Département de mathématiques
Université de Fribourg (Suisse)

# Du volume des quotients arithmétiques de l'espace hyperbolique

THESE

présentée à la Faculté des Sciences de l'Université de Fribourg (Suisse)
pour l'obtention du grade de *Doctor scientiarum mathematicarum*

Vincent Emery

de

Lens (VS)

Thèse n° 1648
UniPrint Fribourg
2009

Acceptée par la Faculté des Sciences de l'Université de Fribourg (Suisse) sur la proposition du jury :

Prof. Dr. Anand Dessai
Université de Fribourg, Président du jury

Prof. Dr. Ruth Kellerhals
Université de Fribourg, Directrice de thèse

Dr. Mikhail Belolipetsky
University of Durham (UK), Corapporteur

Prof. Dr. Eva Bayer Fluckiger
EPF Lausanne, Corapporteur

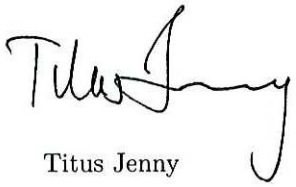
Prof. Dr. Gopal Prasad
University of Michigan, Corapporteur

Fribourg, le 14 octobre 2009

La directrice de thèse :

Ruth Kellerhals

Le doyen :



Titus Jenny

La réalisation de cette thèse a partiellement été soutenue par le Fonds national suisse de la recherche scientifique, projet n° 200020-121506/1.

# Résumé

Soit $\mathbb{H}^n$ l'espace hyperbolique de dimension $n$ et $\mathrm{Isom}^+(\mathbb{H}^n)$ son groupe des isométries préservant l'orientation. Parmi les sous-groupes discrets de $\mathrm{Isom}^+(\mathbb{H}^n)$ apparaissent notamment des sous-groupes arithmétiques. Leur étude est facilitée par des résultats provenant de la théorie des nombres et de la théorie qui concerne les groupes algébriques. En particulier, le volume de certains quotients de $\mathbb{H}^n$ par des sous-groupes arithmétiques peut se calculer à l'aide de la formule de volume de Prasad. Notre travail utilise cette formule, ainsi que plusieurs résultats d'un article de Borel et Prasad, pour déterminer le volume minimal des quotients arithmétiques de $\mathbb{H}^n$ pour $n \geq 5$ impair. Cela complète les résultats précédents de Chinburg-Friedman (pour $n = 3$) et Belolipetsky ($n \geq 4$ pair).

# Abstract

Let $\mathbb{H}^n$ be the hyperbolic $n$-space and $\mathrm{Isom}^+(\mathbb{H}^n)$ its group of isometries preserving the orientation. Among discrete subgroups of $\mathrm{Isom}^+(\mathbb{H}^n)$ appear arithmetic subgroups. Some of their properties can be studied using knowledge from number theory and the theory of algebraic groups. In particular the volume of some $n$-orbifolds defined by arithmetic subgroups can be computed using Prasad's volume formula. In this thesis we use this formula and some results from an article of Borel and Prasad to determine the minimal volume of arithmetic hyperbolic $n$-orbifolds, with $n \geq 5$ odd. This completes previous results of Chinburg-Friedman (for $n = 3$) and Belolipetsky ($n \geq 4$ even) about minimality of volume of arithmetic hyperbolic orbifolds.

# Remerciements

Je tiens en premier lieu à exprimer ma profonde gratitude envers mes deux directeurs de thèse, Ruth Kellerhals et Misha Belolipetsky, pour la précieuse aide que chacun d'entre eux m'a apportée durant la gestation de mon travail de doctorat.

Je remercie sincèrement Gopal Prasad pour l'intérêt qu'il a témoigné pour mon travail et pour la patience dont il a fait preuve pour répondre à chacune de mes questions. La qualité de ma thèse fut largement influencée par ma visite sur son lieu de travail, à Ann Arbor. Je le remercie enfin d'avoir accepté de figurer dans mon jury de thèse.

Je remercie Eva Bayer, qui elle aussi a spontanément accepté de faire partie du jury. Je suis honoré d'avoir comme corapporteurs dans mon jury de thèse deux mathématiciens d'une telle compétence.

Durant mes cinq années de thèse, j'ai exercé la fonction d'assistant au sein du département de mathématiques de Fribourg. Je me suis toujours senti à l'aise dans ce département, et je remercie pour cela les différents collègues que j'y ai côtoyés.

J'adresse finalement un immense merci à Vanessa pour toutes les marques d'encouragement qu'elle m'a témoignées durant ce travail.

# Table des matières

# Chapitre 1. Introduction

## §1.1 L'exemple du groupe modulaire

Le *groupe modulaire* $\mathrm{SL}_2(\mathbb{Z})$ joue un rôle prépondérant dans divers domaines des mathématiques. Pour le géomètre, son importance tient dans son opération sur le plan hyperbolique $\mathbb{H}^2 = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$. En effet, le groupe $\mathrm{SL}_2(\mathbb{R})$ opère sur $\mathbb{H}^2$ comme suit :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z \quad = \quad \frac{az+b}{cz+d} \ ;$$

et cette opération préserve la métrique hyperbolique sur $\mathbb{H}^2$. On a en fait un isomorphisme entre $\mathrm{SL}_2(\mathbb{R})/\{\pm I\}$ et le groupe $\mathrm{Isom}^+(\mathbb{H}^2)$ des isométries de $\mathbb{H}^2$ qui préservent l'orientation. Comme le groupe $\mathrm{SL}_2(\mathbb{Z})$ est discret dans $\mathrm{SL}_2(\mathbb{R})$, son opération sur $\mathbb{H}^2$ est proprement discontinue et l'espace quotient $\mathbb{H}^2/\mathrm{SL}_2(\mathbb{Z})$ possède une certaine géométrie modelée sur $\mathbb{H}^2$. Ce quotient se décrit à l'aide du domaine fondamental bien connu :

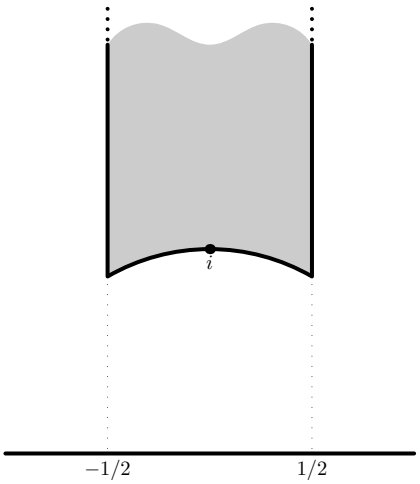



FIG. 1.1 – Domaine fondamental pour $\mathrm{SL}_2(\mathbb{Z})$ dans $\mathbb{H}^2$

Ce domaine n'étant pas borné, on observe que le quotient $\mathbb{H}^2/\mathrm{SL}_2(\mathbb{Z})$ n'est pas compact. On peut aussi facilement calculer le volume du domaine fondamental par rapport à l'élément de volume induit par la métrique hyperbolique : on obtient alors un volume fini pour $\mathbb{H}^2/\mathrm{SL}_2(\mathbb{Z})$.

## §1.2 L'idée de sous-groupe arithmétique

L'exemple de $\mathrm{SL}_2(\mathbb{Z})$ a inspiré une méthode générale pour créer des sous-groupes discrets $\Gamma < \mathrm{Isom}(X)$, où $X$ est un espace symétrique et $\mathrm{Isom}(X)$ son groupe des isométries. Un sous-groupe $\Gamma$, ainsi que le quotient $X/\Gamma$, est appelé « arithmétique » s'il est construit sur le modèle de $\mathrm{SL}_2(\mathbb{Z})$. Nous définirons précisément cette notion au chapitre 3. Nous voulons cependant déjà dans ce paragraphe en présenter l'idée fondamentale.

On écrit le groupe $\mathrm{Isom}(X)$, ou une légère variation de celui-ci, comme groupe de matrices à coefficients réels que nous notons ici par le symbole $G$. L'idée de « légère variation » est illustrée par le paragraphe §1.1, où $\mathrm{SL}_2(\mathbb{R})$ est localement isomorphe (comme groupe de Lie) à la composante connexe de $\mathrm{Isom}(\mathbb{H}^2)$. En prenant alors le sous-groupe $G_\mathbb{Z} < G$ des matrices inversibles à coefficients dans $\mathbb{Z}$, on obtient un sous-groupe discret. On peut cependant imaginer que le groupe $\mathrm{Isom}(X)$ soit représenté par un groupe $G$ dont les matrices possèdent des coefficients horriblement transcendants. Dans ce cas nous aurions $\Gamma = G_\mathbb{Z} = \{1\}$, loin de l'exemple non trivial de $\mathrm{SL}_2(\mathbb{Z})$. Pour obtenir des exemples intéressants, il faut imposer plus de structure sur le groupe $G$. La structure adéquate sur $G$ est celle de groupe algébrique linéaire (défini sur $\mathbb{Q}$). Nous débuterons donc, dès le chapitre 2, avec l'étude de ces groupes.

Un fait remarquable est qu'un quotient arithmétique $X/\Gamma$ possède nécessairement un volume fini (théorème 3.7). Parmi les quotients de $X$ possédant un volume fini, les quotients arithmétiques sont loin d'être quelques cas épars. Le théorème d'arithmeticité de Margulis (théorème 3.22) montre en fait que pour une grande partie des espaces symétriques $X$, chaque espace quotient $X/\Gamma$ de volume fini est arithmétique. Même pour les espaces $X$ pour lesquels le théorème de Margulis ne s'applique pas, les sous-groupes arithmétiques restent une source importante de quotients de $X$.

L'abondance d'exemples arithmétiques $X/\Gamma$ légitime de se restreindre dans certains cas à l'étude des quotients arithmétiques. Le deuxième aspect qui justifie une telle restriction est une question d'efficacité. En effet, bien qu'étant considérés ici sous l'angle de la géométrie (au sens riemannien du terme), les sous-groupes arithmétiques sont par nature liés à la géométrie algébrique et la théorie des nombres. On peut alors combiner certaines connaissances (parfois profondes) dans ces deux domaines pour obtenir des résultats géométriques concernant les quotients arithmétiques. Cette thèse se veut une illustration de ce principe.

## §1.3 Le problème traité et les résultats connus

Les résultats de cette thèse de doctorat concernent le volume des quotients des espaces hyperboliques $X = \mathbb{H}^n$. Plus particulièrement, on s'intéresse à la détermination des quotients orientables $\mathbb{H}^n/\Gamma$ de volume minimal. Commençons par donner une formulation précise du problème général. Pour cela, définissons pour chaque dimension $n \geq 2$ l'ensemble des *quotients orientables* de $\mathbb{H}^n$ :

$$\mathcal{Q}^n \quad := \quad \left\{ \mathbb{H}^n/\Gamma \mid \Gamma < \mathrm{Isom}^+(\mathbb{H}^n) \text{ est discret} \right\},$$

où $\mathrm{Isom}^+(\mathbb{H}^n)$ est le groupe des isométries de $\mathbb{H}^n$ qui préservent l'orientation. Un élément de cet ensemble est ce que l'on nomme « hyperbolic $n$-orbifold » en anglais. Il est assez naturel de séparer l'ensemble $\mathcal{Q}^n$ en deux sous-ensembles :

$$\begin{aligned} \mathcal{Q}^n_{\mathbf{c}} &:= \{\, \mathbb{H}^n/\Gamma \in \mathcal{Q}^n \mid \mathbb{H}^n/\Gamma \text{ est compact}\} \\ \mathcal{Q}^n_{\mathbf{nc}} &:= \{\, \mathbb{H}^n/\Gamma \in \mathcal{Q}^n \mid \mathbb{H}^n/\Gamma \text{ n'est pas compact}\} \end{aligned}$$

Soit alors $\mathrm{vol}_{\mathbb{H}}$ la mesure du *volume hyperbolique* sur $\mathbb{H}^n$, i.e. la mesure volume induite par la métrique riemannienne de $\mathbb{H}^n$. Pour chaque dimension $n$ on obtient alors, par passage aux quotients, une fonction :

$$\mathrm{vol}_{\mathbb{H}} \quad : \quad \mathcal{Q}^n \ \to \ \mathbb{R}_{>0} \cup \{\infty\}\,.$$

La question se pose alors de trouver le minimum dans chacun des ensembles $\mathrm{vol}_{\mathbb{H}}(\mathcal{Q}^n_{\mathbf{nc}})$ et $\mathrm{vol}_{\mathbb{H}}(\mathcal{Q}^n_{\mathbf{c}})$, et d'expliciter les quotients réalisant ces volumes minimaux. Pour $n \geq 4$ le théorème suivant montre que le problème est bien posé, c'est-à-dire que $\mathrm{vol}_{\mathbb{H}}(\mathcal{Q}^n_{\mathbf{nc}})$ et $\mathrm{vol}_{\mathbb{H}}(\mathcal{Q}^n_{\mathbf{c}})$ possèdent bien des minima :

**Théorème 1.1** (Wang)**.** *Soit $n \geq 4$ et $c > 0$ fixés . Alors il existe un nombre fini (à isométrie près) de quotients $\mathbb{H}^n/\Gamma$ avec*

$$\mathrm{vol}_{\mathbb{H}}(\mathbb{H}^n/\Gamma) \quad \leq \quad c.$$

Ce théorème est en fait valable pour une classe bien plus large d'espaces symétriques. Par contre il faut signaler que l'article original de Wang [Wan72] inclut le cas $\mathbb{H}^3$ de façon erronée, pour lequel l'affirmation serait en contradiction avec les résultats de Thurston et Jorgensen [Thu80, §5.11]. Cette question est discutée dans [Bor81, 8.3]. Ce même travail [Thu80, §5.11] montre avec le théorème de Kazhdan-Margulis [Vin93, Ch.7 : theorem 3.6] l'existence des volumes minimaux pour $n = 3$. C'est également avec le théorème de Kazhdan-Margulis qu'on s'assure du cas $n = 2$.

**Remarque 1.2.** Se restreindre aux sous-groupes discrets qui préservent l'orientation nous limite au cas des quotients orientables. Dans le contexte des sous-groupes arithmétiques il sera plus facile de traiter le cas orientable. Un quotient *non orientable* $\mathbb{H}^n/\Gamma$ est donné par un sous-groupe $\Gamma < \mathrm{Isom}(\mathbb{H}^n)$ qui n'est pas inclus dans $\mathrm{Isom}^+(\mathbb{H}^n)$. Le problème du volume minimal se pose de la même façon pour l'ensemble plus général des quotients (orientables ou non) de $\mathbb{H}^n$. Il n'y a pas (à notre connaissance) de passage automatique entre le cas orientable et le cas général (et inversément) pour problème du volume minimal. Tout au plus on aura occasionnellement recours aux constats élémentaires suivants :

- Chaque quotient non orientable $\mathbb{H}^n/\Gamma$ possède un revêtement double qui est orientable. Celui-ci est unique et est obtenu en considérant le groupe discret $\Gamma \cap \mathrm{Isom}^+(\mathbb{H}^n)$. On déduit de cela qui si $\mathbb{H}^n/\Gamma$ non orientable est l'unique quotient (à isométrie près) réalisant le volume minimal, alors son revêtement réalise le minimum dans le cas orientable (mais l'unicité n'est a priori plus garantie).
- Supposons $\mathbb{H}^n/\Gamma$ être orientable et revêtir un quotient non orientable. Si $\mathbb{H}^n/\Gamma$ réalise le volume minimal dans le cas orientable, alors le quotient non orientable dont il est le revêtement réalise le volume minimal dans le cas général. A priori $\mathbb{H}^n/\Gamma$ peut revêtir plusieurs quotients non orientables qui ne sont pas isométriques entre eux.

Passons à présent en revue les résultats connus qui apportent un élément de réponse au problème du volume minimal. Pour $n = 2$ la réponse, aussi bien pour le cas compact que pour le cas non compact, apparaît dans les travaux de Siegel [Sie45]. Notons que pour les quotients orientables non compacts, le minimum est réalisé par le groupe modulaire. En dimension $n = 3$, le cas orientable non compact est résolu par Meyerhoff [Mey85]. En utilisant des méthodes similaires, Hild et Kellerhals prouvent le résultat dans le cas général (pas nécessairement orientable) pour la dimension 4 [HK07], puis Hild pour les dimensions 5 à 9 [Hil07]. Ces résultats montrent dans chacun de ces cas que le volume minimal est réalisé par un quotient unique (à isométrie près), qu'on sait être arithmétique. Signalons que tous ces quotients (orientables ou non) s'obtiennent à partir de groupes de Coxeter hyperboliques.

