{g}' \cap \mathfrak{z}$. Il suffit de montrer que X est nilpotente, car alors $X = 0$ (vu que $X \in \mathfrak{h}$ est diagonalizable). Noter que si A commute à B et C, alors $\mathrm{Tr}(A[B,C]) = 0$, donc pour $k \geq 1$

$$\mathrm{Tr}(X^k) = \sum_{i=1}^d \mathrm{Tr}(X^{k-1}[Y_i, Z_i]) = 0,$$

et donc X est nilpotente. Montrons enfin que $(\mathfrak{g}')' = \mathfrak{g}'$. Or

$$\mathfrak{g}' = [\mathfrak{g}, \mathfrak{g}] = [\mathfrak{g}' + \mathfrak{z}, \mathfrak{g}' + \mathfrak{z}] = [\mathfrak{g}', \mathfrak{g}'] = (\mathfrak{g}')'$$

et si $X \in \mathfrak{g}'$ vérifie $[X, \mathfrak{g}'] = 0$, alors $[X, \mathfrak{g}] = [X, \mathfrak{z} + \mathfrak{g}'] = 0$, donc $X \in \mathfrak{z}$ et $X \in \mathfrak{z} \cap \mathfrak{g}' = 0$. □

Corollaire 2.1. *Si G est un groupe algébrique connexe semi-simple, alors $G = G'$, en particulier $X(G) = 1$. En particulier, si G est défini sur $\mathbf{Q}$ alors*[3] *$G(\mathbf{Z})$ est un réseau de $G(\mathbf{R})$.*

Corollaire 2.2. *Soit G un k-groupe réductif connexe et $T = Z(G)^0$, un k-tore. La restriction $X(G)_k \to X(T)_k$ est injective et son image est d'indice fini.*

Proof. Le morphisme $T \times G' \to G, (t,x) \to tx$ est surjectif, défini sur k, de noyau s'identifiant au groupe fini $T \cap G'$. Soit d son cardinal. On a donc un isomorphisme

$$X(G)_k \simeq \{\chi \in X(T \times G')_k | \chi(T \cap G') = 1\}.$$

Il est clair que $X(T \times G')_k = X(T)_k \times X(G')_k = X(T)_k$, puisque $X(G') = 1$ (vu que $(G')' = G'$). Donc la restriction à T identifie $X(G)_k$ à $\{\chi \in X(T)_k |\, \chi(T \cap G') = 1\}$, qui contient $|T \cap G'| \cdot X(T)_k$ et donc est d'indice fini dans $X(T)_k$. □

Exercice 2.2. Montrer que si G est un groupe réductif défini sur $\mathbf{R}$, alors $G(\mathbf{R})$ est unimodulaire.

3 Compacité et anisotropie

Rappelons qu'un k-tore T est dit **déployé sur** k si $X(T) = X(T)_k$, ce qui équivaut à l'existence d'un k-isomorphisme de groupes algébriques $T \simeq D_n(\mathbf{C})$. Si T est un

[3] Par le théorème 1.3.

k-tore arbitraire, on montre[4] que T est déployé sur une extension finie galoisienne K de k.

Exercice 3.1. Soit T un k-tore, déployé sur une extension finie galoisienne K de k. Le groupe $\Gamma = \mathrm{Gal}(K/k)$ agit sur $X(T)$ par $(\gamma.\chi)(x) = \gamma(\chi(\gamma^{-1}.x))$, et sur $X_*(T) := \mathrm{Hom}_{\mathrm{gr.alg}}(\mathbf{C}^*, T)$ par une formule similaire. Montrer qu'il y a une bijection naturelle entre les sous-k-tores de T et les sous-espaces vectoriels de $(X_*(T))_k \otimes \mathbf{Q}$ stables sous Γ.

La notion "opposée" à celle de tore déployé est celle de k-tore **anisotrope sur** k, i.e. tel que $X(T)_k = 0$. L'exercice suivant en construit:

Exercice 3.2. Soit K une extension galoisienne de k de degré $d > 1$. Soit $T = (K \otimes_k \mathbf{C})^*$.

a) Montrer qu'on a un isomorphisme naturel $T \simeq \prod_{\sigma \in \mathrm{Gal}(K/k)} \mathbf{C}^*$. En déduire que T est un tore algébrique.

b) Montrer que T est défini sur k et déployé sur K. Décrire $X(T)$ en tant que représentation de $\mathrm{Gal}(K/k)$.

c) L'application norme $K \to k$ induit une application norme $N : T \to \mathbf{C}^*$. Montrer que le noyau de N est un sous-tore de T qui est anisotrope sur k.

Exercice 3.3. Montrer que si T est un k-tore, alors T possède un plus grand k-sous-tore déployé sur k, noté T_d, ainsi qu'un plus grand k-sous-tore anisotrope sur k, noté T_a. De plus $T_{\mathrm{a}} = (\bigcap_{\chi \in X(T)_k} \ker(\chi))^0$ et l'application produit $T_a \times T_d \to T$ est surjective, de noyau fini.

Nous allons utiliser la discussion précédente pour établir deux résultats importants.