Les méthodes qui permettent les succès énoncés sont de nature géométrique. Elles trouvent leur limite lorsque considérées pour le cas compact ($n \geq 3$) et pour les dimensions supérieures ($n \geq 10$) du cas non compact. On met alors en pratique l'idée énoncée en fin de §1.2, en restreignant l'étude de la fonction $\mathrm{vol}_{\mathbb{H}}$ aux ensembles formés des quotients (orientables) arithmétiques :

$$\begin{aligned} \mathcal{AQ}^n_{\mathbf{c}} &:= \{\, \mathbb{H}^n/\Gamma \in \mathcal{Q}^n_{\mathbf{c}} \mid \Gamma \text{ est arithmétique}\} \\ \mathcal{AQ}^n_{\mathbf{nc}} &:= \{\, \mathbb{H}^n/\Gamma \in \mathcal{Q}^n_{\mathbf{nc}} \mid \Gamma \text{ est arithmétique}\} \end{aligned}$$

Le problème de trouver le minimum de $\mathrm{vol}_{\mathbb{H}}(\mathcal{AQ}^3_{\mathbf{c}})$ trouve ainsi réponse dans le travail de Chinburg et Friedman [CF86]. Leur preuve repose sur des calculs de volume effectués par Borel [Bor81] pour les quotients arithmétiques $\mathbb{H}^3/\Gamma$. Là encore le volume minimal (parmi les quotients orientables arithmétiques) est réalisé par un unique quotient, lié à un groupe de Coxeter. Aucun quotient orientable non arithmétique $\mathbb{H}^3/\Gamma$ n'est connu pour réaliser un volume inférieur au minimum arithmétique. Il semble que les travaux de Gehring, Marshall et Martin puissent aboutir à une preuve que le minimum arithmétique donne également le minimum de $\mathrm{vol}_{\mathbb{H}}(\mathcal{Q}^3_{\mathbf{c}})$ [GM09].

Les calculs de volume de Borel pour les quotients arithmétiques de $\mathbb{H}^3$ sont généralisés par une formule de volume de Prasad [Pra89], qui rend possible le calcul de volume de certains quotients arithmétiques de n'importe quel espace symétrique $X$. Cette formule, combinée à certains résultats d'un article conjoint de Borel et Prasad [BP89] permet (avec une certaine imprécision donnée par un facteur rationnel) le calcul du volume des quotients arithmétiques $X/\Gamma$, où $\Gamma$ est un sous-groupe maximal (au sens de l'inclusion) dans $\mathrm{Isom}^+(X)$. Grâce à ces éléments, Belolipetsky [Bel04] [Bel07] donne dans le cas orientable une réponse à la question du minimum arithmétique pour les dimensions paires $n \geq 4$, aussi bien pour le cas compact que pour le cas non compact (nettement plus facile). L'unicité de ces quotients orientables arithmétiques de volume minimal est prouvée dans [Bel07].

## §1.4 Contenu et résultats

Les principaux résultats de cette thèse sont énoncés dans les deux théorèmes qui suivent. Le symbole $\zeta_k$ y désigne la fonction zêta associée au corps de nombres $k$, et pour une extension quadratique $k \subset \ell$ le symbole $L_{\ell|k}$ est la fonction $L$ associée (cf. §4.7).

**Théorème 1.3.** *Pour chaque dimension $n = 2r - 1 \geq 5$, le minimum $\nu_{\mathbf{c}}^n$ de l'ensemble $\mathrm{vol}_{\mathbb{H}}(\mathcal{AQ}_{\mathbf{c}}^n)$ est donné par :*

$$\nu_{\mathbf{c}}^n = \frac{1}{N_0(r)} \frac{5^{r^2-r/2} \cdot 11^{r-1/2} \cdot (r-1)!}{2^{2r-1}\pi^r} L_{\ell_0|k_0}(r) \prod_{j=1}^{r-1} \frac{(2j-1)!^2}{(2\pi)^{4j}} \zeta_{k_0}(2j),$$

*où $N_0(r)$ est un élément de $\{1, 2\}$, $k_0 = \mathbb{Q}(\sqrt{5})$ et $\ell_0$ est le corps de nombres de discriminant $-275$ (donné par $\ell_0 \cong \mathbb{Q}[x]/(x^4 - x^3 + 2x - 1)$).*

**Théorème 1.4.** *Pour les dimensions $n = 2r - 1 \geq 5$ on notera par $\nu_{\mathbf{nc}}^n$ le minimum de l'ensemble $\mathrm{vol}_{\mathbb{H}}(\mathcal{AQ}_{\mathbf{nc}}^n)$. On distingue alors les trois cas suivants :*

1. *si $r \equiv 1\ (4)$ :*

$$\nu_{\mathbf{nc}}^n = \frac{1}{2^{r-2}} \zeta(r) \prod_{j=1}^{r-1} \frac{(2j-1)!}{(2\pi)^{2j}} \zeta(2j);$$

2. *si $r \equiv 3\ (4)$ :*

$$\nu_{\mathbf{nc}}^n = \frac{1}{N_1(r)} \frac{(2^r - 1)(2^{r-1} - 1)}{3 \cdot 2^{r-1}} \zeta(r) \prod_{j=1}^{r-1} \frac{(2j-1)!}{(2\pi)^{2j}} \zeta(2j);$$

3. *si $r$ est pair :*

$$\nu_{\mathbf{nc}}^n = \frac{1}{N_1(r)} \frac{3^{r-1/2}}{2^{r-1}} L_{\ell_1|\mathbb{Q}}(r) \prod_{j=1}^{r-1} \frac{(2j-1)!}{(2\pi)^{2j}} \zeta(2j),$$

*où $N_1(r) \in \{1, 2\}$ et $\ell_1 = \mathbb{Q}(\sqrt{-3})$.*

Pour $n = 5, 7$ et $9$ on peut comparer les résultats de ce dernier théorème avec les résultats de [Hil07], où les quotients de volume minimal sont orientables et tous arithmétiques. Comme les travaux de Hild comportent un résultat d'unicité, on déduit de notre remarque 1.2 que $\nu_{\mathbf{nc}}^5$, $\nu_{\mathbf{nc}}^7$ et $\nu_{\mathbf{nc}}^9$ doivent correspondre au double des volumes minimaux donnés dans [Hil07]. On voit alors que les résultats concordent, avec $N_1(3) = N_1(4) = 1$.

La démonstration des théorèmes 1.3 et 1.4 suit essentiellement les idées du travail de Belolipetsky cité plus haut. Nous présentons ci-dessous une brève esquisse de la méthode qui sera utilisée aux chapitres 14 et 15 pour obtenir une preuve. Cela permettra notamment d'expliquer l'apparition des facteurs entiers $N_0(r)$ et $N_1(r)$, lesquels impliquent un certain défaut de notre résultat.

Soient deux sous-groupes arithmétiques $\Gamma, \Lambda < \mathrm{Isom}^+(\mathbb{H}^n)$ avec $\Lambda < \Gamma$. On sait alors que le quotient $\mathbb{H}^n/\Lambda$ est un revêtement de $\mathbb{H}^n/\Gamma$ et que les volumes de ces quotients sont reliés par l'égalité :

$$\mathrm{vol}_{\mathbb{H}}(\mathbb{H}^n/\Gamma) = \frac{1}{[\Gamma : \Lambda]} \mathrm{vol}_{\mathbb{H}}(\mathbb{H}^n/\Lambda).$$

Cette propriété élémentaire permet de restreindre la recherche de $\nu_{\mathbf{c}}^n$ et $\nu_{\mathbf{nc}}^n$ à l'inspection des sous-groupes arithmétiques qui sont maximaux dans $\mathrm{Isom}^+(\mathbb{H}^n)$.

Or un sous-groupe $\Gamma$ qui est maximal peut s'écrire sous la forme d'un normalisateur d'un sous-groupe arithmétique $\Lambda$ qui possède une forme particulière, et qu'on appelle « principal ». Les sous-groupes arithmétiques principaux sont précisément ceux pour lesquels la formule de volume de Prasad s'applique. On est ainsi capable de calculer les volumes des quotients arithmétiques qui peuvent potentiellement atteindre $\nu_{\mathbf{c}}^n$ (ou $\nu_{\mathbf{nc}}^n$) si l'on parvient à calculer l'indice $[\Gamma : \Lambda]$. L'article [BP89] contient des résultats qui permettent d'estimer cet indice, à défaut d'un calcul précis dans tous les cas.

Pour chaque dimension on construira au chapitre 14 des sous-groupes arithmétiques principaux $\Lambda_0$ et $\Lambda_1$ dont les normalisateurs $\Gamma_0$ et $\Gamma_1$ donnent des quotients $\mathbb{H}^n/\Gamma_0$ (compact) et $\mathbb{H}^n/\Gamma_1$ (non compact) qui sont des candidats pour réaliser le volume arithmétique minimal dans le cas orientable. Il nous sera possible de calculer l'indice $[\Gamma_i : \Lambda_i]$ à un facteur 2 près, ce qui avec la formule de Prasad donnera les volumes des quotients $\mathbb{H}^n/\Gamma_0$ et $\mathbb{H}^n/\Gamma_1$ (à un facteur 2 près). Ces valeurs sont précisément celles qui apparaissent dans les théorèmes 1.3 et 1.4. Au chapitre 15 il sera effectivement démontré qu'aucun quotient orientable arithmétique ne peut posséder un volume plus petit que la plus basse valeur proposée pour $\nu_{\mathbf{c}}^n$ (resp. $\nu_{\mathbf{nc}}^n$).

Cette thèse ne résout pas la question d'une éventuelle unicité du quotient réalisant le minimum. On expliquera cependant dans la remarque 15.5 comment la résolution de ce problème est théoriquement possible. L'autre problème ouvert, la détermination précise de l'entier $N_i(r)$, est également une question qui devrait pouvoir obtenir une réponse dans l'avenir (cf. remarque 15.4). Nous espérons du moins que la version finale de l'article en préparation [BE] puisse résoudre ces deux problèmes.

L'effort de notre travail culmine dans les deux derniers chapitres avec la démonstration des résultats annoncés. Pour le reste il s'agit d'une exposition que nous avons voulu le plus complète possible du problème des quotients arithmétiques et du calcul de leurs volumes. En particulier nous ne travaillerons qu'à la fin avec les espaces hyperboliques, et jusqu'au chapitre 12 le texte peut être utilisé pour traiter le cas d'un espace symétrique $X$ quelconque. Ces chapitres de préparation sont écrits sous la forme d'un survol structuré de résultats certes connus, mais pour beaucoup uniquement exposés dans des articles ou livres très spécialisés. Pour notre part nous nous adressons à un lecteur géomètre, sans connaissances particulières dans les domaines qui touchent aux sous-groupes arithmétiques. A ces égards l'auteur espère que cette thèse apporte un peu plus que les seuls résultats des théorèmes énoncés ci-haut.

# Chapitre 2. Groupes algébriques linéaires

Le concept de sous-groupe arithmétique sera défini en considérant certains sous-groupes dans des groupes algébriques linéaires. L'étude des sous-groupes arithmétiques est ainsi fortement liée à la théorie générale qui concerne les groupes algébriques. Nous débutons ici l'exposition de cette théorie, qui sera poursuivie avec une plus grande profondeur au chapitre 7. Les références standard sur le sujet sont [Bor91], [Hum75] et [Spr98].

N'ayant rien voulu supposer des connaissances du lecteur dans le domaine de la géométrie algébrique, nous utiliserons un language dont le degré de sophistication réduit devrait convenir au lecteur néophyte. Ainsi plusieurs de nos définitions seront introduites de façon différente (mais équivalente) de ce qui se fait habituellement dans la littérature.

## §2.1 Conventions concernant les corps

Nous admettrons le lecteur au fait des aspects élémentaires de la théorie des corps. Au besoin il peut se référer à [Mor96]. Pour autant, il nous a semblé nécessaire de réunir ici quelques conventions qui seront admises tout au long du texte.

Soient $K$ et $k$ deux corps, avec l'inclusion $k \subset K$ qui préserve la structure d'anneau. On parle alors d'une *extension de corps*, que l'on note $K|k$. Le groupe de Galois d'une telle extension sera noté $\mathrm{Gal}(K|k)$.

Pour un corps $k$ nous noterons par $\overline{k}$ une *clôture algébrique* de $k$ fixée, c'est-à-dire un corps algébriquement clos contenant $k$. On a donc $\overline{k}|k$. De plus, si $K|k$ est une extension de corps, on identifiera $\overline{k}$ avec un sous-corps de $\overline{K}$. Par exemple, considérant l'inclusion $\mathbb{Q} \subset \mathbb{R}$, et $\mathbb{C}$ comme clotûre algébrique de $\mathbb{R}$, on prendra comme clôture algébrique de $\mathbb{Q}$ le sous-corps $\overline{\mathbb{Q}} \subset \mathbb{C}$ formé des nombres algébriques.

Dans ce chapitre, $k$ désignera un corps qui est soit fini, soit de caractéristique nulle. $K$ désignera une extension de $k$, qui sera supposée algébrique si $k$ est fini. En particulier, $k$ et $K$ sont des corps qu'on qualifie de *parfait* [Mor96, def. 4.11], propriété qui par la remarque 2.2 simplifiera notre discussion. Tous les corps que nous rencontrerons dans cette thèse satisferont à ces restrictions. On relève encore que sous ces hypothèses on a en particulier qu'une extension finie $K|k$ est nécessairement *séparable* [Mor96, def. 4.7]. Dans ce cas le nombre de monomorphismes $\sigma : K \to \overline{k}$ correspond au degré $[K : k]$.

## §2.2 Variétés algébriques affines

Notons par $\mathcal{A}_k^n$ l'ensemble $\overline{k}^{\,n}$, appelé *espace affine* sur $k$ de dimension $n$. Chaque polynôme $f \in k[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ sera vu comme une fonction

$$f \quad : \quad \mathcal{A}_k^n \ \to \ \overline{k},$$

associant à $x = (x_1, \ldots, x_n) \in \mathcal{A}_k^n$ la valeur $f(x) := f(x_1, \ldots, x_n) \in \overline{k}$.

**Définition 2.1.** Une *variété (algébrique) affine sur $k$*, ou *$k$-variété affine*, est un sous-ensemble $X \subset \mathcal{A}_k^n$ (pour un certain entier $n$) de la forme :

$$X = \{(x_1, \ldots, x_n) \in \mathcal{A}_k^n \mid f_s(x_1, \ldots, x_n) = 0 \ \ \forall s \in S\},$$

où $\{f_s\}_{s \in S}$ est un ensemble de polynômes de $k[\mathrm{T}_1, \ldots, \mathrm{T}_n]$. On dit alors que $X$ est *définie* sur $k$ ou que $k$ est le *corps de définition* de $X$. Lorsque $k = \overline{k}$ on parlera simplement de *variété (algébrique) affine*.

**Remarque 2.2.** Si le corps $k$ n'est pas supposé parfait on se doit (afin de conserver une théorie suffisamment riche) d'être plus prudent et de définir la notion de $k$-variété affine d'une manière plus stricte. Mais lorsque le corps $k$ est parfait, et c'est notre cas par le choix fait en §2.1, notre définition est équivalente à la définition générale (que l'on peut trouver expliquée dans [Hum75, 34.1]).

En définissant une notion de morphisme nous faisons de l'ensemble des $k$-variétés affines une catégorie :

**Définition 2.3.** Soit $X \subset \mathcal{A}_k^n$ et $Y \subset \mathcal{A}_k^m$ deux $k$-variétés affines. Une application

$$\phi = (\phi_1, \ldots, \phi_m) \quad : \quad X \ \to \ Y$$

est un *morphisme sur $k$* (ou *$k$-morphisme*) si chacune des $m$ composantes $\phi_i : X \to \overline{k}$ peut s'écrire comme un élément de $k[\mathrm{T}_1, \ldots, \mathrm{T}_n]$. Comme pour les variétés, on parlera simplement de *morphisme* dans la situation $k = \overline{k}$.