Théorème 3.4. *Soit G un k-groupe réductif connexe, avec $k \subset \mathbf{R}$. Soit S le plus grand tore k-déployé contenu dans le centre de G et soit $A = S(\mathbf{R})^0$. Le groupe $G^1 = \cap_{\chi \in X(G)_k} \ker(\chi^2)$ est un k-groupe algébrique réductif et on a une décomposition $G(\mathbf{R}) \simeq G^1(\mathbf{R}) \times A_G$.*

Proof. Soit $T = Z(G)^0$, un k-tore. Les restrictions $X(G)_k \to X(T)_k \to X(T_d)_k = X(T_d)$ sont injectives et leurs images sont d'indice fini (cor. 2.2). De plus, comme T_d est déployé sur k on a un isomorphisme canonique $A_G = T_d(\mathbf{R})^0 \simeq \mathrm{Hom}(X(T_d), \mathbf{R}_{>0})$ (via $t \to (\chi \to \chi(t))$). On veut montrer que pour tout $g \in G(\mathbf{R})$ il existe un unique $t \in T_d(\mathbf{R})^0$ tel que $\chi(t) = |\chi(g)|$ pour tout $\chi \in X(G)_k$. L'unicité est facile, montrons l'existence. Si $\chi \in X(T_d)$ il existe n tel que χ^n se prolonge en un élément de $X(G)_k$ et on pose $i(\chi) = \sqrt[n]{|\chi^n(g)|}$ (cela ne dépend pas du choix de n). On obtient un morphisme $i : X(T_d) \to \mathbf{R}_{>0}$, qui correspond à un $t \in T(\mathbf{R})^0$. □

Exercice 3.5. Prenons $k = \mathbf{Q}$ dans le théorème.

[4]Soit $\chi_1, ..., \chi_n$ une famille génératrice de $X = X(T)$. Soit $(f_i)_{i \in I}$ une k-base de $k[T]$. C'est aussi une $\mathbf{C}$-base de $\mathbf{C}[T]$ et donc on peut écrire $\chi_j = \sum_i a_{ij} f_i$, avec $a_{ij} \in \mathbf{C}$ nuls pour presque tout i. Il suffit de montrer que les a_{ij} vivent dans une extension finie de $\mathbf{Q}$, car alors tous les χ_i seront définis sur une extension finie galoisienne K de $\mathbf{Q}$ et donc T sera déployé sur K. Il suffit donc de vérifier que si $\chi \in X(T)$, et si $\chi = \sum_{i=1}^n a_i f_i$, avec $f_i \in k[T]$ libres sur k et $a_i \in \mathbf{C}$, alors $a_i \in \bar{\mathbf{Q}}$. Les f_i étant libres sur k, un exercice standard d'algèbre linéaire montre que $\det(f_i(T_j))$ n'est pas identiquement nul. Comme les points de torsion de T sont denses, on peut donc choisir $t_j \in T$ de torsion tels que $\det f_i(t_j) \neq 0$. Alors $\chi(t_j) \in \bar{\mathbf{Q}}$ (racines de l'unité!), et le système $\chi(t_j) = \sum_i a_i f_i(t_j)$ montre que les $a_i \in \bar{\mathbf{Q}}$.

a) Montrer que $G^1(\mathbf{R})$ contient tout sous-groupe compact de $G(\mathbf{R})$.
b) Si $\Gamma \subset G(\mathbf{Q})$ est arithmétique, alors Γ est un réseau dans $G^1(\mathbf{R})$.

Le théorème suivant est délicat, et la preuve n'est pas auto-contenue (elle utilise de manière cruciale un théorème assez délicat de Jacobson-Morozov).

Théorème 3.6. *Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ un k-groupe réductif connexe. Les assertions suivantes sont équivalentes:*
a) G ne contient aucun tore déployé sur k et non réduit à 1.
b) On a $X(G)_k = 1$ et $G(k)$ ne contient pas de matrice unipotente $\neq I_n$.

Un tel k-groupe est appelé **anisotrope sur** k (bien sûr, cette nouvelle définition est compatible avec la précédente pour les k-tores!).

Proof. Montrons que b) entraîne a). Soit S un tore déployé sur k dans G. Les espaces de racines relatifs $\mathfrak{g}_\alpha^k = \{X \in \mathfrak{g} | \, sXs^{-1} = \alpha(s)X, s \in S\}$ sont alors nuls pour $\alpha \in X(S) - \{0\}$. En effet, $\mathfrak{g}_\alpha^k$ est défini sur k, donc s'il est nontrivial il possède des éléments k-rationnels non nuls X. Un tel X est forcément nilpotent (prendre s tel que $\alpha(s) \neq 1$ et contempler l'égalité $sXs^{-1} = \alpha(s)X$) et e^X fournit un élément non trivial unipotent dans $G(k)$. On en déduit que $\mathfrak{g} = \mathrm{Lie}(Z_G(S))$ et donc $G = Z_G(S)$ (car G est connexe). Ainsi S est central, donc $X(Z(G)^0)_k$ se surjecte sur $X(S)_k$. Comme $X(G)_k = 1$, le groupe $X(Z(G)^0)_k$ est fini (cor. 2.2), donc $X(S)_k$ aussi, et cela force $S = 1$.