Ces deux définitions nous permettent d'introduire plusieurs concepts concernant les variétés affines que nous développons ici. Dans ces explications, « variété » signifie « variété algébrique affine ». $X$ désigne une $k$-variété comme dans la définition 2.1 et $K|k$ est une extension qui suit les conventions de §2.1.

**2.4 Variété produit.** En plus de $X$ considérons une seconde $k$-variété $Y \subset \mathcal{A}_k^m$, définie par l'ensemble de polynômes $\{g_{s'}\}_{s' \in S'} \subset k[\mathrm{T}_1, \ldots, \mathrm{T}_m]$. La *variété produit* $X \times Y \subset \mathcal{A}_k^{m+n}$ est la variété déterminée par l'ensemble de polynômes $\{h_{ss'} \mid (s, s') \in S \times S'\} \subset k[\mathrm{T}_1, \ldots, \mathrm{T}_{n+m}]$ donnés par :

$$h_{ss'}(T_1, \ldots, T_{n+m}) := f_s(\mathrm{T}_1, \ldots, \mathrm{T}_n) \cdot g_{s'}(\mathrm{T}_{n+1}, \ldots, \mathrm{T}_{n+m}).$$

Le produit $X \times Y$ est alors une variété définie sur $k$. En ce sens, il s'agit d'un objet plus subtil que le simple produit cartésien entre $X$ et $Y$.

**2.5 Extension des scalaires.** A la variété $X$ sur $k$ est associée une variété sur l'extension $K$, obtenue par les mêmes polynômes mais en remplaçant l'espace

affine $\mathcal{A}_k^n$ par l'espace affine $\mathcal{A}_K^n$. On dit que cette nouvelle variété définie sur $K$ est obtenue par *extension des scalaires*. Si $K|k$ est algébrique a priori rien ne change : nous sommes en présence du même sous-ensemble de $\overline{k}^{\,n}$. Mais en fait, même dans cette situation, il faut garder à l'esprit que la catégorie des $K$-variétés diffère de celle des $k$-variétés. La précision du corps avec lequel on travaille peut devenir capital. Pour cette raison nous utiliserons les notations $X|k$ et $X|K$ pour distinguer la variété sur $k$ de celle obtenue par extension des scalaires.

**2.6 Points rationnels.** L'ensemble des points dits *k-rationnels* de $X$ est défini par

$$X(k) := X \cap k^n.$$

Considérant $X|K$ par extension des scalaires, l'ensemble $X(K)$ des points $K$-rationnels est alors également défini. On a en particulier $X = X(\overline{k})$. De plus si $Y$ est une $k$-variété et $\phi$ un $k$-morphisme entre $X$ et $Y$, alors $\phi(X(k)) \subset Y(k)$. Ceci montre que l'ensemble des points rationnels est invariant par isomorphisme.

**2.7 Opération du groupe de Galois.** Le groupe de Galois $\mathrm{Gal}(\overline{k}|k)$ opère sur l'espace $\mathcal{A}_k^n$, en agissant sur chacune des coordonnées. Etant défini par un ensemble de polynômes à coefficients dans $k$, la variété $X$ est stable sous cette opération : ${}^{\sigma}X = X \ \ \forall\, \sigma \in \mathrm{Gal}(\overline{k}|k)$. L'ensemble $X(k)$ est composé des points fixes de cette opération :

$$X(k) \quad = \quad \left\{ x \in X \mid {}^{\sigma}x = x \quad \forall\, \sigma \in \mathrm{Gal}(\overline{k}|k) \right\}. \tag{2.1}$$

On note encore que si $W$ est une variété affine (pas nécessairement définie sur $k$), alors ${}^{\sigma}W$ est également une variété affine.
Si $\phi : X \to Y$ est un $\overline{k}$-morphisme (pas nécessairement défini sur $k$) et $\sigma \in \mathrm{Gal}(\overline{k}|k)$, alors l'application

$$\begin{array}{rcl} {}^{\sigma}\phi & : & X \to Y \\ & & x \mapsto {}^{\sigma}(\phi(x)) \end{array} \tag{2.2}$$

est également un $\overline{k}$-morphisme, les polynômes décrivant ${}^{\sigma}\phi$ s'obtenant en appliquant $\sigma$ sur les coefficients des polynômes décrivant $\phi$. On voit alors que $\phi$ est défini sur $k$ si et seulement $\phi$ est fixé par chaque élément de $\mathrm{Gal}(\overline{k}|k)$. Dans ce cas, pour $x \in X$, on obtient :

$${}^{\sigma}(\phi(x)) \quad = \quad \phi\left({}^{\sigma}x\right). \tag{2.3}$$

**2.8 Espace tangent.** Soit $x \in X$. On définit l'*espace tangent* à $X$ au point $x$ par le sous-ensemble de $\mathcal{A}_k^n$ suivant :

$$\mathcal{T}_x X \quad := \quad \left\{ (a_1, \ldots, a_n) \in \mathcal{A}_k^n \;\middle|\; \sum_{i=0}^{n} \frac{\partial f_s}{\partial \mathrm{T}_i}(x) \cdot a_i = 0 \quad \forall s \in S \right\},$$

$\frac{\partial f_s}{\partial \mathrm{T}_i}$ désignant le poynôme obtenu par différentiation formelle de $f_s$ par rapport à la variable $\mathrm{T}_i$. On voit que $\mathcal{T}_x X$ forme un sous-espace vectoriel de $\overline{k}^{\,n}$. De

plus en considérant le sous-ensemble $(\mathcal{T}_x X)_k \subset \mathcal{T}_x X$ formé des éléments avec coordonnées dans $k$, on obtient une *$k$-structure* sur le $\overline{k}$-espace vectoriel $\mathcal{T}_x X$, i.e. le $k$-espace vectoriel $(\mathcal{T}_x X)_k$ est tel que

$$\mathcal{T}_x X \quad = \quad (\mathcal{T}_x X)_k \otimes_k \overline{k}.$$

Si l'on prend $k = \mathbb{R}$ et $x \in X(\mathbb{R})$, alors l'espace translaté $x + (\mathcal{T}_x X)_{\mathbb{R}}$ correspond bien à l'idée géométrique que l'on peut se faire d'un espace tangent. Notons tout de même que $X(\mathbb{R})$ peut posséder certains points singuliers qui peuvent l'empêcher d'en faire une sous-variété de $\mathbb{R}^n$.

**2.9 Différentielle.** Si $\phi$ est un $k$-morphisme entre $X$ et $Y$, alors on obtient par différentiation formelle $\frac{\partial \phi_k}{\partial \mathrm{T}_i}(x)$ pour chaque $x \in X$ une application $k$-linéaire $d\phi_x : \mathcal{T}_x X \to \mathcal{T}_{\phi(x)} Y$, appelée *différentielle* de $\phi$ en $x$.

**2.10 Topologie de Zariski.** Il n'est pas difficile de montrer que les variétés (sur $\overline{k}$) dans $\mathcal{A}_k^n$ forment les fermés d'une topologie, qu'on appelle *topologie de Zariski*. Chaque variété sur $k$ est alors considérée avec la topologie induite. On constate que les morphismes sont continus pour cette topologie. En considérant seulement les $k$-variétés dans $\mathcal{A}_k^n$, on obtient là aussi les fermés d'une topologie plus grossière : la *$k$-topologie (de Zariski)*. On parlera de *$k$-fermé* (resp. *$k$-ouvert*) à propos des ensembles fermés (resp. ouverts) de la $k$-topologie. Si on parle d'ensemble « fermé » ou « ouvert » on l'entend pour la $\overline{k}$-topologie. Il vaut la peine de signaler que la topologie de Zariski sur un produit de variétés ne correspond pas à la topologie produit.

**2.11 Théories absolue et relative.** Les situations les plus simples à traiter (et c'est par celles-ci qu'on commence d'ordinaire) sont celles où l'étude est menée avec un corps algébriquement clos, i.e. lorsque $k = \overline{k}$. La théorie traitant ce cas particulier est connue sous le nom de *théorie absolue*. Par opposition à la théorie absolue, on parle de *théorie relative* lorsque l'étude est menée avec la perspective d'un sous-corps strict $k \subset \overline{k}$.

## §2.3 Variétés affines et structure de groupe

**Définition 2.12.** Un *groupe algébrique (linéaire)* défini sur $k$, ou *$k$-groupe (algébrique linéaire)*, est une variété affine $G$ définie sur $k$ qui possède une structure de groupe, pour laquelle la multiplication

$$\begin{array}{rcl} G \times G & \to & G \\ (a, b) & \mapsto & ab \end{array}$$

et l'inversion

$$\begin{array}{rcl} G & \to & G \\ a & \mapsto & a^{-1} \end{array}$$

sont des $k$-morphismes.

L'adjectif « linéaire » se rapporte au fait que la variété algébrique sous-jacente au groupe algébrique considéré est une variété affine. En considérant d'autres types de variétés (e.g. les variétés dites *projectives*) on peut obtenir des groupes algébriques qui ne sont pas englobés dans cette définition. Cependant, comme nous ne considérerons que des groupes algébriques construit sur des variétés affines, nous laisserons tomber le qualificatif « linéaire ».

**Exemple 2.13.** L'espace affine $\mathcal{A}^1_k$ muni de l'addition $(a, b) \mapsto a + b$ est un groupe algébrique, appelé *groupe additif* (sur $k$) est noté par le symbole $\mathbf{G}_{\mathrm{a}}$.

**Exemple 2.14.** Soit dans $\mathcal{A}^2_k$ la variété définie par le polynôme $f(\mathrm{X}, \mathrm{Y}) = \mathrm{XY} - 1$. Munie de la loi de composition suivante : $(a, \frac{1}{a}) \cdot (b, \frac{1}{b}) := (ab, \frac{1}{ab})$, cette variété forme le *groupe multiplicatif*, noté $\mathbf{G}_{\mathrm{m}}$. Ce groupe correspond en fait au groupe multiplicatif $\overline{k}^{\times}$, grâce à l'isomorphisme $a \in k^{\times} \mapsto (a, \frac{1}{a})$. Avec notre définition de groupe algébrique il nous est nécessaire de voir $\mathbf{G}_{\mathrm{m}}$ comme un sous-ensemble de $\mathcal{A}^2_k$, l'ensemble $\overline{k}^{\times}$ ne pouvant s'exprimer comme les zéros de polynômes à une seule variable. L'inversion dans $\mathbf{G}_{\mathrm{m}}$ est donnée par $(a, \frac{1}{a}) \mapsto (\frac{1}{a}, a)$, i.e. par les polynômes $\phi_1(\mathrm{X}, \mathrm{Y}) = \mathrm{Y}$ et $\phi_2(\mathrm{X}, \mathrm{Y}) = \mathrm{X}$ (en reprenant la notation de la définition 2.3).

La définition 2.12, liant structure de groupe et structure de variété algébrique a des implications très fortes :

**Proposition 2.15.** *Soit $G$ un $k$-groupe algébrique.*

1. *La structure de groupe de $G|k$ s'étend de façon unique à une structure de groupe sur $G|K$ pour laquelle $G|K$ est un groupe algébrique.*
2. *$G(k)$ est un groupe (pour la loi de groupe sur $G$).*

Idée de la preuve. On peut voir que le groupe $G|K$ correspond à l'adhérence de $G(\overline{k})$ dans $\mathcal{A}^n_K$ (pour la $\overline{K}$-topologie). Par densité de $G(\overline{k})$ dans $G|K$, on voit alors que les morphismes de multiplication et d'inversion étendu à $G|K$ préservent les axiomes de groupe sur $G|K$.

Comme les $k$-morphismes conservent les points $k$-rationnels, il suit que $G(k)$ est bien fermé pour la multiplication et l'inversion. Il suffit donc de voir que $1 \in G(k)$. Par (2.3) appliqué au $k$-morphisme de multiplication, on a que ${}^{\sigma}(1)({}^{\sigma}1) = {}^{\sigma}1$ pour chaque $\sigma \in \mathrm{Gal}(\overline{k}|k)$, ce qui à l'aide de (2.1) prouve que $1 \in G(k)$. □

**Exemple 2.16.** Soit $k$ un corps de caractéristique $\neq 2$, et soit $f$ une forme quadratique à coefficients dans $k$, de dimension $n$. Alors $f$ détermine une forme bilinéaire sur $k^n$, et l'on notera par $\mathbf{V}_f$ cet *espace quadratique*. Par extension on obtient un espace quadratique $\mathbf{V}_f \otimes_k \overline{k}$. Le *groupe orthogonal* $\mathrm{O}_f$ des matrices $n \times n$ à coefficients dans $\overline{k}$ qui représentent des transformations orthogonales de $\mathbf{V}_f \otimes \overline{k}$ est un $k$-groupe algébrique (le fait de préserver la forme bilinéaire s'exprime à l'aide d'équations polynomiales). Son sous-groupe $\mathrm{SO}_f := \mathrm{O}_f \cap \mathrm{SL}_n$, le *groupe spécial orthogonal*, est également un $k$-groupe. $\mathrm{O}_f(k)$ ($\mathrm{SO}_f(k)$) est le groupe des transformations (spéciales) orthogonales de $\mathbf{V}_f$.

**Remarque 2.17.** Les exemples liés aux formes quadratiques vont nous accompagner tout au long de cette thèse. Quand il en sera question, on admettra toujours les conventions suivantes :

- le corps sur lequel sera défini la forme quadratique sera de caractéristique $\neq 2$ ;
- toute forme quadratique sera supposée *non dégénérée* (c'est-à-dire que seul le sous-espace $\{0\}$ est orthogonal à tout $\mathbf{V}_f$)

Le lecteur peut se référer à [O'M63] pour la théorie générale des formes quadratiques.

**Définition 2.18.** Les morphismes dans la catégorie des $k$-groupes algébriques sont constitués des applications qui sont à la fois homomorphismes de groupes et $k$-morphismes entre $k$-variétés. On les appelera *homomorphismes algébriques sur* $k$ ou *$k$-homomorphismes (algébriques)*. On parle simplement d'*homomorphisme algébrique* lorsque $k = \overline{k}$.

La notion d'isomorphisme entre deux $k$-groupes algébriques $G$ et $H$ est alors claire : $G \cong H$ si et seulement si, par définition, il existe deux homomorphismes sur $k$ :

$$\phi : G \to H \quad \text{et} \quad \psi : H \to G$$

tels que $\phi \circ \psi = \mathrm{id}|_H$ et $\psi \circ \phi = \mathrm{id}|_G$. On dit que $\phi$ et $\psi$ sont des *$k$-isomorphismes* et que $G$ et $H$ sont *$k$-isomorphes*. Deux groupes non isomorphes sur $k$ peuvent le devenir sur l'extension $K|k$, i.e. après extension des scalaires.

**Définition 2.19.** Soit $G$ un $k$-groupe algébrique et considérons que l'extension de corps $K|k$ est fixée. Un $k$-groupe algébrique $H$ est appelé une *$k$-forme* de $G$ si $H$ est $K$-isomorphe à $G$, c'est-à-dire si $G|K$ et $H|K$ sont isomorphes comme $K$-groupes.

**Exemple 2.20.** Il existe une notion naturelle d'isomorphisme entre deux espaces quadratiques $\mathbf{V}_f$ et $\mathbf{V}_g$ (donnés par deux formes $f$ et $g$ sur $k$ de même dimension). Si $\mathbf{V}_f \cong \mathbf{V}_g$ on dit aussi que $f$ et $g$ sont *équivalentes*. Dans ce cas on a que $\mathrm{SO}_f$ et $\mathrm{SO}_g$ sont $k$-isomorphes. Commes toutes les formes quadratiques sur $\overline{k}$ d'une même dimension sont équivalentes entre elles, on a que si $f$ et $g$ sont de même dimension, nécessairement $\mathrm{SO}_f$ est une $k$-forme de $\mathrm{SO}_g$.

## §2.4 Sous-groupes algébriques

**Définition 2.21.** Soit $G$ un $k$-groupe algébrique. Un *$k$-sous-groupe (algébrique)* est un sous-groupe $H < G$ qui est une $k$-variété algébrique. En d'autres termes il s'agit d'un sous-groupe $k$-fermé de $G$. Pour un $\overline{k}$-sous-groupe on parle de *sous-groupe algébrique*.