L'autre sens est nettement plus délicat. Il est facile de voir que $X(G)_k = 1$ (utiliser la discussion ci-dessus pour le k-tore $T = Z(G)^0$). Supposons qu'il existe $g \in G(k)$ unipotent nontrivial. Alors $\log(g) \in \mathfrak{g}_k$ est nilpotent non nul (exercice) et le théorème de Jacobson-Morozov (qui est valable sur k) montre l'existence d'un $\mathfrak{sl}_2$-triplet (e, f, h) dans $\mathfrak{g}_k$ tel que $e = \log(g)$. On montre alors "à la main" que l'application

$$\varphi : \mathbf{C}^* \to G, \varphi(t) = e^{-f/t} e^{(t-1)e} e^f e^{(\frac{1}{t}-1)e}$$

est un morphisme de groupes algébriques, défini sur k. Le fait que c'est une application polynomiale en t et t^{-1} se voit sur son expression, en se rappelant que e, f son nilpotents; de même, le fait que φ est défini sur k découle de la k-rationalité de e, f. Le point nontrivial consiste à vérifier que $\varphi(tt') = \varphi(t)\varphi(t')$. Une façon de faire est la suivante: le morphisme $\mathfrak{sl}_2 \to \mathfrak{g}$ se relève (par simple connexité de $\mathbf{SL}_2(\mathbf{C})$) en un morphisme de groupes de Lie $F : \mathbf{SL}_2(\mathbf{C}) \to G$, et $\varphi(t)$ n'est rien d'autre que $F(\mathrm{diag}(t, t^{-1}))$ (comme on le constate directement par un calcul dans $\mathbf{SL}_2(\mathbf{C})$). Enfin, l'image de φ définit un tore déployé sur k dans G, donc trivial, autrement dit φ est trivial. En dérivant en $t = 1$ on aboutit facilement à une contradiction. □

Exercice 3.7. Soit F une forme quadratique non dégénérée à coefficients dans $\mathbf{Q}$ et soit $G = SO(F)$. Montrer que G est anisotrope sur $\mathbf{Q}$ si et seulement si l'équation $F(x) = 0$ n'a pas de solution non-triviale dans $\mathbf{Q}^n$.

Le beau théorème suivant montre les liens profonds entre compacité et anisotropie pour les groupes réels:

Théorème 3.8. *(Bruhat-Tits) Un $\mathbf{R}$-groupe algébrique G connexe est réductif et anisotrope sur $\mathbf{R}$ si et seulement si $G(\mathbf{R})$ est compact.*

Proof. La partie délicate est de montrer la compacité de $G(\mathbf{R})$ quand G est réductif et anisotrope sur $\mathbf{R}$. Quitte à conjuguer, on peut supposer que $G(\mathbf{R})$ est auto-adjoint dans $\mathbf{GL}_n(\mathbf{R})$. Soit K un sous-groupe compact maximal de $G(\mathbf{R})$ et soit $\mathfrak{a}_0$ un sous-espace de Cartan dans $\mathfrak{p}_0 = \{X \in \mathfrak{g}_0 = \mathrm{Lie}(G(\mathbf{R}))|\, X = X^T\}$. Nous avons vu que $G(\mathbf{R}) = KAK$, avec $A = e^{\mathfrak{a}_0}$. Si $X \in \mathfrak{a}_0$ est non nul, la composante neutre de l'adhérence de Zariski de $e^{\mathbf{R}X}$ est un tore déployé sur $\mathbf{R}$ contenu dans G (immédiat), donc triviale et donc $X = 0$, autrement dit $A = 1$ et $G(\mathbf{R}) = K$ est bien compact. □

Exercice 3.9. Montrer le sens facile du théorème ci-dessus: si G est connexe et $G(\mathbf{R})$ est compact, alors G est réductif et anisotrope sur $\mathbf{R}$.

Le théorème suivant est l'analogue du théorème de Bruhat-Tits pour les groupes définis sur $\mathbf{Q}$. Nous n'allons pas faire la preuve en entier (elle est cependant **beaucoup** plus simple que celle du théorème 1.3), mais établir suffisamment de cas particuliers importants pour donner une idée des techniques utilisées dans la démonstration.

Théorème 3.10. *(Borel, Harish-Chandra) Soit G $\mathbf{Q}$-groupe réductif connexe. Alors $G(\mathbf{Z})\backslash G(\mathbf{R})$ est compact si et seulement si G est anisotrope sur $\mathbf{Q}$.*

Si $G \subset \mathbf{GL}_n(\mathbf{C})$ est un $\mathbf{Q}$-groupe, on note $\mathscr{R}_G = G(\mathbf{Z})\backslash G(\mathbf{R})$. C'est naturellement un espace métrique, pour la topologie quotient. Si $G = \mathbf{GL}_n(\mathbf{C})$, $\mathscr{R}_G$ s'identifie naturellement à l'espace $\mathscr{R} = \mathscr{R}_n$ des réseaux dans $\mathbf{R}^n$, en envoyant $G(\mathbf{Z})g$ sur le réseau $R_g = g^{-1}(\mathbf{Z}^n)$. De plus, le plongement $G \subset \mathbf{GL}_n(\mathbf{C})$ fournit une injection naturelle $\iota : \mathscr{R}_G \to \mathscr{R}$, identifiant $\mathscr{R}_G$ avec la $G(\mathbf{R})$-orbite du réseau $\mathbf{Z}^n$. Un premier point fondamental est le:

Théorème 3.11. *Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ un $\mathbf{Q}$-groupe réductif. Alors l'injection $\iota : \mathscr{R}_G \to \mathscr{R}$ est un homéomorphisme sur son image, qui est fermée.*