Un premier exemple de sous-groupe algébrique est donné à l'aide de la topologie de Zariski :

**Définition 2.22.** Un groupe algébrique est dit *connexe* s'il est connexe pour la topologie de Zariski. On note par $G^\circ$ la composante connexe de l'unité du groupe $G$.

**Proposition 2.23.** *Soit $G$ un groupe algébrique. La composante connexe $G^\circ$ est un sous-groupe normal fermé de $G$.*

PREUVE. La continuité de la muliplication et de l'inversion montre que $G^\circ$ est bien un sous-groupe de $G$. De plus, la composante connexe $G^\circ$ est un ensemble fermé (toujours vrai dans un espace topologique) de $G$, et donc bien un sous-groupe algébrique. Par continuité de l'opération de conjugaison de $G$ sur $G^\circ$, on voit que ce dernier est normal dans $G$. □

Soit $H$ un $k$-sous-groupe connexe du $k$-groupe $G$. Le *centralisateur* $Z_G(H)$ de $H$ dans $G$ s'écrit par définition comme :

$$Z_G(H) \quad = \quad \left\{ g \in G \mid gxg^{-1} = x \quad \forall\, x \in H \right\}. \tag{2.4}$$

Pour chaque $x \in H$ l'égalité $gxg^{-1} = x$ correspond à un ensemble d'équations polynomiales (à coefficients dans $\overline{k}$). On constate donc que $Z_G(H)$ est un sous-groupe algébrique de $G$. On peut également considérer le *normalisateur* de $H$ dans $G$ :

$$N_G(H) \quad := \quad \left\{ g \in G \mid gHg^{-1} \subset H \right\}. \tag{2.5}$$

Bien que cela soit un peu moins évident à voir, il s'agit là aussi d'un sous-groupe algébrique (sur $\overline{k}$). Le lecteur peut consulter [Hum75, 8.2] pour la preuve.

## §2.5 Linéarisation des groupes algébriques

Le groupe $\mathrm{SL}_n$ défini par le polynôme

$$\det(\mathrm{T}_{ij}) - 1$$

est un $k$-groupe algébrique dans $\mathcal{A}_k^{n^2}$ pour la multiplication matricielle. Ici les variables utilisées pour décrire les polynômes sur $\mathcal{A}_k^{n^2}$ sont indexés par des couples, afin de faciliter la vision matricielle. Le groupe linéaire général est défini par

$$\det(\mathrm{T}_{ij}) \quad \neq \quad 0.$$

Mais cette inégalité ne décrit pas un ensemble fermé de $\mathcal{A}_k^{n^2}$. La solution est de faire comme dans l'exemple 2.14, où $\overline{k}^\times$ était plongé dans $\mathcal{A}_k^2$. On considère alors $\mathcal{A}_k^{n^2+1}$ avec son algèbre de polynômes $\overline{k}[\mathrm{T}_{11}, \mathrm{T}_{12}, \ldots, \mathrm{T}_{nn}, \mathrm{Y}]$. Le $k$-groupe algébrique $\mathrm{GL}_n$ est alors défini par l'ensemble des solutions dans $\mathcal{A}_k^{n^2+1}$ de

$$\det(\mathrm{T}_{ij}) \cdot \mathrm{Y} \quad = \quad 1.$$

Dans $\mathrm{GL}_n$ la variable additionnelle Y correspond donc à l'inverse du déterminant. De la sorte l'inversion matricielle est un $k$-morphisme dans $\mathrm{GL}_n$ et on a bien une structure de $k$-groupe algébrique. Pour $n = 1$ on retrouve le groupe multiplicatif : $\mathrm{GL}_1 = \mathbf{G}_\mathrm{m}$. On se permettra de noter les éléments de $\mathrm{GL}_n$ sous leur forme habituelle : comme matrices carrées à coefficients dans $\overline{k}$. En fait chaque groupe algébrique linéaire est matriciel [Bor91, prop. 1.10] :

**Théorème 2.24.** *Soit $G$ un groupe algébrique sur $k$. Alors il existe un $k$-sous-groupe algébrique $H < \mathrm{GL}_n$ (pour un certain $n \in \mathbb{N}$) avec un $k$-isomorphisme $\phi : G \to H$.*

L'application $\phi$ du théorème sera appelée un *plongement matriciel* de $G$. On pourra donc toujours munir un groupe algébrique d'un tel plongement. Grâce à la notion de plongement on définit :

**Définition 2.25.** Un élément $g$ d'un groupe algébrique $G$ est dit *unipotent* s'il existe un plongement matriciel $\phi : G \to \mathrm{GL}_n$ pour lequel la matrice $\phi(g)$ est de la forme triangulaire

$$\phi(g) \quad = \quad \begin{pmatrix} 1 & * & * \\ & \ddots & * \\ 0 & & 1 \end{pmatrix}$$

**Exemple 2.26.** Le groupe additif $\mathbf{G}_{\mathrm{a}}$ possède le plongement matriciel suivante :

$$x \in \mathbf{G}_{\mathrm{a}} \quad \mapsto \quad \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

Ainsi tous éléments de $\mathbf{G}_{\mathrm{a}}$ sont unipotents.

## §2.6 Restriction des scalaires

Le concept qui fait l'objet de ce paragraphe n'apparaît pas comme un sujet incontournable de la théorie des groupes algébriques linéaires. Il s'avère cependant très utile lors de la discussion des sous-groupes arithmétiques. Son introduction est due à Weil [Wei82, §1.3] dans le cadre plus général des variétés algébriques. Nous allons pour notre part suivre la vision plus concrète que propose [PR94, 2.1.2].

Nous commençons par un travail au niveau des corps. Nous supposons dans tout ce paragraphe que l'extension $K|k$ est finie, de degré $d := [K : k]$. On choisit une base $\omega_1, \ldots, \omega_d$ de $K|k$. Pour chaque $a \in K$, l'application

$$\begin{array}{ccc} K & \to & K \\ x & \mapsto & ax \end{array}$$

est un endomorphisme $k$-linéaire de $K$, et nous notons par $\rho(a)$ sa matrice correspondante par rapport à la base choisie. $\rho(K)$ est alors une sous-algèbre de $\mathrm{Mat}_{d\times d}(k)$, isomorphe à $K$. Comme sous-espace vectoriel, $\rho(K)$ s'écrit certainement comme noyau d'un endomorphisme $k$-linéaire que nous notons par $\Phi$. Etendons $\Phi$ à $\mathrm{Mat}_{d\times d}(\overline{k})$ (c'est-à-dire en considérant $\Phi \otimes \mathrm{id}_{\overline{k}}$) et prenons le noyau de cette application. On obtient alors une sous-algèbre de $\mathrm{Mat}_{d\times d}(\overline{k})$ qui par construction est isomorphe à $K \otimes_k \overline{k}$. Ce produit tensoriel, considéré comme $\overline{k}$-algèbre, se décrit de la façon suivante :

**Proposition 2.27.** *L'application linéaire donnée par*

$$\begin{array}{ccc} K \otimes_k \overline{k} & \to & \overline{k}^d \\ a \otimes 1 & \mapsto & (\sigma a)_\sigma \end{array}$$

*où les composantes du vecteur $(\sigma a)_\sigma$ sont indexées par les $d$ monomorphismes $\sigma : K \to \overline{k}$, est un isomorphisme de $\overline{k}$-algèbres.*

**Remarque 2.28.** On note par $\sigma x$ ou $\sigma(x)$ l'image de $x \in K$ par $\sigma$. Le symbole $\sigma$ est aussi utilisé dans ce texte pour les éléments du groupe de Galois $\mathrm{Gal}(\overline{k}|k)$. Dans ce contexte l'action de $\sigma$ sur $x \in \overline{k}$ est notée ${}^{\sigma}x$ (cf. 2.7).

Prenons à présent un groupe algébrique $G$ défini sur $K$. Nous allons utiliser le matériel présenté ci-dessus pour associer à $G$ un groupe défini sur $k$. Pour cela identifions (grâce au théorème 2.24) $G$ avec un sous-groupe $K$-fermé de $\mathrm{GL}_n$, et supposons que $\{f_s\}$ soit l'ensemble de polynômes qui annulent $G$. Considérons le groupe $\mathrm{GL}_{nd}$, dont on écrit les éléments à l'aide des coordonnées matricielles :

$$\left(\left(x_{ij}^{\alpha\beta}\right)_{\alpha,\beta}\right)_{i,j},$$

où $\alpha, \beta = 1, \ldots, d$ et $i, j = 1, \ldots, n$. On peut considérer sur chaque bloc de variables $(x_{ij}^{\alpha\beta})_{\alpha,\beta}$ ($i, j$ fixés) l'application linéaire $\Phi$ introduite plus haut. Pour $i, j$ fixés on peut noter par $\Phi_{ij}$ cette application. Ainsi l'ensemble des zéros communs de $\{\Phi_{ij}\}$ dans $\mathrm{GL}_{nd}(k)$ correspond par l'application $\rho$ à $\mathrm{GL}_n(K)$. On complète la construction comme suit. Pour chaque polynôme $f_s$ qui définit $G$ on considère le polynôme matricielle $\rho(f_s)$ qu'on obtient en appliquant $\rho$ sur chaque coefficient de $f_s$. La réunion $\{\rho(f_s)\} \cup \{\Phi_{ij}\}$ détermine un ensemble de polynômes sur $k$ qui donne un sous-groupe $k$-fermé de $\mathrm{GL}_{nd}$, noté $\mathbf{R}_{K|k}(G)$. On notera par le même symbole $\rho$ l'application

$$\rho \quad : \quad G(K) \to \mathbf{R}_{K|k}(G)(k) \tag{2.6}$$

qui envoie $(a_{ij})_{i,j}$ sur $(\rho(a_{ij}))_{i,j}$.

Le groupe $\mathbf{R}_{K|k}(G)$ est dit obtenu par *restriction des scalaires* à partir de $G$. A $k$-isomorphisme près il ne dépend ni du choix du plongement matriciel choisi pour $G$, ni du choix de la base $\omega_1, \ldots, \omega_d$ de $K$ sur $k$. Nous donnons dans la proposition suivante les propriétés caractéristiques que possède $\mathbf{R}_{K|k}$. Elles suivent immédiatement de la construction.

**Proposition 2.29.** *Soit $H := \mathbf{R}_{K|k}(G)$ le groupe obtenu par restriction des scalaires à partir du $K$-groupe $G$. Alors :*

1. *$\rho : G(K) \to H(k)$ est un isomorphisme.*
2. *On a un isomorphisme défini sur $\overline{k}$ :*

$$H \quad \cong \quad \prod_{\sigma} G^{\sigma}$$

*où $\sigma$ parcourt les $d$ $k$-monomorphismes $\sigma : K \to \overline{k}$ et $G^{\sigma} := \sigma(G)$.*

**Remarque 2.30.** La partie *2* doit se voir comme une généralisation de la proposition 2.27, qui correspond au cas $G = \mathbf{G}_{\mathrm{a}}$.

**Exemple 2.31.** Soit $K = k(\sqrt{\alpha})$ une extension quadratique d'un corps $k$, et considérons $\mathbf{G}_{\mathrm{m}}$ comme $K$-groupe. On choisit $\{1, \sqrt{\alpha}\}$ comme base de $K|k$. Les $k$-points de $\mathbf{R}_{K|k}(\mathbf{G}_{\mathrm{m}})$ correspondent à $K^{\times}$ par l'isomorphisme :

$$a + \sqrt{\alpha}b \in K^{\times} \quad \mapsto \quad \begin{pmatrix} a & b\alpha \\ b & a \end{pmatrix}.$$

**Remarque 2.32.** L'exemple 2.31 est quelque peu trivial dans le sens où $\mathbf{G}_{\mathrm{m}}$ peut déjà être vu comme un groupe sur $k$. On ne tire donc pas pleinement parti de la possibilité qu'offre le foncteur $\mathbf{R}_{K|k}$ d'associer un $k$-groupe à un groupe qui ne serait « que défini sur $K$ ». Cet exemple permet cependant de remarquer que la restriction des scalaires n'est pas l'opération inverse de l'extension des scalaires vue en 2.5 : la proposition 2.29 (partie 2) montre en effet que le $k$-groupe $\mathbf{R}_{K|k}(\mathbf{G}_{\mathrm{m}}|K)$ est isomorphe au produit $\mathbf{G}_{\mathrm{m}} \times \mathbf{G}_{\mathrm{m}}$, et non à $\mathbf{G}_{\mathrm{m}}$.

## §2.7 Algèbre de Lie et représentation adjointe

Nous allons nous intéresser dans ce paragraphe à l'espace tangent $\mathcal{T}_e G$ d'un $k$-groupe $G$, où $e = 1$ désigne l'élément neutre. Nous définissons la *dimension* de $G$, notée $\dim(G)$ comme étant la dimension du $\overline{k}$-espace vectoriel $\mathcal{T}_e G$. Ceci correspond donc à la dimension sur $k$ de $(\mathcal{T}_e G)_k$. Supposons ici que $G$ est de dimension $n$.

Nous voulons introduire sur $\mathcal{T}_e G$ une structure d'algèbre de Lie. Pour cela munissons $G$ d'un plongement matriciel dans $\mathrm{GL}_N$ (pour un certain entier $N$), c'est-à-dire qu'on identifie $G$ avec son image par un tel plongement. L'espace tangent $\mathcal{T}_e G$ se trouve alors être un sous-espace vectoriel de dimension $n$ de l'ensemble des matrices carrées $\mathrm{Mat}_{N\times N}(\overline{k})$. Introduisons alors sur $\mathcal{T}_e G$ le produit

$$[X, Y] \quad := \quad XY - YX,$$

où la multiplication $XY$ est donnée par la multiplication matricielle. On vérifie que ce crochet de Lie est bien fermé sur $\mathcal{T}_e G$. Nous noterons par le symbole habituelle $\mathfrak{g}$ l'espace $\mathcal{T}_e G$ muni de cette structure d'*algèbre de Lie*, et par $\mathfrak{g}_k$ l'espace $(\mathcal{T}_e G)_k$ muni du crochet issu de $\mathfrak{g}$ par restriction. On a alors une $k$-structure sur $\mathfrak{g}$ :

$$\mathfrak{g} = \mathfrak{g}_k \otimes_k \overline{k}.$$

Toutes ces définitions sont indépendantes du plongement matriciel choisi pour le $k$-groupe $G$ : si $\phi : G \to H$ est un $k$-isomorphisme entre groupes matriciels, la différentielle $d\phi_e : \mathfrak{g}_k \to \mathfrak{h}_k$ est un isomorphisme d'algèbre de Lie.

**Exemple 2.33.** Soit $G$ un $k$-groupe avec $k \subset \mathbb{R}$. Alors par la proposition 2.15 l'ensemble $G(\mathbb{R})$ est un groupe. Les fonctions qui définissent $G$ ou $G(\mathbb{R})$ sont des polynômes, et sont donc différentiables. Ceci permet de montrer que $G(\mathbb{R})$ possède en fait une structure de groupe de Lie. L'algèbre de Lie de $G(\mathbb{R})$ s'identifie alors à $\mathfrak{g}_{\mathbb{R}}$. En particulier la dimension de $G$ est égale à la dimension du groupe de Lie $G(\mathbb{R})$.

Continuons de voir $G$ comme un groupe matriciel. Soit en plus $H$ un sous-groupe algébrique de $G$. Le groupe $H$ opère sur $\mathfrak{g}$ de la façon suivante : si $h \in H$, on définit

$$\mathrm{Ad}(h)X \quad := \quad hXh^{-1}. \tag{2.7}$$

L'application $\mathrm{Ad}(h) : \mathfrak{g} \to \mathfrak{g}$ est alors un isomorphisme de $\mathfrak{g}$ qui préserve le crochet de Lie. Cette opération est appelée *opération adjointe* de $H$ sur $\mathfrak{g}$.

## §2.8 Simplicité et semi-simplicité

On rappele qu'un groupe de Lie est dit *semi-simple* si son algèbre de Lie est semi-simple, c'est-à-dire si celle-ci n'est pas abélienne et ne possède aucun idéal non-trivial. La définition de semi-simplicité d'un groupe algébrique est introduite directement au niveau du groupe.