Proof. L'injection est évidemment continue. Supposons que $\iota(G(\mathbf{Z})g_k)$ converge vers $\mathbf{GL}_n(\mathbf{Z})g$, i.e. il existe $\gamma_k \in \mathbf{GL}_n(\mathbf{Z})$ tels que $\gamma_k g_k$ converge vers g dans $\mathbf{GL}_n(\mathbf{R})$. Nous allons montrer qu'il existe une représentation algébrique définie sur $\mathbf{Q}$ $\rho : \mathbf{GL}_n(\mathbf{C}) \to \mathrm{GL}(V)$ et un vecteur rationnel $v \in V(\mathbf{Q})$ tel que $G = \{g \in \mathbf{GL}_n(\mathbf{C})|\, \rho(g)v = v\}$. Admettons cela pour l'instant, on a alors $\rho(\gamma_k)\rho(g_k)v \to \rho(g)v$, donc $\rho(\gamma_k)v \to \rho(g)v$. Mais v étant rationnel et $\rho(\gamma_k)$ restant dans un réseau, on a forcément $\rho(\gamma_k)v = \rho(g)v$ pour k assez grand, donc $g^{-1}\gamma_k \in G$, i.e. $\gamma_k^{-1}g \in G(\mathbf{R})$, et donc $\mathbf{GL}_n(\mathbf{Z})g$ est dans l'image de ι. Ensuite, montrons que $G(\mathbf{Z})g_k$ converge dans $\mathscr{R}_G$, i.e. il existe $u_k \in G(\mathbf{Z})$ tels que $u_k g_k$ converge dans $G(\mathbf{R})$. Fixons k_0 tel que $g^{-1}\gamma_{k_0} \in G$ et posons $u_k = \gamma_{k_0}^{-1}\gamma_k$ pour $k \geq k_0$. Alors $u_k \in \mathbf{GL}_n(\mathbf{Z}) \cap G(\mathbf{R}) = G(\mathbf{Z})$ (car $\gamma_{k_0}^{-1}g$ et $\gamma_k g^{-1}$ sont dans $G(\mathbf{R})$) et $u_k g_k$ converge vers $\gamma_{k_0}^{-1}g$ dans $G(\mathbf{R})$.

Il reste à voir l'existence de ρ. Nous avons déjà vu que $X = \mathbf{GL}_n(\mathbf{C})//G$ est une variété algébrique avec action transitive de $\mathbf{GL}_n(\mathbf{C})$, et G est le stabilisateur d'un point rationnel x_0 de X. Comme G est défini sur $\mathbf{Q}$, il est clair que X l'est aussi, et les arguments d'un cours précédent montrent qu'il existe une immersion fermée $\varphi : X \to \mathbf{C}^m$ définie sur $\mathbf{Q}$ et une représentation définie sur $\mathbf{Q}$ $\rho : \mathbf{GL}_n(\mathbf{C}) \to \mathbf{GL}_m(\mathbf{C})$ telle que $\varphi(g.x) = \rho(g)\varphi(x)$. Mais alors G est le stabilisateur de $v = \varphi(x_0)$, un vecteur rationnel de $\mathbf{C}^m$. □

Exercice 3.12. Montrer que si G est un $\mathbf{Q}$-groupe réductif connexe tel que $G(\mathbf{Z})\backslash G(\mathbf{R})$ est compact, alors G est anisotrope sur $\mathbf{Q}$.

Remarque 3.13. On peut remplacer l'hypothèse que G est réductif par l'hypothèse $X(G)_{\mathbf{Q}} = 1$. En effet, l'existence d'un ρ comme dans la preuve découle alors du théorème de Chevalley (cf. cours 5). Cette hypothèse est satisfaite si G est formé de matrices unipotentes (exercice).

Dans un deuxième temps, nous allons utiliser le théorème 1.5 pour démontrer le beau critère de compacité suivant:

Théorème 3.14. *(critère de Mahler) Soit $M \subset \mathbf{GL}_n(\mathbf{R})$ un sous-ensemble tel qu'il existe $c > 0$ tel que*

$$\det(g) \geq c, \ \inf_{x \in \mathbf{Z}^n \setminus \{0\}} ||g^{-1}x|| \geq c$$

pour tout $g \in M$. Alors l'image de M dans $\mathscr{R}$ est d'adhérence compacte.

Proof. Prenons une suite $(g_j)_j$ dans M. Il faut montrer qu'il existe une sous-suite $(g_{j_k})_k$ et des $u_{j_k} \in \mathbf{GL}_n(\mathbf{Z})$ tels que $u_{j_k} g_{j_k}$ converge dans $\mathbf{GL}_n(\mathbf{R})$. En appliquant $g \to g^{-1}$ au théorème 1.5 on voit qu'il existe $t, u > 0$ tels que $\mathbf{GL}_n(\mathbf{R}) = \mathbf{GL}_n(\mathbf{Z}) N_u A'_t K$, où $A'_t = \{\mathrm{diag}(a_1, ..., a_n) \in A |\, a_1/a_2 \geq t, ..., a_{n-1}/a_n \geq t\}$. On peut donc écrire $g_j = \gamma_j n_j a_j k_j$, avec $\gamma_j \in \mathbf{GL}_n(\mathbf{Z})$, $n_j \in N_u$, $a_j \in A'_t$ et $k_j \in K$. Nous allons montrer que les a_j restent dans un compact de A, ce qui permettra de conclure. Mais $|\det(g_j)| = |\det(a_j)| \geq c$ pour tout j, et $\inf_{x \in \mathbf{Z}^n \setminus \{0\}} ||k_j^{-1} a_j^{-1} n_j^{-1} \gamma_j^{-1} x|| \geq c$, ce qui se traduit par $\inf_{x \in \mathbf{Z}^n \setminus \{0\}} ||a_j^{-1} n_j^{-1} x|| \geq c$. En prenant x le premier vecteur e_1 de la base canonique de $\mathbf{Z}^n$ on a $n_j^{-1} x = x$ et donc $||a_j^{-1} e_1|| \geq c$. Ecrivons $a_j = \mathrm{diag}(x_j^{(1)}, ..., x_j^{(n)})$, alors $x_j^{(1)}/x_j^{(2)} \geq t, ..., x_j^{(n-1)}/x_j^{(n)} \geq t$, $x_j^{(1)} ... x_j^{(n)} = |\det(a_j)| \geq c$ et $1/x_j^{(1)} = ||a_j^{-1} e_1|| \geq c$. Il s'ensuit que les $x_j^{(n)}$ restent dans un interval du type $[a, b]$ avec $a, b > 0$, ce qui permet de conclure. □

Corollaire 3.1. *Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ un $\mathbf{Q}$-groupe réductif, tel que $|\det(g)| = 1$ pour tout $g \in G(\mathbf{R})$. Supposons que pour toute suite $g_j \in G(\mathbf{R})$ et toute suite $v_j \in \mathbf{Z}^n$ telles que $g_j v_j \to 0$ on ait $v_j = 0$ pour tout j assez grand. Alors $G(\mathbf{Z})\backslash G(\mathbf{R})$ est compact.*

Proof. L'espace $G(\mathbf{Z})\backslash G(\mathbf{R})$ s'identifie à un sous-espace fermé de $\mathscr{R}$ (th. 3.11), il suffit donc de voir que l'image de $G(\mathbf{R})$ dans $\mathscr{R}$ est relativement compacte, ce qui découle directement de nos hypothèses et du critère de Mahler. □

Le résultat suivant sera notre "critère pratique" pour vérifier la compacité des quotients $G(\mathbf{Z})\backslash G(\mathbf{R})$.

Corollaire 3.2. *Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ un $\mathbf{Q}$-groupe algébrique réductif tel que $|\det(g)| = 1$ pour $g \in G(\mathbf{R})$. S'il existe un polynôme G-invariant $P \in \mathbf{Q}[\mathbf{C}^n]$ tel que l'équation $P(v) = 0$ a l'unique solution $v = 0$ dans $\mathbf{Q}^n$, alors $G(\mathbf{Z})\backslash G(\mathbf{R})$ est compact.*

Proof. Prenons un réseau R de V. D'après le corollaire précédent il suffit de voir que si $g_j \in G(\mathbf{R})$ et $v_j \in R$ satisfont $g_j v_j \to 0$, alors $v_j = 0$ pour j assez grand. Mais $P(g_j v_j)$ tend vers $P(0) = 0$ et donc $P(v_j) \to 0$ car P est G-invariant. Mais $P(v_j)$ restent dans un réseau de V, donc forcément $P(v_j) = 0$ pour j assez grand et donc $v_j = 0$ pour j assez grand, par hypothèse. □

Le résultat suivant est le cas essentiel du théorème 3.10. Cependant, il est assez pénible de passer de ce cas particulier au cas général (le centre de G pose des problèmes assez surprenants).

Théorème 3.15. *Soit $G \subset \mathbf{GL}_n(\mathbf{C})$ un $\mathbf{Q}$-groupe connexe, réductif, anisotrope sur $\mathbf{Q}$. Si le centre de G est trivial, alors $G(\mathbf{Z})\backslash G(\mathbf{R})$ est compact.*

Proof. L'argument magique suivant est dû à Mostow et Tamagawa. Nous avons vu que $X(G)_{\mathbf{Q}} = 1$, donc $|\det(g)| = 1$ pour $g \in G(\mathbf{R})$. Comme G est de centre trivial et connexe, la représentation adjointe $\mathrm{Ad} : G \to \mathbf{GL}(\mathfrak{g})$ est fidèle (i.e. injective). D'après le corollaire 3.2 il suffit de montrer l'existence d'un polynôme G-invariant $P \in \mathbf{Q}[\mathfrak{g}]$ tel que $P(X) = 0$ a l'unique solution $X = 0$ dans $\mathfrak{g}(\mathbf{Q})$. Ecrivons

$$\det(T \cdot I - X) = T^d + \sum_{i=0}^{d-1} p_i(X) T^i,$$

alors clairement $\varphi = \sum_{i=0}^{d-1} P_i^2 \in \mathbf{Q}[\mathfrak{g}]^G$. Supposons que $X \in \mathfrak{g}(\mathbf{Q})$ vérifie $\varphi(X) = 0$, donc $P_i(X) = 0$ pour tout i et donc X est nilpotent. Mais alors e^X est un élément unipotent de $G(\mathbf{Q})$, donc est forcément trivial par hypothèse, donc $X = 0$. Cela permet de conclure. □

Exemple 3.1. Dans chacun des cas suivants $G(\mathbf{Z})\backslash G(\mathbf{R})$ est compact:

• $G = O(F)$, F étant une forme quadratique non dégénérée à n variables, à coefficients rationnels et telle que l'équation $F(x) = 0$ a l'unique solution $x = 0$ dans $\mathbf{Q}^n$.