**Définition 2.34.** Soit $G$ un groupe algébrique défini sur $k$.

1. Si $G$ ne possède aucun sous-groupe algébrique connexe normal et résoluble autre que $\{1\}$, alors $G$ est appelé *semi-simple*.
2. $G$ est dit *$k$-simple* s'il ne possède pas de $k$-sous-groupe connexe normal propre. Si $G|\overline{k}$ est $\overline{k}$-simple, on dit que $G$ est *absolument simple*.

Il est clair par définition que « absolument simple » implique à la fois « $k$-simple » et « semi-simple ». Pour le cas $k = \mathbb{R}$ on retrouve la notion exposée précédemment [Hum75, 13.5] :

**Proposition 2.35.** *Soit $G$ un $\mathbb{R}$-groupe algébrique. Alors $G$ est semi-simple si et seulement si le groupe de Lie $G(\mathbb{R})$ est semi-simple.*

**Exemple 2.36.** Pour n'importe quel corps $k$, le $k$-groupe $\mathrm{SL}_2$ est absolument simple. Il s'agit d'un groupe algébrique connexe.

**Exemple 2.37.** Soit $f$ une forme quadratique de dimension $n \geq 3$. Le groupe $\mathrm{SO}_f$ est connexe et, pour autant que $n \neq 4$, il est absolument simple. Pour $n = 4$ le groupe $\mathrm{SO}_f$ est semi-simple, sans être absolument simple. Le groupe $\mathrm{O}_f$ n'est par contre pas semi-simple ($n$ quelconque).

## §2.9 Quotients et isogénies

Si $G$ est un groupe algébrique et que $H < G$ est un sous-groupe algébrique normal, il est possible d'identifier de façon naturelle le quotient $G/H$ avec un groupe algébrique, dont la dimension vaut

$$\dim(G) - \dim(H).$$

On s'autorisera donc à considérer sur $G/H$ la structure de groupe algébrique issue de l'identification naturelle existante. Le lecteur peut trouver dans [Hum75, Ch. IV] une méthode pour expliciter la structure de groupe algébrique sur le quotient $G/H$. Nous nous contentons d'expliquer ici certaines propriétés de $G/H$ pour deux cas particuliers.

Par la proposition 2.23 le sous-groupe $G^\circ$ d'un groupe algébrique $G$ est normal et fermé. On peut donc considérer le quotient $G/G^\circ$. On a alors :

**Proposition 2.38.** *Le groupe $G/G^\circ$ est fini.*

Idée de la preuve. Le groupe $G^\circ$ possède en fait la même dimension que $G$. Le quotient $G/G^\circ$ est donc de dimension 0. Or un groupe algébrique de dimension 0 est nécessairement fini. Pour se convaincre de ce fait on peut imaginer la situation où le groupe est inclus dans $\mathcal{A}^1_k$ : dans ce cas le groupe est donné par un polynôme non-nul à une seule variable. Or un tel polynôme possède

seulement un nombre fini de zéros. Ceci se généralise pour n'importe quel groupe de dimension 0 (en fait déjà au niveau des variétés algébriques). □

Le deuxième sous-groupe que nous voulons considérer est le *centre* $Z_G$ du $k$-groupe $G$ :

$$Z_G \quad := \quad Z_G(G). \tag{2.8}$$

Comme il s'agit d'un centralisateur, nous savons que $Z_G$ est un sous-groupe fermé de $G$. En fait, il s'agit même d'un sous-groupe $k$-fermé [Spr98, 12.1.7]. Or il est vrai en général que si le sous-groupe $H < G$ est défini sur $k$, alors $G/H$ est un $k$-groupe. Le groupe algébrique

$$\overline{G} \quad := \quad G/Z_G \tag{2.9}$$

est donc défini sur $k$. Le groupe $\overline{G}$ s'identifie (comme groupe abstrait) naturellement avec le groupe des automorphismes internes de $G$, en associant à $g \in G$ l'homomorphisme algébrique de conjugaison :

$$x \in G \quad \mapsto \quad g^{-1}xg. \tag{2.10}$$

De plus, la projection naturelle

$$\pi \quad : \quad G \to \overline{G} \tag{2.11}$$

est un $k$-homomorphisme. Pour autant que $k$ soit de caractéristique nulle, la structure de variété algébrique de $\overline{G}$ est même compatible avec la nature des automorphismes internes :

**Proposition 2.39.** *Supposons que $k$ est de caractéristique nulle. Alors $\pi(g) \in \overline{G}(k)$ exactement lorsque l'automorphisme* (2.10) *est défini sur $k$.*

Grâce à cette propriété nous pouvons apporter une précision essentielle sur l'application $\pi$. Bien que $\pi$ est par définition surjective, sa restriction :

$$\pi \quad : \quad G(k) \to \overline{G}(k)$$

n'est pas nécessairement surjective. Cette constatation aura un rôle important dans la suite. Voici un contre-exemple :

**Exemple 2.40.** Considérons le $\mathbb{Q}$-groupe $G := \mathrm{SL}_2$. Son centre vaut $\{\pm I\}$, où $I$ est la matrice identité. Pour $\alpha \in \mathbb{Q}^\times$, l'élément

$$g \quad = \quad \begin{pmatrix} \sqrt{\alpha} & 0 \\ 0 & \sqrt{\alpha}^{-1} \end{pmatrix}$$

est envoyé sur l'automorphisme interne

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} a & b/\alpha \\ \alpha c & d \end{pmatrix}$$

qui est clairement défini sur $\mathbb{Q}$. Par la proposition 2.39 on a donc $\pi(g) \in \overline{G}(\mathbb{Q})$. Or si $\alpha$ n'est pas un carré, ni $g$ ni $-g$ n'est élément de $G(\mathbb{Q})$.

Supposons maintenant que $G$ soit semi-simple. Par définition de la semi-simplicité il suit que $Z_G^\circ = 1$. De la proposition 2.38 on en déduit que $Z_G$ est un groupe fini. L'application $\pi$ possède donc un noyau fini et rentre dans le cadre de la définition suivante :

**Définition 2.41.** Soit $G$ et $H$ deux $k$-groupes. Un $k$-homomorphisme $\pi : G \to H$ est une *$k$-isogénie* si $\pi$ est surjective et son noyau $\ker(\pi)$ est fini. On parle simplement d'*isogénie* pour la situation $k = \overline{k}$.

Jusqu'à la fin de ce paragraphe, nous allons travailler avec des corps de caractéristique nulle. En caractéristique positive les définitions que nous allons donner doivent être adaptées, en remplaçant la notion d'isogénie par celle d'*isogénie centrale* [Bor91, 22.3]. Tout comme dans le cas des groupes de Lie, on peut identifier le groupe $\overline{G}$ associé au groupe semi-simple $G$ avec l'image $\mathrm{Ad}(G)$ par sa représentation adjointe. Ceci explique la définition qui suit :

**Définition 2.42.** Soit $G$ un groupe semi-simple défini sur un corps $k$ de caractéristique nulle. Le $k$-groupe $\overline{G}$ est appelé *groupe adjoint* de $G$. Si $G$ ne possède pas de centre (i.e. $Z_G = 1$) on dit que $G$ est *adjoint*.

Un groupe semi-simple adjoint possède la propriété de ne pas revêtir par isogénie non triviale un autre groupe algébrique. A l'inverse de cette situation on trouve :

**Définition 2.43.** Un groupe algébrique semi-simple $G$ sur un corps de caractéristique nulle est dit *simplement connexe* s'il est connexe et si chaque isogénie

$$\pi \quad : \quad H \to G$$

entre un groupe algébrique $H$ et $G$ est un isomorphisme.

On verra au chapitre 6 que les groupes simplement connexes possèdent des propriétés fort intéressantes. Il sera ainsi pour nous essentiel de ramener un problème qui concerne un groupe semi-simple quelconque à un problème dans un groupe simplement connexe. Pour cela nous utiliserons le résultat suivant [Tit66, prop. 2] :

**Proposition 2.44.** *Soit $H$ un $k$-groupe semi-simple et connexe ($k$ de caractéristique nulle). Alors il existe un $k$-groupe semi-simple simplement connexe $G$ et une $k$-isogénie*

$$\pi \quad : \quad G \to H.$$

**Exemple 2.45.** Le $k$-groupe orthogonal $\mathrm{SO}_f$ attaché à une forme quadratique (de dimension $\geq 3$) n'est pas simplement connexe (cf. explication donnée dans la remarque 2.49). Son revêtement algébrique simplement connexe est noté $\mathrm{Spin}_f$, et appelé *groupe des spineurs* de $f$. Pour une définition de $\mathrm{Spin}_f$ on consultera [Sch85, Ch. 9 §3]. La $k$-isogénie

$$\mathrm{Spin}_f \quad \to \quad \mathrm{SO}_f$$

est alors un revêtement double.

## §2.10 Topologie des groupes réels

Nous revenons à la situation de l'exemple 2.33 où $G$ est un groupe défini sur $\mathbb{R}$. La topologie que porte le groupe de Lie $G(\mathbb{R})$ est bien entendu la topologie induite par la topologie usuelle (donnée par la métrique euclidienne) sur $\mathbb{R}^N$. Celle-ci se différencie fortement de la topologie de Zariski sur $G$. Il faut donc prendre garde de bien faire la distinction entre $G(\mathbb{R})^\circ$ et $G^\circ(\mathbb{R})$. En particulier, même si $G$ est connexe, ce dernier ensemble $G^\circ(\mathbb{R})$ n'est pas forcément connexe pour la topologie usuelle, comme le montre l'exemple suivant :

**Exemple 2.46.** Considérons la forme quadratique réelle :

$$f(x_0, \ldots, x_n) \quad = \quad -x_0^2 + x_1^2 + \cdots + x_n^2$$

et son groupe spécial orthogonal $\mathrm{SO}_{(n,1)} := \mathrm{SO}_f$. Le groupe des points réels

$$\mathrm{SO}(n,1) \quad := \quad \mathrm{SO}_{(n,1)}(\mathbb{R})$$

opère alors continûment sur l'*hyperboloïde* $\left\{x \in \mathbb{R}^{n+1} \mid f(x) = -1\right\}$, et cette opération en permute les deux composantes connexes. Ceci montre que $\mathrm{SO}(n,1)$ n'est pas connexe, alors même que $\mathrm{SO}_{(n,1)}$ est un groupe algébrique connexe. Notons qu'en utilisant comme modèle pour $\mathbb{H}^n$ la partie supérieure de hyperboloïde (éléments de coordonnée $x_0 > 0$), on identifie $\mathrm{SO}(n,1)^\circ$ avec le groupe $\mathrm{Isom}^+(\mathbb{H}^n)$ des isométries hyperboliques préservant l'orientation.

La proposition suivante pose certaines limites au phénomène du dernier exemple. On trouve sa démonstration dans [PR94, §3.1 : corol. 1].

**Proposition 2.47.** *Soit $G$ un $\mathbb{R}$-groupe. Alors le groupe $G(\mathbb{R})$ possède un nombre fini de composantes connexes. De plus, si $G$ est connexe et $G(\mathbb{R})$ est compact, alors $G(\mathbb{R})$ est connexe.*

On doit également faire attention lorsqu'on parle de groupe « simplement connexe ». En effet, le $\mathbb{R}$-groupe $\mathrm{SL}_2$ est simplement connexe (au sens de la définition 2.43), et pourtant $\mathrm{SL}_2(\mathbb{R})$ n'est pas simplement connexe (au sens topologique). Pour avoir une bonne correspondance entre les deux notions, il faut en fait considérer les points complexes : $\mathrm{SL}_2(\mathbb{C})$ est bien simplement connexe. Il y a toutefois quelque chose d'intéressant à dire sur les points réels d'un groupe algébrique simplement connexe [Mar91, Ch. I §2.3 : remark 2] :

**Proposition 2.48.** *Soit $G$ un $\mathbb{R}$-groupe semi-simple simplement connexe. Alors $G(\mathbb{R})$ est connexe.*

**Remarque 2.49.** Soit $f$ une forme quadratique définie sur un corps $k \subset \mathbb{R}$. Comme toutes les formes quadratiques d'une dimension fixée sont équivalentes sur $\mathbb{C}$, le groupe $\mathrm{SO}_f|\mathbb{R}$ est une $\mathbb{R}$-forme de $\mathrm{SO}_{(n,1)}$ pour un certain $n$ (cf. exemple 2.16). La propriété « simplement connexe » étant une notion absolue (i.e. ne dépend que du groupe considéré sur la clôture algébrique), on en conclut par l'exemple 2.46 que $\mathrm{SO}_f$ n'est pas simplement connexe. Comme il en est déjà

question dans l'exemple 2.45, ceci reste en fait vrai pour un corps quelconque (de caractéristique $\neq 2$). De façon similaire à $\mathrm{SO}(n,1)$, on définit le groupe de Lie suivant :

$$\mathrm{Spin}(n,1) \quad := \quad \mathrm{Spin}_{(n,1)}(\mathbb{R}). \tag{2.12}$$

Le phénomène observé dans l'exemple 2.40 apparaît à nouveau : l'application continue $\mathrm{Spin}(n,1) \to \mathrm{SO}(n,1)$ n'est pas surjective (l'image devrait être connexe).

# Chapitre 3. Réseaux arithmétiques

Nous en venons maintenant à l'étude du sujet annoncé au paragraphe §1.2 : les réseaux construits comme sous-groupes arithmétiques. Parmi les textes qui contiennent des éléments qui introduisent à cette matière on peut citer [Bor69], [PR94], [OV00], [Rag72] et [Zim84].

## §3.1 Sous-groupes arithmétiques des $\mathbb{Q}$-groupes

Soit $G$ un groupe algébrique défini sur $\mathbb{Q}$. Pour un certain plongement de $G$ dans $\mathrm{GL}_N$, on pose

$$G(\mathbb{Z}) := \mathrm{GL}_N(\mathbb{Z}) \cap G,$$

où $\mathrm{GL}_N(\mathbb{Z})$ est le groupe des matrices entières inversibles. Cette définition dépend du plongement choisi pour $G$, comme le montre l'exemple suivant.

**Exemple 3.1.** Plongeons le groupe additif $\mathbf{G}_\mathrm{a}$ dans $\mathrm{GL}_2(\overline{\mathbb{Q}})$ des deux façons suivantes :

$$\begin{aligned} x \in \overline{\mathbb{Q}} &\mapsto \begin{pmatrix} 1 & \frac{x}{2} \\ 0 & 1 \end{pmatrix} \\ x \in \overline{\mathbb{Q}} &\mapsto \begin{pmatrix} 1 & \frac{x}{3} \\ 0 & 1 \end{pmatrix} \end{aligned}$$

De la sorte $\mathbf{G}_\mathrm{a}(\mathbb{Z})$ correspond à $2\mathbb{Z}$ dans le premier cas, et à $3\mathbb{Z}$ dans le second.

La définition de $G(\mathbb{Z})$ n'est donc pas intrinsèque au groupe $G$. Cependant l'exemple précédent illustre le fait que deux plongements différents donnent naissance à des groupes qui sont *commensurables* entre eux, i.e. leur intersection possède un indice fini dans chacun des deux groupes.