• $G \subset \mathbf{GL}_n(\mathbf{C})$ est un $\mathbf{Q}$-groupe algébrique formé de matrices unipotentes.

Proof. Le premier cas découle directement du corollaire 3.2. Pour le second nous allons utiliser le corollaire 3.1. Il faut voir que si $v_j \in \mathbf{Z}^n$ et $g_j \in G(\mathbf{R})$ vérifient $g_j v_j \to 0$, alors $v_j = 0$ pour j assez grand. Par un résultat non-trivial (version algébrique du théorème d'Engel) on peut trouver $A \in \mathbf{GL}_n(\mathbf{Q})$ telle que AGA^{-1} soit contenu dans le groupe N des matrices unipotentes supérieures. Posons $n^{(j)} = Ag_jA^{-1}$ et $w^{(j)} = Av_j$. Les $w^{(j)}$ restent dans un réseau de $\mathbf{Q}^n$ et $n^{(j)}w^{(j)} \to 0$. En notant $w_1^{(j)}, ..., w_n^{(j)}$ les coordonnées de $w^{(j)}$ dans la case canonique, on voit que $w_n^{(j)}$ tend vers 0, donc est égal à 0 pour j assez grand, ensuite $n^{(j)}w^{(j)} \to 0$ entraîne $w_{n-1}^{(j)} \to 0$ donc $w_{n-1}^{(j)} = 0$ pour j assez grand, etc. □

L'exemple suivant demande quelques préliminaires sur les algèbres de quaternions. Soient a, b des entiers non nuls. On leur associe un anneau de quaternions $D = D_{a,b}$, ayant une base $1, i, j, k$ sur $\mathbf{Z}$ telle que $i^2 = a, j^2 = b$ et $ij = -ji = k$. Si A est un anneau, on pose $D(A) = D \otimes_{\mathbf{Z}} A$, que l'on identifie à $A \oplus Ai \oplus Aj \oplus Ak$, avec les même règles de multiplication, faisant de $D(A)$ une A-algèbre. Par exemple, si $a = b = -1$ alors $D(\mathbf{R})$ est l'algèbre des quaternions de Hamilton. L'involution $x \to \bar{x}$ donnée par

$$\bar{x} = x_1 - x_2 i - x_3 j - x_4 k \quad \text{si} \quad x = x_1 + x_2 i + x_3 j + x_4 k,$$

vérifie $\bar{xy} = \bar{y}\bar{x}$, ce qui fait que l'application **norme réduite**

$$N : D(A) \to A, \quad x \to N(x) = x\bar{x} = x_1^2 - ax_2^2 - bx_3^2 + abx_4^2$$

est multiplicative et $D(A)^* = \{x \in D(A) |\, N(x) \in A^*\}$. Posons $D(A)^1 = \{x \in D(A) |\, N(x) = 1\}$, un sous-groupe de $D(A)^*$. Si K est un corps, $D(K)$ est une algèbre à division (i.e. $D(K)^* = D(K) \setminus \{0\}$) si et seulement si l'équation $N(x) = 0$ a uniquement la solution triviale $x = 0$ dans K.

Exercice 3.16. a) Montrer que si $b = p$ est premier et a n'est pas un résidu quadratique modulo p, alors $D_{a,b}(\mathbf{Q})$ est une algèbre à division.

b) Montrer que $D_{a,b}(\mathbf{Q})$ est soit une algèbre à division, soit isomorphe à $M_2(\mathbf{Q})$.

Théorème 3.17. *Soit $D = D_{a,b}$ comme ci-dessus.*

a) $D(\mathbf{C})^*$, $D(\mathbf{C})^1$ sont des groupes algébriques réductifs connexes, définis sur $\mathbf{Q}$.

b) Si $D(\mathbf{Q})$ est une algèbre à division, alors $D(\mathbf{Z})^1 \backslash D(\mathbf{R})^1$ est compact.

Proof. a) Le morphisme d'algèbres

$$l : D(\mathbf{C}) \to \mathrm{End}_{\mathbf{C}-ev.}(D(\mathbf{C})), x \to l(x) = (y \to xy)$$

est injectif et son image est l'ensemble des endomorphismes $\varphi \in \mathrm{End}_{\mathbf{C}}(D(\mathbf{C}))$ qui commutent avec les endomorphismes r_i, r_j, r_k, où $r_x : y \to yx$ (exercice facile). En prenant la base de $D(\mathbf{C})$ définie par $1, i, j, k$, les matrices des r_i, r_j, r_k sont à coefficients dans $\mathbf{Z}$ et $\mathrm{End}_{\mathbf{C}}(D(\mathbf{C}))$ s'identifie à $M_4(\mathbf{C})$. Donc $D(\mathbf{C})^*$ s'identifie au sous-groupe de $\mathbf{GL}_4(\mathbf{C})$ des matrices commutant à r_i, r_j, r_k, qui est évidemment un sous-groupe algébrique de $\mathbf{GL}_4(\mathbf{C})$, défini sur $\mathbf{Q}$.

Ensuite, pour $x \in D(\mathbf{C})$ le polynôme caractéristique de $l(x)$ est $N(T - x)^2 = (T^2 - \mathrm{Tr}(x)T + N(x))^2$, où $\mathrm{Tr}(x) = x + \bar{x}$. Ainsi on voit que la condition $N(x) = 1$ est de nature polynomiale (à coefficients rationnels) en les coefficients de la matrice de l_x dans la base $1, i, j, k$, ce qui montre que $D(\mathbf{C})^1$ est aussi un sous-groupe algébrique de $\mathbf{GL}_4(\mathbf{C})$, défini sur $\mathbf{Q}$.