**Proposition 3.2.** *Soit $G$ et $H$ deux groupes algébriques matriciels sur $\mathbb{Q}$ et soit $\phi : G \to H$ un $\mathbb{Q}$-isomorphisme. Le groupe $\phi(G(\mathbb{Z}))$ est alors commensurable à $H(\mathbb{Z})$.*

Preuve. L'isomorphisme $\phi$ est donné par $\phi = (\phi_{kl})$, avec $\phi_{kl}$ des éléments de $\mathbb{Q}[(\mathrm{T}_{ij}), \mathrm{Y}]$ (la variable Y correspondant à l'inverse du déterminant de $(\mathrm{T}_{ij})$, cf. §2.5). Restreint à $\mathrm{GL}_N$, on a $\phi_{kl}\left((\mathrm{T}_{ij}), \det((\mathrm{T}_{ij}))^{-1}\right) \in \mathbb{Q}[(\mathrm{T}_{ij})]$. Définissons les polynômes $f_{kl}$ de la manière suivante :

$$f_{kl}\left((\mathrm{T}_{ij})\right) \quad := \quad \phi_{kl}\left(I + (\mathrm{T}_{ij}), \det(I + (\mathrm{T}_{ij}))^{-1}\right) - \delta_{kl},$$

où $I$ est la matrice identité et $\delta_{kl}$ le symbole de Kronecker. Comme $\phi$ est un homomorphisme on a $f_{kl}((0)) = 0$ $(\forall\ k, l)$, et cela montre que ces polynômes ne

possèdent pas de terme constant. Soit alors $\alpha \in \mathbb{Z}$ tel que $\alpha f_{kl} \in \mathbb{Z}[(\mathrm{T}_{ij})]$ pour tous les indices $(k,l)$. On a donc que $f_{kl}(\alpha A) \in \mathbb{Z}$ pour n'importe quelle matrice $A \in G(\mathbb{Z})$. Ceci montre que le sous-groupe de $G(\mathbb{Z})$ d'indice fini

$$G(\mathbb{Z})_\alpha \quad := \quad \{\, A \in G(\mathbb{Z}) \mid A \equiv I \ (\alpha)\}$$

est envoyé dans $H(\mathbb{Z})$. On applique alors le même raisonnement sur $\phi^{-1}$ et $H(\mathbb{Z})$. Ceci permet de conclure que $\phi(G(\mathbb{Z})_\alpha)$ est d'indice fini dans $H(\mathbb{Z})$. □

Suivant l'exemple du groupe modulaire $\mathrm{SL}_2(\mathbb{Z})$, on voudrait définir un sous-groupe comme étant arithmétique lorsqu'il est de la forme $G(\mathbb{Z})$, pour un certain plongement matriciel de $G$. Il est cependant plus approprié d'englober sous cette dénomination l'ensemble des sous-groupes qui sont commensurables à un tel $G(\mathbb{Z})$. Une deuxième extension est alors raisonnable : considérer des sous-groupes de $G(\mathbb{R})$. D'où la définition :

**Définition 3.3.** Soit $G$ un $\mathbb{Q}$-groupe algébrique et soit $K = \mathbb{Q}$ ou $\mathbb{R}$. Un sous-groupe de $G(K)$ qui est commensurable avec $G(\mathbb{Z})$ est appelé *sous-groupe arithmétique de* $G(K)$.

Notons que par la proposition 3.2 cette définition est indépendante du plongement matriciel implicitement choisi pour $G$. La classe (la commensurabilité est une relation d'équivalence) des sous-groupes arithmétiques de $G(K)$ est ainsi un invariant du $\mathbb{Q}$-groupe $G$. Il est à souligner que cette définition nécessite de préciser le corps $K$. Ainsi les notions de sous-groupe arithmétique de $G(\mathbb{Q})$, respectivement de $G(\mathbb{R})$, n'ont pas le même degré de généralité.

## §3.2 Le théorème de Borel et Harish-Chandra

De manière générale, un sous-groupe discret $\Gamma$ d'un groupe de Lie $\mathscr{G}$ présente un intérêt à travers le quotient $\mathscr{G}/\Gamma$ qu'il définit, qui se trouve être un espace topologique « modelé » sur $\mathscr{G}$. La question de la compacité d'un tel quotient se pose alors. Si $\mathscr{G}/\Gamma$ est compact, on dira que $\Gamma$ est *cocompact*.

Un second aspect important de l'étude du quotient $\mathscr{G}/\Gamma$ concerne la notion de mesure : le choix d'une mesure de Haar $\mu$ sur $\mathscr{G}$ associe au quotient $\mathscr{G}/\Gamma$ une mesure $\mu(\mathscr{G}/\Gamma) \in \mathbb{R}_{\geq 0} \cup \{\infty\}$. La question de la finitude de cette mesure se pose alors, et ce de manière d'autant plus évidente que ce problème ne dépend pas de la mesure $\mu$ choisie (la mesure de Haar étant unique à un facteur près). Lorsque la mesure $\mu(\mathscr{G}/\Gamma)$ est finie, on dira que $\Gamma$ est *de covolume fini* (dans $\mathscr{G}$). Notons qu'un quotient compact aura nécessairement, par propriété de la mesure de Haar, une mesure finie.

**Définition 3.4.** Un sous-groupe discret $\Gamma$ du groupe de Lie $\mathscr{G}$ est appelé *réseau* de $\mathscr{G}$ s'il est de covolume fini.

Supposons que $\Gamma$ et $\Gamma'$ sont deux sous-groupes discrets de $\mathscr{G}$ avec une inclusion $\Gamma' < \Gamma$ d'indice fini. Pour la mesure de Haar $\mu$, on obtient très facilement l'égalité :

$$\mu(\mathscr{G}/\Gamma') \quad = \quad [\Gamma : \Gamma']\, \mu(\mathscr{G}/\Gamma) \tag{3.1}$$

Un peu plus généralement on a l'énoncé :

**Proposition 3.5.** *Soient* $\Gamma$ *et* $\Gamma'$ *deux sous-groupes d'un groupe de Lie* $\mathscr{G}$*, qu'on suppose commensurables entre eux. Alors* $\Gamma$ *est discret (resp. cocompact, resp. de covolume fini) si et seulement si* $\Gamma'$ *est discret (resp. cocompact, resp. de covolume fini).*

Soit $G$ un groupe algébrique sur $\mathbb{Q}$. Le groupe de ses points réels $G(\mathbb{R})$ est alors un groupe de Lie. Pour la topologie induite par ce groupe de Lie, un sous-groupe arithmétique $\Gamma$ de $G(\mathbb{R})$ est alors discret. Les propriétés de compacité et de finitude de la mesure du quotient $G(\mathbb{R})/\Gamma$ peuvent alors être étudiées.

**Exemple 3.6.** Le sous-groupe $\{\pm 1\}$ de $\mathbf{G}_{\mathrm{m}}(\mathbb{Q})$ est clairement arithmétique. Le quotient $\mathbb{R}^{\times}/\{\pm 1\}$ possède une mesure infinie, pour n'importe quelle mesure de Haar sur $\mathbb{R}^{\times}$.

Cet exemple montre qu'en général un sous-groupe arithmétique n'est pas forcément un réseau. Mais la théorie des espaces symétriques accorde aux groupes semi-simples une place prépondérante en géométrie, et pour ceux-ci le théorème suivant donne une réponse fort satisfaisante aux questions posées ci-dessus.

**Théorème 3.7** (Borel - Harish-Chandra [BHC62])**.** *Soit* $G$ *un* $\mathbb{Q}$*-groupe algébrique semi-simple, et soit* $\Gamma$ *un sous-groupe arithmétique de* $G(\mathbb{R})$*. Alors :*

1. $\Gamma$ *est de covolume fini dans* $G(\mathbb{R})$*.*
2. $\Gamma$ *est cocompact si et seulement si* $G(\mathbb{Q})$ *ne contient pas d'élément unipotent non trivial.*

La preuve de la partie *1* s'obtient avec des efforts considérables en approximant un domaine fondamental pour $\Gamma$ dans $G(\mathbb{R})$. La partie *2* du théorème est connue sous le nom de *critère de compacité de Godement*, celui-ci ayant conjecturé le résultat. La preuve, qu'on peut trouver dans [OV00, Ch. 3 : 3.3], est nettement plus accessible et a du reste été découverte indépendemment par Mostow et Tamagawa [MT62].

**Remarque 3.8.** Les propositions 3.2 et 3.5 nous indiquaient déjà, avant même la formulation du théorème 3.7, qu'on devait s'attendre à obtenir des critères pour la compacité et la finitude du volume indépendants de la classe de commensurabilité de $\Gamma$. C'est en effet le cas, les conditions du théorème 3.7 étant données sur le $\mathbb{Q}$-groupe $G$. Notons que la question du calcul précis de la mesure $\mu(G(\mathbb{R})/\Gamma)$, qui dépend elle complètement de $\Gamma$, ne peut donc obtenir une réponse aussi concise.

**Exemple 3.9.** $\mathrm{SL}_2(\mathbb{Z})$ est un sous-groupe arithmétique, et donc un réseau de $\mathrm{SL}_2(\mathbb{R})$. Comme

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Q})$$

est unipotent, $\mathrm{SL}_2(\mathbb{Z})$ n'est pas cocompact. Le plan hyperbolique $\mathbb{H}^2$ pouvant s'écrire comme l'espace symétrique

$$\mathbb{H}^2 = \mathrm{SL}_2(\mathbb{R})/\mathrm{SO}(2),$$

où $\mathrm{SO}(2)$ est compact, on voit que ceci coïncide avec le fait exposé en §1.1 que le quotient $\mathbb{H}^2/\mathrm{SL}_2(\mathbb{Z})$ n'est pas compact.

**Exemple 3.10.** Pour $n \geq 2$ on considère la forme quadratique $f$ de l'exemple 2.46, vue comme forme quadratique sur $\mathbb{Q}$. Le groupe $\mathrm{SO}_f(\mathbb{Z})$ est alors un réseau de $\mathrm{SO}(n,1)$, non cocompact par le critère de Godement. On obtient immédiatement alors que son intersection $\mathrm{SO}_f(\mathbb{Z}) \cap \mathrm{SO}(n,1)^\circ$ est un réseau de $\mathrm{Isom}^+(\mathbb{H}^n)$ qui n'est pas cocompact.

## §3.3 Sous-groupes arithmétiques et corps de nombres

Si $H$ est un $\mathbb{Q}$-groupe qui n'est pas $\mathbb{Q}$-simple, on peut l'écrire comme produit de deux $\mathbb{Q}$-groupes infinis :

$$H \quad = \quad H_1 \cdot H_2.$$

Ainsi $H(\mathbb{Z}) = H_1(\mathbb{Z}) \cdot H_2(\mathbb{Z})$ et l'étude des sous-groupes arithmétiques de $H$ se réduit à l'étude des sous-groupes arithmétiques de $H_1$ et de $H_2$. Il semble donc parfaitement justifié de se restreindre à l'étude des sous-groupes arithmétiques dans les groupes $\mathbb{Q}$-simples. Ces sous-groupes arithmétiques sont appelés *irréductibles*. Dans ce contexte on bénéficie de l'existence du résultat suivant [BT65, 6.21 (ii)] :

**Proposition 3.11.** *Soit $H$ un $\mathbb{Q}$-groupe qui est $\mathbb{Q}$-simple et simplement connexe. Il existe alors une extension de corps finie $k|\mathbb{Q}$ et un $k$-groupe $G$ absolument simple (nécessairement simplement connexe), tel que :*

$$H \quad = \quad \mathbf{R}_{k|\mathbb{Q}}(G)$$

Cette proposition revêt pour nous une importance fondamentale. Moyennant la concession de considérer des corps plus généraux que $\mathbb{Q}$, elle va nous permettre l'utilisation dans notre théorie de groupes moins compliqués, car absolument simples. Considérer des groupes sur des corps $k$ plus larges que $\mathbb{Q}$ présentera même un côté avantageux : on s'attend en effet à ce que l'extension $k|\mathbb{Q}$ fournisse une partie des informations sur le $\mathbb{Q}$-groupe $H$.

**Remarque 3.12.** Il y a priori une limitation avec la proposition 3.11, due au fait que nous avons limité son domaine de validité au groupes simplement connexes (le résultat est en fait également correct pour les groupes adjoints). Pour l'étude des sous-groupes arithmétiques cette restriction est en fait sans conséquence. En effet, on peut étudier la classe de commensurabilité des sous-groupes arithmétiques d'un groupe semi-simple $H$ en se ramenant à l'étude de la classe du $\mathbb{Q}$-groupe simplement connexe qui revête $H$ par une $\mathbb{Q}$-isogénie (cf. proposition 2.44). Comme la proposition 3.2 se généralise au cas des $\mathbb{Q}$-isogénies entre groupes semi-simples [OV00, Ch. 1 : theorem 7.10], les sous-groupes arithmétiques sont conservés par cette $\mathbb{Q}$-isogénie.

Afin de tirer profit de la proposition 3.11 pour l'étude des sous-groupes arithmétiques, il faut observer ce que l'application $\rho$ définie par (2.6) fait correspondre au sous-groupe $H(\mathbb{Z})$, où $H$ simplement connexe est donné par $\mathbf{R}_{k|\mathbb{Q}}(G)$ comme dans la proposition 3.11. On utilise ici librement la matière présentée dans §2.6. On rappelle que, même si cela ne change pas la classe de $\mathbb{Q}$-isomorphie de $\mathbf{R}_{k|\mathbb{Q}}(G)$, l'application $\rho$ dépend du choix de la base $\omega_1, \ldots, \omega_d$ de $k|\mathbb{Q}$ (où

l'on suppose désormais que $[k : \mathbb{Q}] = d$). On va supposer que la base $\omega_1, \ldots, \omega_d$ soit telle que l'anneau

$$\mathscr{O} \quad = \quad \mathbb{Z}[\omega_1, \ldots, \omega_d] \tag{3.2}$$

est libre, de rang $d$. Un sous-anneau $\mathscr{O} \subset k$ de ce type est appelé *ordre* de $k$. Un élément de $a \in \mathscr{O}$ correspond alors par $\rho$ (restreint à $k$) à une matrice à coefficients dans $\mathbb{Z}$. Plus précisément :

$$\rho(G(\mathscr{O})) \quad = \quad H(\mathbb{Z}).$$

La discussion qui précède montre que les sous-groupes arithmétiques irréductibles de $H(\mathbb{R}) = \mathbf{R}_{k|\mathbb{Q}}(G)(\mathbb{R})$ sont les sous-groupes qui sont commensurables avec $G(\mathscr{O})$, où $G$ est $k$-groupe absolument simple, $k|\mathbb{Q}$ est un *corps de nombres* (i.e. un sous-corps de $\mathbb{C}$ qui est une extension finie de $\mathbb{Q}$), et $\mathscr{O}$ est un ordre de $k$. On insiste sur le fait que, contrairement à $G(k)$, l'ensemble $G(\mathscr{O})$ n'est que défini à commensurabilité près (si aucun plongement matriciel de $G$ n'est spécifié). Si on remplace $\mathscr{O}$ par un autre ordre $\mathscr{O}'$ de $k$, on obtient un groupe $G(\mathscr{O}')$ commensurable avec $G(\mathscr{O})$. On peut choisir arbitrairement de travailler avec un ordre de $k$ particulier : c'est ce que nous allons faire, en prenant l'unique ordre maximal de $k$, communément appelé *anneau des entiers algébriques* de $k$, qui sera noté $\mathscr{O}_k$. Ainsi l'étude des sous-groupes arithmétiques, que nous avons pour l'instant exclusivement lié à la théorie des groupes algébriques, se trouve également liée à la donnée $(k, \mathscr{O}_k)$, qui sera l'objet du chapitre 4.

Il nous reste à décrire le groupe de Lie $H(\mathbb{R}) = \mathbf{R}_{k|\mathbb{Q}}(G)(\mathbb{R})$ dans lequel se situe la classe de commensurabilité de $G(\mathscr{O}_k)$. Nous présentons ceci par une analogie avec la partie *2* de la proposition 2.29. Celle-ci nous assure l'existence d'un isomorphisme

$$H(\overline{\mathbb{Q}}) \quad \cong \quad \prod_{\sigma} G^{\sigma}(\overline{\mathbb{Q}}). \tag{3.3}$$

Par extension on a $H(\mathbb{C}) \cong \prod_{\sigma} G^{\sigma}(\mathbb{C})$. Ceci doit être adapté pour décrire $H(\mathbb{R})$ plutôt que $H(\mathbb{C})$. On rappelle que l'isomorphisme (3.3) découle de la proposition 2.27, qui décrit $k \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$. Il s'agit donc de considérer l'algèbre $k \otimes_{\mathbb{Q}} \mathbb{R}$ plutôt que l'algèbre $k \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$.

Pour le corps de nombres $k$ de degré $d$ on suppose comme d'habitude que $\sigma$ parcourt les $d$ monomorphismes $\sigma : k \to \overline{\mathbb{Q}} \subset \mathbb{C}$. On range ces monomorphismes par classes

$$[\sigma] \quad := \quad \{\sigma, \overline{\sigma}\},$$

où $\overline{\sigma}$ désigne le conjugué complexe de $\sigma$. Il existe donc $r + s$ de ces classes, $r$ désignant le nombre de monomorphismes *réels* (i.e. avec $\sigma(k) \subset \mathbb{R}$) et $2s$ le nombre de monomorphismes *complexes* (i.e. avec $\sigma(k) \not\subset \mathbb{R}$). Si $\sigma(k) \subset \mathbb{R}$ alors $[\sigma] = \{\sigma\}$, sinon $[\sigma]$ contient deux monomorphismes distincts.

**Proposition 3.13.** *On a un isomorphisme entre $\mathbb{R}$-algèbres donné par :*

$$\begin{array}{rcl} k \otimes_{\mathbb{Q}} \mathbb{R} & \to & \mathbb{R}^r \times \mathbb{C}^s \\ a \otimes 1 & \mapsto & (\sigma a)_{[\sigma]}, \end{array}$$

*où les coordonnées des vecteurs dans $\mathbb{R}^r \times \mathbb{C}^s$ sont indexées par les classes $[\sigma]$. Cette isomorphisme donne un isomorphisme entre $\mathbf{R}_{k|\mathbb{Q}}(G)(\mathbb{R})$ et le groupe de Lie*

$$G_\infty \quad := \quad \prod_{\#[\sigma]=1} G^\sigma(\mathbb{R}) \times \prod_{\#[\sigma]=2} G^\sigma(\mathbb{C}). \tag{3.4}$$

*Cet isomorphisme fait correspondre $\mathbf{R}_{k|\mathbb{Q}}(G)(\mathbb{Q})$ à l'image de $G(k)$ dans $G_\infty$ donnée par l'injection diagonale $g \mapsto (\sigma g)_{[\sigma]}$.*

**Remarque 3.14.** Le choix qui consiste à prendre $\sigma$ ou son conjugué $\overline{\sigma}$ dans la classe $[\sigma]$ pour représenter $k \otimes_{\mathbb{Q}} \mathbb{R}$ est bien entendu arbitraire. Il en est de même à propos de l'ordre des facteurs indexés par $[\sigma]$.

**Exemple 3.15.** On modifie l'exemple 3.10 en considérant la forme définie sur $k = \mathbb{Q}(\sqrt{5})$

$$f(x_0, \ldots, x_n) \quad = \quad -\omega\, x_0^2 + x_1^2 + \cdots + x_n^2, \tag{3.5}$$

où $\omega := \frac{1+\sqrt{5}}{2}$. L'anneau $\mathbb{Z}[\omega]$ est l'anneau des entiers $\mathscr{O}_k$ de $k$. Ainsi $\mathrm{SO}_f(\mathscr{O}_k)$ est un réseau dans $\mathbf{R}_{k|\mathbb{Q}}(\mathrm{SO}_f)(\mathbb{R})$. La forme quadratique $f$ est de signature réelle $(n, 1)$. Mais pour le monomorphisme non trivial $\sigma : \sqrt{5} \mapsto -\sqrt{5}$, la forme conjuguée $\sigma f$ ne possède que des coefficients positifs (i.e. signature $(n, 0)$). Ceci montre que $\mathbf{R}_{k|\mathbb{Q}}(\mathrm{SO}_f)(\mathbb{R})$ correspond au produit suivant :

$$\mathbf{R}_{k|\mathbb{Q}}(\mathrm{SO}_f)(\mathbb{R}) \quad \cong \quad \mathrm{SO}(n, 1) \times \mathrm{SO}(n + 1).$$

Comme $\mathrm{SO}(n + 1)$ est compact, il est facile de constater que $\mathrm{SO}_f(\mathscr{O}_k)$ reste un réseau lorsque projeté sur le facteur $\mathrm{SO}(n, 1)$. En prenant l'intersection avec $\mathrm{SO}(n, 1)^\circ$, on obtient donc un réseau de $\mathrm{Isom}^+(\mathbb{H}^n)$.

## §3.4 Réseaux définis arithmétiquement

Inspiré par l'exemple 3.15 nous voulons définir la notion de réseau arithmétique d'un groupe de Lie semi-simple $\mathscr{G}$. Afin de se simplifier légèrement la tâche on va en fait se restreindre au cas d'un groupe de Lie $\mathscr{G}$ qu'on supposera connexe et ne possédant pas de sous-groupe compact normal non trivial (en particulier $\mathscr{G}$ est de centre trivial, i.e. $\mathscr{G}$ est *adjoint*). Dans le contexte de l'étude des espaces symétriques cette situation est tout à fait générale. On va également se restreindre à l'arithméticité des réseaux irréductibles. Si $\mathscr{G}$ s'écrit comme produit de deux groupes de Lie semi-simples $\mathscr{G}_1 \times \mathscr{G}_2$, le réseau $\Gamma < \mathscr{G}$ est dit *irréductible* s'il n'est pas égal à un produit $\Gamma_1 \times \Gamma_2$ avec $\Gamma_i < \mathscr{G}_i$ un réseau. Cette notion est analogue à l'irréductibilité des sous-groupes arithmétiques évoquée plus haut.

Soit $G$ un groupe absolument simple défini sur un corps de nombres $k$, pour lequel on admettra que le groupe $G_\infty$ n'est pas compact. Si un monomorphisme $\sigma : k \to \mathbb{C}$ est complexe, alors le groupe $G^\sigma(\mathbb{C})$ est non compact. Par contre si $\sigma$ est réel, il se peut très bien que $G^\sigma(\mathbb{R})$ soit compact. Notons par $\mathcal{S}$ l'ensemble des classes $[\sigma]$ de monomorphismes pour lesquelles le facteur correspondant dans $G_\infty$ est non compact. Ceci détermine un groupe $G_\mathcal{S}$ définit de façon analogue à $G_\infty$, en omettant simplement les facteurs $G^\sigma(\mathbb{R})$ qui sont compacts. On admet le groupe $G(k)$ inclus diagonalement dans $G_\mathcal{S}$, comme dans $G_\infty$. On généralise la définition 3.3 comme suit :

**Définition 3.16.** $\Gamma < G_{\mathcal{S}}$ est un *sous-groupe arithmétique* de $G_{\mathcal{S}}$ s'il est commensurable avec $G(\mathscr{O}_k)$. On dira dans ce cas que $\Gamma$ est *défini sur* $k$.

Les éléments présentés plus haut dans ce chapitre montrent alors qu'un sous-groupe arithmétique de $G_{\mathcal{S}}$ est un réseau dans $G_{\mathcal{S}}$ : la projection $G_\infty \to G_{\mathcal{S}}$ possède un noyau compact et conserve ainsi les réseaux.

**Définition 3.17.** Soit $\mathscr{G}$ un groupe de Lie connexe ne possédant pas de sous-groupe normal compact autre que $\{1\}$. Un réseau irréductible $\Gamma < \mathscr{G}$ est dit *arithmétique* s'il existe un corps de nombres $k$ et un $k$-groupe $G$ simplement connexe et absolument simple tel que $\mathscr{G}$ s'écrive comme

$$\mathscr{G} \quad = \quad G_{\mathcal{S}}/\mathcal{Z},$$

où $\mathcal{Z}$ désigne le centre de $G_{\mathcal{S}}$, et que $\Gamma$ s'écrive comme quotient d'un sous-groupe arithmétique de $G_{\mathcal{S}}$ par $\mathcal{Z}$. On dira dans ce cas que $\Gamma$ est *rattaché* à $(G, k)$. Le groupe algébrique $G$ est lui dit *admissible* (pour $\mathscr{G}$).

**Remarque 3.18.** Notre définition, qui demande que le groupe algébrique $G$ soit simplement connexe, semble a priori oublier les exemples 3.10 et 3.15, où les groupes $\mathrm{SO}_f$ ne sont pas simplement connexes (voir l'exemple 2.46). La remarque 3.12 montre cependant que les réseaux de $\mathrm{Isom}^+(\mathbb{H}^n)$ donnés dans ces exemples sont bien arithmétiques au sens de la définition 3.17.

Même si la différence n'est pas toujours marquée dans la littérature, pour notre part nous ferons bien la distintion entre « sous-groupes arithmétiques » de $G_{\mathcal{S}}$ et « réseaux arithmétiques » de $\mathscr{G}$ (même dans la situation où $\mathcal{Z} = 1$). Dans le premier cas on entend une seule classe de commensurabilité, spécifiée par le groupe algébrique (ici $G$). La seconde notion englobe une multitude de classes de commensurabilité, car elle admet de faire varier le couple $(G, k)$ parmi tous les groupes admissibles pour $\mathscr{G}$. Or faire varier le groupe admissible implique bien la variation de la classe de commensurabilité. Cela suit du résultat suivant, qui montre qu'un réseau arithmétique détermine uniquement (à isomorphisme près) le couple $(G, k)$ auquel il est rattaché :

**Proposition 3.19.** *Soit $G$ (resp. $G'$) un groupe algébrique simplement connexe absolument simple, défini sur le corps de nombres $k$ (resp. $k'$). Comme ci-haut on suppose que $\mathcal{S}$ (resp. $\mathcal{S}'$) désigne l'ensemble maximal des classes de monomorphimes de $k$ (resp. $k'$) tel que $G_{\mathcal{S}}$ (resp. $G_{\mathcal{S}'}$) soit sans facteur compact. Si $G_{\mathcal{S}} = G'_{\mathcal{S}'}$ avec $G(\mathscr{O}_k)$ commensurable à $G'(\mathscr{O}_{k'})$ alors on a que $k = k'$ (à $\mathbb{Q}$-isomorphisme près), $\mathcal{S} = \mathcal{S}'$ et $G$ est $k$-isomorphe à $G'$.*

Idée de la preuve. La preuve repose en grande partie sur un théorème de Borel qui affirme que le sous-groupe $G(\mathscr{O}_k)$ est Zariski-dense dans $G_{\mathcal{S}}$. En particulier si on sait que $k = k'$ le résultat suit immédiatement. Nous n'avons connaissance d'aucune preuve dans la littérature, à l'exception de [PR09] qui comble cette lacune dans la partie préliminaire de l'article. Dans ce récent travail, la proposition est présentée comme étant un résultat « bien connu ». □

Le théorème 3.7 montre que pour prouver l'existence d'un réseau dans $\mathscr{G}$ il suffit de trouver un groupe algébrique admissible. On montre effectivement de cette manière l'existence de réseaux (arithmétiques) dans le groupe des

isométries de chacun des espaces symétriques [Rag72, Ch. XIV]. Plus précisément on montre même l'existence simultanée de réseaux cocompacts et de réseaux non cocompacts. Le cas cocompact est dû à Borel [Bor63]. Il est en lien avec le critère suffisant suivant pour la cocompacité :

**Proposition 3.20.** *Soit $G$ un $k$-groupe algébrique admissible pour $\mathscr{G}$. Si $G_\infty$ possède un facteur compact (i.e $G_\infty \neq G_\mathcal{S}$) alors $G(\mathscr{O}_k)$ est cocompact dans $G_\mathcal{S}$ (et de même pour sa projection dans $\mathscr{G}$).*

Idée de la preuve. La restriction des scalaires transforme le critère de compacité de Godement en l'affirmation suivante : $G(\mathscr{O}_k)$ est cocompact dans $G_\infty$ (ou de manière équivalente dans $G_\mathcal{S}$) si et seulement si $G(k)$ ne possède pas d'élément unipotent non trivial. Or un groupe compact ne possède pas d'élément unipotent non trivial (pour s'en faire une idée on peut considérer tout élément de la forme $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, qui pour $x \neq 0$ engendre le groupe non compact $\mathbb{R}$). Comme $G(k)$ est inclus diagonalement dans $G_\infty$ on conclut que si ce dernier possède un facteur compact, le seul élément unipotent de $G(k)$ doit être 1. □

**Exemple 3.21.** En particulier cette proposition s'applique sur l'exemple 3.15, prouvant que le réseau arithmétique qui y est défini est cocompact.

Il a déjà été question dans l'introduction du théorème suivant. Le résultat, conjecturé par Selberg et Piatetski-Shapiro, se déduit du *théorème de superrigidité* de Margulis. La démonstration (difficile) de celui-ci passe notamment par l'utilisation de la *théorie ergodique*. Le livre [Zim84] donne une introduction à ces travaux de Margulis.

**Théorème 3.22** (d'arithméticité de Margulis)**.** *Soit $\mathscr{G}$ un groupe de Lie comme dans la définition 3.17, qui de plus possède un rang réel $\geq 2$. Dans ce cas tous les réseaux irréductibles de $\mathscr{G}$ sont arithmétiques.*

On rappelle que le *rang réel* de $\mathscr{G}$ peut se définir comme l'entier $r$ maximal tel que $\mathscr{G}$ possède un sous-groupe isomorphe à $(\mathbb{R}^\times)^r$. Le groupe $\mathrm{SO}(n,1)$, et par conséquent aussi $\mathrm{Isom}(\mathbb{H}^n)$, possède un rang réel égal à 1. Le théorème d'arithméticité ne s'applique donc pas au cas de la géométrie hyperbolique. Gromov et Piatetski-Shapiro ont effectivement montré [GPS87] que pour chaque dimension $n$ il existe un quotient $\mathbb{H}^n/\Gamma$ non arithmétique de volume fini (i.e. $\Gamma$ est un réseau de $\mathrm{Isom}(\mathbb{H}^n)$). Auparavant Makarov [Mak66] puis Vinberg [Vin67] avaient prouvé l'existence de groupes de Coxeter hyperboliques non arithmétiques. Outre ces exemples en géométrie hyperbolique *réel*, il a été montré par Deligne et Mostow [DM86] que les *espaces hyperboliques complexes* $\mathbb{H}^2_\mathbb{C}$ et $\mathbb{H}^3_\mathbb{C}$ possèdent des quotients non arithmétiques de volume fini. L'espace hyperbolique complexe $\mathbb{H}^n_\mathbb{C}$ de dimension $n$ est l'espace symétrique associé au groupe $\mathrm{PU}(n,1)$, dont le rang réel vaut 1. Le problème de savoir si $\mathrm{PU}(n,1)$ contient pour $n \geq 4$ des réseaux non arithmétiques reste ouvert. Hormis ces cas énoncés, tous les autres groupes de Lie semi-simple de rang réel égal à 1 ont été prouvés (au cas par cas) être satisfaisant à la conclusion de 3.22. On lira [OV00, Ch. 3 : 6.6] pour un rapide survol du problème de l'arithméticité.

# Chapitre 4. Corps de nombres et entiers algébriques

Au paragraphe §3.3 nous avons abordé la possibilité d'utiliser des groupes algébriques sur des corps de nombres pour construire les sous-groupes (ou réseaux) arithmétiques. Certaines des propriétés d'un sous-groupe arithmétique défini sur $k$ pourront être déduites de l'étude de la paire $(k, \mathscr{O}_k)$, où l'anneau des entiers algébriques $\mathscr{O}_k$ (que nous avons déjà utilisé en §3.3) sera défini précisément dans ce qui suit. L'étude de $(k, \mathscr{O}_k)$, connue sous le nom de *théorie algébrique des nombres*, est fort bien développée et documentée. Ce présent chapitre donne la première approche classique qu'a connu cette théorie. Une seconde approche, qui fait à présent partie de la théorie classique, sera présentée au chapitre 5. Nous citerons dans ce chapitre essentiellement le livre de Neukirch [Neu99]. La référence [Lan86] peut tout aussi bien convenir.