Enfin, montrons qu'il existe des isomorphismes de groupes algébriques $D(\mathbf{C})^* \simeq \mathbf{GL}_2(\mathbf{C})$ et $D(\mathbf{C})^1 \simeq \mathbf{SL}_2(\mathbf{C})$, et donc $D(\mathbf{C})^*$ et $D(\mathbf{C})^1$ sont réductifs connexes. En effet, prenons $\alpha, \beta \in \mathbf{C}$ tels que $\alpha^2 = a$ et $\beta^2 = b$. On a un isomorphisme de $\mathbf{C}$-algèbres

$$\varphi : D(\mathbf{C}) \simeq M_2(\mathbf{C}),\ \varphi(x_1 + x_2 i + x_3 j + x_4 k) = \begin{pmatrix} x_1 + x_2\alpha & x_3 + x_4\alpha \\ b(x_3 - x_4\alpha) & x_1 - x_2\alpha \end{pmatrix},$$

tel que $\det(\varphi(x)) = N(x)$. Cela permet de conclure.

b) La norme réduite définit un polynôme invariant sur $D(\mathbf{C})^1$. Le résultat découle alors du corollaire 3.2. □

Remarque 3.18. Si $a, b > 0$ on a un isomorphisme de $\mathbf{R}$-algèbres

$$\varphi : D(\mathbf{R}) \simeq M_2(\mathbf{R}),\ \varphi(x_1 + x_2 i + x_3 j + x_4 k) = \begin{pmatrix} x_1 + x_2\sqrt{a} & x_3 + x_4\sqrt{a} \\ b(x_3 - x_4\sqrt{a}) & x_1 - x_2\sqrt{a} \end{pmatrix},$$

induisant des isomorphismes de groupes $D(\mathbf{R})^* \simeq \mathbf{GL}_2(\mathbf{R})$ et $D(\mathbf{R})^1 \simeq \mathbf{SL}_2(\mathbf{R})$. Ainsi $\varphi(D(\mathbf{Z})^1)$ devient un sous-groupe discret co-compact de $\mathbf{SL}_2(\mathbf{R})$, si $D(\mathbf{Q})$ est une algèbre à division.

4 Sous-groupes paraboliques

Ce qui suit est un survol sans démonstrations, tous les résultats ci-dessus demandent beaucoup de travail et nous n'avons plus le temps de les discuter sérieusement. Les résultats ci-dessous seront pleinement utilisés dans le dernier cours pour étudier la croissance des formes automorphes.

Définition 4.1. Soit G un groupe algébrique. Un **sous-groupe parabolique** de G est un sous-groupe Zariski fermé P de G qui est co-compact dans G, i.e. G/P est compact. Si G est défini sur $k \subset \mathbf{C}$, un **k-parabolique** est un sous-groupe parabolique de G défini sur k.

Cette définition "analytique" a un équivalent algébrique: un sous-groupe Zariski fermé P de G est parabolique si et seulement si G/P est une variété projective[5].

Exercice 4.1. Soit $G = \mathbf{GL}_n(\mathbf{C})$ et B le groupe des matrices triangulaires supérieures dans G. Montrer que B est un parabolique de G. Indication: montrer que $G = BK$, avec $K = U(n)$.

Exemple 4.1. Si $G = \mathbf{GL}_n(\mathbf{C})$, on peut montrer que tout parabolique de G contient un conjugué de B. D'autre part, les paraboliques contenant B sont décrits comme suit: on se donne une partition $n = n_1 + ... + n_k$ de n et on considère le groupe $P(n_1, ..., n_k)$ des matrices triangulaires supérieures par blocs, les blocs diagonaux étant de tailles $n_1, ..., n_k$. Alors les $P(n_1, ...n_k)$ épuisent les paraboliques contenant B. Pour $G = \mathbf{SL}_n(\mathbf{C})$ on a une description analogue.

Je ne sais pas démontrer simplement[6] le résultat suivant:

Théorème 4.2. *Soit K un sous-groupe compact maximal du groupe réductif G.*

a) On a $G = PK$ pour tout parabolique P de G.

b) Si G est défini sur $\mathbf{R}$, K_0 un sous-groupe compact maximal de $G(\mathbf{R})$ et P un $\mathbf{R}$-parabolique de G, alors $G(\mathbf{R}) = P(\mathbf{R})K_0$.

Soit G un k-groupe réductif connexe et P un k-parabolique. Un théorème fondamental et difficile de Chevalley montre que P est connexe. Soit $U = R_u(P)$ le **radical unipotent de** P, i.e. le plus grand sous-groupe distingué de P formé de matrices unipotentes[7]. Le groupe U est défini sur k (car invariant par $\mathrm{Aut}(\mathbf{C}/k)$, par son unicité). Grâce à un théorème de Mostow (ou bien par d'autres moyens, cf. la discussion ci-dessous) il existe un k-groupe $L \subset P$ tel que le morphisme $L \to P \to P/U$ soit un isomorphisme de k-groupes (de manière équivalente tel que la multiplication $L \times U \to P$ soit un isomorphisme de k-variétés[8]). Un tel L s'appelle un **k-sous-groupe de Levi de** P et la décomposition $P = UL$ s'appelle une **décomposition de Levi de** P. Tous les k-Levi de P sont conjugués sous $U(k)$ et ils sont des k-groupes réductifs connexes (si G est connexe).

Nous allons expliquer maintenant comment construire et classifier les k-paraboliques d'un k-groupe réductif connexe $G \subset \mathbf{GL}_n(\mathbf{C})$.

Construction/ classification I: méthode dynamique: on part d'un k-morphisme de groupes algébriques $\lambda : \mathbf{C}^* \to G$ et on pose

$$P(\lambda) = \{g \in G | \lim_{t \to 0} \lambda(t) g \lambda(t)^{-1} \text{ existe}\}.$$

Un théorème difficile de Borel et Tits affirme que les $P(\lambda)$ sont précisément les k-paraboliques de G (on peut avoir $P(\lambda) = P(\lambda')$ sans que $\lambda = \lambda'$). Une k-décomposition de Levi de $P(\lambda)$ est fournie par $P(\lambda) = U(\lambda)Z(\lambda)$, avec $U(\lambda) :=$

[5]Nous n'avons pas discuté les variétés projectives, mais on laisse au lecteur s'imaginer ce qu'est un fermé Zariski de l'espace projectif...

[6]i.e. sans la structure des sous-groupes paraboliques, discutée ci-dessous...

[7]L'existence d'un plus grand tel sous-groupe n'est pas évidente!

[8]Pas forcément de k-groupes algébriques!.

$\{g \in G | \lim_{t\to 0} \lambda(t)g\lambda(t)^{-1} = 1\}$ (le radical unipotent de $P(\lambda)$) et $Z(\lambda) = \{g \in G | \lambda(t)g = g\lambda(t), t \in \mathbf{C}^*\}$ le centralisateur de l'image de λ (un k-groupe réductif connexe).

Exercice 4.3. Montrer que $P(\lambda)$ est bien parabolique quand $G = \mathbf{GL}_n(\mathbf{C})$. Si $\lambda : \mathbf{C}^* \to G$ se factorise par le tore diagonal $D_n(\mathbf{C}) \subset G$, décrire la partition $n_1, ..., n_k$ de n correspondant à $P(\lambda)$. Vérifier que $P(\lambda) = U(\lambda)Z(\lambda)$ est bien une décomposition de Levi de $P(\lambda)$.

Construction/classification II: méthode "radicielle": on part cette fois d'un tore S déployé sur k maximal de G (un théorème difficile de Borel et Tits affirme que les choix possibles de S sont conjugués sous $G(k)$).

Le choix de S fournit un système de racines relatif $\Phi_k = \Phi_k(G, S)$, dont les éléments sont les $\alpha \in X(S) \setminus \{0\}$ tels que $\mathfrak{g}^k_\alpha := \{X \in \mathfrak{g} | sXs^{-1} = \alpha(s)X, s \in S\}$ soit non nul. Le groupe $L = Z_G(S)$ est réductif connexe (cf. un exercice du cours précédent), défini sur $\mathbf{Q}$ et on a une décomposition $\mathfrak{g} = \mathrm{Lie}(L) \oplus \oplus_{\alpha\in\Phi_k} \mathfrak{g}^{\mathbf{Q}}_\alpha$.

On choisit un système de racines positives $\Phi^+_k \subset \Phi_k$ et on pose $\mathfrak{u} = \sum_{\alpha\in\Phi^+_k} \mathfrak{g}^k_\alpha$. Il n'est pas très difficile de vérifier que toute matrice dans $\mathfrak{u}$ est nilpotente. Posons $U = e^{\mathfrak{u}} = \{e^X | X \in \mathfrak{u}\}$. En utilisant la formule de Campbell-Hausdorff, on montre que U est un groupe algébrique défini sur $\mathbf{Q}$ et formé de matrices unipotentes (le dernier point est évident, le fait que c'est une variété algébrique définie sur $\mathbf{Q}$ est aussi facile, le point non-trivial est le fait que U est bien un sous-groupe de $\mathbf{GL}_n(\mathbf{C})$). On vérifie aussi sans mal que U est normalisé par $L = Z_G(S)$ (exercice) et $U \cap L = 1$. On pose $P = Z_G(S)U$. Le théorème suivant est très délicat:

Théorème 4.4. *(Borel, Tits) a) Les k-paraboliques minimaux de G sont précisément les $G(k)$-conjugués de $P = Z_G(S)U$.*

b) Soit Δ_k la base associée à Φ^+_k. Il y a une bijection entre les sous-ensembles I de Δ_k et les k-paraboliques de G contenant P, en envoyant I sur $P_I = Z_G(S_I)U$, avec $S_I = (\cap_{\alpha\in I} \ker(\alpha))^0$.

Noter que $P_\emptyset = P, P_{\Delta_{\mathbf{Q}}} = G$ et $P_I \cap P_J = P_{I\cap J}$, donc $I \subset J$ entraîne $P_I \subset P_J$. La décomposition de Levi de P_I est $P_I = Z_G(S_I)U_I$, et

$$\mathrm{Lie}(U_I) = \sum_{\alpha\in\Phi^+_k\setminus \mathrm{Vect}(I)} \mathfrak{g}^k_\alpha \subset \mathrm{Lie}(U).$$

Les k-racines de $Z_G(S_I)$ sont $\Phi_k \cap \mathrm{Vect}(I)$.