## §4.1 L'anneau des entiers algébriques

Un élément de $\overline{\mathbb{Q}}$ est appelé *entier algébrique* s'il est racine d'un polynôme normé à coefficients dans $\mathbb{Z}$. On peut montrer que l'ensemble des entiers algébriques est fermé pour l'addition et la multiplication. Pour un corps de nombres $k$, le sous-ensemble

$$\mathscr{O}_k := \{x \in k \mid x \text{ entier algébrique}\}$$

est alors un anneau, qu'on appelle *anneau des entiers algébriques* de $k$. Cette dénomination est justifiée par le fait que $\mathscr{O}_k$ est une généralisation de $\mathbb{Z}$. On a en effet $\mathscr{O}_{\mathbb{Q}} = \mathbb{Z}$. De plus le corps $k$ peut se voir comme le corps des fractions de $\mathscr{O}_k$. Le paragraphe §3.3 suggérait déjà une similarité entre $\mathbb{Z}$ et $\mathscr{O}_k$. Le théorème suivant, qui généralise le théorème fondamental de l'arithmétique (factorisation dans $\mathbb{Z}$), insiste encore plus dans cette direction [Neu99, Ch. I (3.3)] :

**Théorème 4.1.** *Chaque idéal $\mathfrak{a}$ de $\mathscr{O}_k$ différent de $\mathscr{O}_k$ et $(0)$ possède une factorisation en idéaux premiers distincts $\mathfrak{p}_i$ $(1 \leq i \leq \alpha)$ :*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_\alpha^{e_\alpha},$$

*pour des puissances $e_i \in \mathbb{N}_{>0}$ $(1 \leq i \leq \alpha)$. Cette factorisation est unique à l'ordre des facteurs près.*

**Remarque 4.2.** La multiplication entre deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ qui intervient dans ce dernier théorème est donnée par

$$\mathfrak{a} \cdot \mathfrak{b} \quad = \quad \left\{ \sum_i a_i b_i \;\middle|\; a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \right\}.$$

Ce théorème admet une extension sur tout le corps $k$ (et pas seulement limité à $\mathscr{O}_k$), une fois que l'on généralise la notion d'idéal comme suit : un *idéal fractionnaire* de $k$ est un $\mathscr{O}_k$-sous-module non nul de $k$ de type fini. L'ensemble des idéaux fractionnaires de $k$ devient alors un groupe commutatif (pour la multiplication donnée comme dans la remarque 4.2). L'élément neutre est $(1) = \mathscr{O}_k$ et l'élément inverse d'un idéal fractionnaire $\mathfrak{a}$ est donné par

$$\mathfrak{a}^{-1} \quad = \quad \{\, x \in k \mid x\mathfrak{a} \subset \mathscr{O}_k \}\,.$$

On notera par $\mathcal{J}_k$ le *groupe des idéaux fractionnaires* de $k$. On démontre alors facilement à partir du théorème 4.1 [Neu99, Ch. I (3.9)] :

**Corollaire 4.3.** *Chaque idéal fractionnaire $\mathfrak{a} \neq (1)$ de $k$ admet une unique factorisation :*

$$\mathfrak{a} \quad = \quad \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_\alpha^{e_\alpha},$$

*où $\mathfrak{p}_i$ sont des idéaux premiers distincts de $\mathscr{O}_k$ et les puissances $e_i$ sont dans $\mathbb{Z} \setminus \{0\}$ (pour $i = 1, \ldots, \alpha$).*

Contrairement au cas de $\mathbb{Z}$ il n'est pas garanti que l'anneau $\mathscr{O}_k$ soit *principal*, c'est-à-dire que chacun de ses idéaux soit de la forme $(x) = x\mathscr{O}_k$ pour un $x \in \mathscr{O}_k$ (un tel idéal est dit *principal*). Pour mesurer de combien l'anneau $\mathscr{O}_k$ se différencie d'un anneau principal on s'appuie sur la structure de groupe de $\mathcal{J}_k$ :

**Définition 4.4.** Notons par $\mathcal{P}_k$ le sous-groupe de $\mathcal{J}_k$ des *idéaux fractionnaires principaux* de $k$, c'est-à-dire les élément de $\mathcal{J}_k$ de la forme $(x) = x\mathscr{O}_k$ pour $x \in k^\times$. Le groupe quotient

$$\mathscr{C}_k = \mathcal{J}_k / \mathcal{P}_k$$

est appelé le *groupe des classes (d'idéaux)* de $k$.

Plus le groupe $\mathscr{C}_k$ est compliqué, plus l'anneau $\mathscr{O}_k$ se différencie d'un anneau principal, et plus son étude devient difficile. Le théorème suivant prédit une certaine limite à cette difficulté [Neu99, Ch. I (6.3)] :

**Théorème 4.5.** *Le groupe $\mathscr{C}_k$ des classes d'idéaux d'un corps de nombres $k$ est fini.*

On appelle *nombre de classes* la cardinalité de $\mathscr{C}_k$, et cette valeur est notée par le symbole $h_k$. L'anneau $\mathscr{O}_k$ est ainsi principal si et seulement si $h_k = 1$. On a par exemple $h_\mathbb{Q} = 1$.

Nous terminons ce paragraphe en énonçant la proposition qui montre que $\mathscr{O}_k$ est un ordre de $k$, fait sur lequel nous nous sommes appuyé pour développer le paragraphe §3.3.

**Proposition 4.6.** *$\mathscr{O}_k$ est un module libre sur $\mathbb{Z}$ de rang $d = [k : \mathbb{Q}]$.*

Idée de la preuve. On montre qu'on peut choisir une base de $k|\mathbb{Q}$ dont tous les éléments sont dans $\mathscr{O}_k$. Il s'ensuit que $\mathscr{O}_k$ est un $\mathbb{Z}$-module de type fini, nécessairement sans torsion (comme ici $k \subset \mathbb{C}$). Mais un tel $\mathbb{Z}$-module est nécessairement libre. Ceci suit par exemple du théorème de structure des modules sur les anneaux principaux. La preuve repose donc sur le fait que $h_\mathbb{Q} = 1$. Une base de $\mathscr{O}_k$ est alors également une base de $k|\mathbb{Q}$, ce qui détermine le rang de $\mathscr{O}_k$. □

## §4.2 Norme

Rappelons la notion de norme dans une extension de corps finie $K|k$ (où pour le moment ces corps ne sont pas nécessairement dans $\mathbb{C}$) :

**Définition 4.7.** Soit $a \in K$. La *norme* de $a$ dans l'extension $K|k$, notée $N_{K|k}(a)$, est définie comme le déterminant de l'application $k$-linéaire :

$$\begin{aligned} K &\to K \\ x &\mapsto ax \end{aligned}$$

Par propriété du déterminant, la norme $N_{K|k}$ est multiplicative. Pour $k$ et $K$ qui respectent les conventions de §2.1 la norme peut se calculer comme suit [Neu99, Ch. I : (2.6)] :

**Proposition 4.8.** *La norme d'un élément $a \in K$ dans $K|k$ est donnée par :*

$$N_{K|k}(a) \quad = \quad \prod_{\sigma} \sigma a,$$

*où $\sigma$ parcours les $[K : k]$ $k$-monomorphismes $\sigma : K \to \overline{k}$.*

Revenons à présent à la situation où le corps $k$ est un corps de nombres. En prenant une base sur $\mathbb{Z}$ de $\mathscr{O}_k$, on peut voir immédiatement à partir de la définition 4.7 que

$$N_{k|\mathbb{Q}}(\mathscr{O}_k) \subset \mathbb{Z}. \tag{4.1}$$

On introduit une seconde notion de norme, cette fois pour les idéaux, grâce à la définition suivante :

**Définition 4.9.** Soit $\mathfrak{a}$ un idéal non nul de $\mathscr{O}_k$. Une légère généralisation de la proposition 4.6 montre que $\mathfrak{a}$ est un sous-module libre de $\mathscr{O}_k$ de même rang que $\mathscr{O}_k$, ce qui permet de voir que l'anneau quotient $\mathscr{O}_k/\mathfrak{a}$ est fini. On définit alors la *norme* de l'idéal $\mathfrak{a}$ comme étant la cardinalité de $\mathscr{O}_k/\mathfrak{a}$. Cette norme sera notée $\mathcal{N}_{k|\mathbb{Q}}(\mathfrak{a})$.

La norme d'idéal est essentiellement une généralisation de la notion de la norme des éléments dans $k|\mathbb{Q}$. On a en effet pour $a \in \mathscr{O}_k$ et son idéal principal $(a) = a\mathscr{O}_k$ associé :

$$\mathcal{N}_{k|\mathbb{Q}}\,(\,(a)\,) \quad = \quad \big|N_{k|\mathbb{Q}}(a)\big| \tag{4.2}$$

A la vue de (4.1) cette correspondance apparaît plausible. Tout comme $N_{k|\mathbb{Q}}$, la norme d'idéal $\mathcal{N}_{k|\mathbb{Q}}$ est multiplicative.

## §4.3 Plongements archimédiens

Jusqu'à la fin du chapitre nous allons considérer que $k$ désigne un corps de nombres. On reprend les notations de §3.3 introduites pour $k$ : on désigne par $r$ le nombre de monomorphismes $k \to \mathbb{R}$, et par $s$ le nombre de monomorphismes $k \to \mathbb{C}$ complexes. La paire $(r, s)$ est appelée *signature* de $k$. Ces monomorphismes

$k \to \mathbb{C}$ seront désormais appelés *plongements archimédiens* de $k$. Ils sont rangés par classes $[\sigma] = \{\sigma, \overline{\sigma}\}$.

Nous avons vu dans la proposition 3.13 que $k \otimes_{\mathbb{Q}} \mathbb{R}$ se décrit comme le produit $\mathbb{R}^r \times \mathbb{C}^s$. Il est utile de réserver une notation pour cet ensemble. Suivant la même ligne que la définition donnée en (3.4) on notera

$$k_\infty \quad := \quad \mathbb{R}^r \times \mathbb{C}^s, \tag{4.3}$$

et l'on considérera $k_\infty$ comme un espace vectoriel réel, muni de la structure de $k$-algèbre donnée par le plongement diagonal :

$$a \in k \quad \mapsto \quad (\sigma a)_{[\sigma]}.$$

Selon la discussion menée en §3.3 l'anneau $\mathscr{O}_k$ (ou plus généralement n'importe quel ordre de $k$) est discret dans $k_\infty$ (plongé diagonalement). Cette discussion reposait cependant sur le concept plutôt élaboré de la restricition des scalaires. C'est pourquoi nous donnons ici une seconde preuve, indépendante de §3.3 :

**Proposition 4.10.** *L'anneau $\mathscr{O}_k$ est discret dans $k_\infty$.*

Preuve. Soit $(x_n)$ une suite dans $\mathscr{O}_k \hookrightarrow k_\infty$ qui converge vers 0. Il suit que $N_{k|\mathbb{Q}}(x_n)$ tend vers 0, la norme $N_{k|\mathbb{Q}}$ étant la restriction à $k$ d'une fonction continue sur $k_\infty$. Comme par (4.1) la suite $(N_{k|\mathbb{Q}}(x_n))_n$ est dans $\mathbb{Z}$, elle doit se stabiliser sur zéro. Mais seule la norme de 0 est nulle, ce qui montre que la suite $(x_n)$ se stabilise sur $0 \in k_\infty$. Ce point est donc isolé, et $(\mathscr{O}_k, +)$ est un sous-groupe discret de $(k_\infty, +)$. □

**Exemple 4.11.** L'anneau des entiers $\mathbb{Z}[i]$ du corps $\mathbb{Q}(i)$ est bien discret dans $\mathbb{C}$ (indépendemment du plongement complexe choisi : $i \mapsto i$ ou $i \mapsto -i$). Un seul des deux plongements complexes est donc nécessaire pour voir $\mathbb{Z}[i]$ comme un groupe discret. Ceci correspond bien à l'idée plus générale d'indexer les facteurs de $k_\infty$ par les classes $[\sigma]$, et non pas par tous les plongements $\sigma$.

## §4.4 Idéaux premiers

Intéressons-nous un instant aux idéaux premiers apparaissant dans la factorisation du théorème 4.1. Par *idéal premier* de $\mathscr{O}_k$ on entendra donc un idéal premier différent de (0). La propriété remarquable commune à tous ces idéaux, est qu'ils sont en fait maximaux [Neu99, Ch. I (3.1)] :

**Proposition 4.12.** *Chaque idéal premier $\mathfrak{p}$ de $\mathscr{O}_k$ est maximal. Le quotient $\mathscr{O}_k/\mathfrak{p}$ est donc un corps, qu'on notera par $\mathbb{F}_\mathfrak{p}$.*

Fixons-nous un idéal premier $\mathfrak{p} \subset \mathscr{O}_k$. Le corps $\mathbb{F}_\mathfrak{p}$ possède une cardinalité finie donnée par $\mathcal{N}_{k|\mathbb{Q}}(\mathfrak{p})$. Or les corps finis sont entièrement déterminés par le nombre de leurs éléments, et cette cardinalité doit être de la forme $p^f$ pour un nombre premier $p \in \mathbb{N}$ et un entier $f \in \mathbb{N}_{>0}$. Le nombre premier $p$ lié à $\mathfrak{p}$ s'obtient également de la façon suivante : l'intersection $\mathfrak{p} \cap \mathbb{Z}$ doit être un idéal premier de $\mathbb{Z}$, et donc de la forme $p'\mathbb{Z}$ pour un nombre premier $p' \in \mathbb{Z}$. Mais du coup on obtient une inclusion du corps fini $\mathbb{F}_{p'} := \mathbb{Z}/p'\mathbb{Z}$ dans le corps $\mathbb{F}_\mathfrak{p} = \mathscr{O}_k/\mathfrak{p}$,

et ceci impose l'égalité $p' = p$. On peut encore voir que l'idéal $\mathfrak{p}$ est l'un des facteurs premiers apparaissant dans la factorisation de l'idéal $(p) = p\mathscr{O}_k$ dans $\mathscr{O}_k$. L'idéal $\mathfrak{p}$ *divise* donc $(p)$, ce que l'on note par $\mathfrak{p}|p$ (et que l'on pourrait définir plus précisément par $\mathfrak{p}|p \Leftrightarrow (p) \subset \mathfrak{p}$). On dira aussi dans cette situation que $\mathfrak{p}$ est *au-dessus* de $p$. Nous pouvons lister (théoriquement) tous les idéaux premiers de $\mathscr{O}_k$ en factorisant dans $\mathscr{O}_k$ chaque nombre premier $p \in \mathbb{N}$.

**Définition 4.13.** Soit $p \in \mathbb{N}$ un nombre premier et $\mathfrak{p}$ un idéal premier de $\mathscr{O}_k$ avec $\mathfrak{p}|p$. On définit :
- la multiplicité de $\mathfrak{p}$ dans la factorisation de l'idéal $(p) = p\mathscr{O}_k$, notée par $e_\mathfrak{p} \in \mathbb{N}_{>0}$, est appelée *indice de ramification* de $\mathfrak{p}$. Si $e_\mathfrak{p} > 1$ l'idéal $\mathfrak{p}$ est dit *ramifié*. Dans le cas contraire il est dit *non ramifié*.
- le degré de l'extension de corps $\mathbb{F}_\mathfrak{p}|\mathbb{F}_p$ est appelé *degré d'inertie* de $\mathfrak{p}$. On le note par $f_\mathfrak{p} := [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]$.

Inertie et ramification au-dessus d'un entier $p \in \mathbb{N}$ sont tenues entre elles par l'identité suivante [Neu99, Ch. I (8.2)] :

**Proposition 4.14.** *Soit $k|\mathbb{Q}$ un corps de nombres. Alors pour chaque nombre premier $p \in \mathbb{N}$, on a l'équalité :*

$$\sum_{\mathfrak{p}|p} e_\mathfrak{p} f_\mathfrak{p} \quad = \quad [k : \mathbb{Q}].$$

**Définition 4.15.** Un nombre premier $p \in \mathbb{N}$ est dit *ramifié* dans l'extension $k|\mathbb{Q}$ si sa factorisation dans $\mathscr{O}_k$ contient un idéal premier ramifié. Dans le cas contraire, $p$ est dit *non ramifié*. Si l'idéal $(p)$ est lui-même premier dans $\mathscr{O}_k$, alors $p$ est dit *inerte* dans $k|\mathbb{Q}$.

## §4.5 Le discriminant

Nous introduisons à présent un invariant important des corps de nombres : le discriminant. De définition simple, cet invariant possède deux interprétations que nous allons développer. Toutes deux auront leur importance par la suite.

Soit $k$ un corps de nombres de degré $d = [k : \mathbb{Q}]$. Soit $\omega_1, \ldots, \omega_d$ une base libre de $\mathscr{O}_k$ (dont l'existence est garantie par la proposition 4.6). De plus, on note par $\sigma_1, \ldots, \sigma_d$ les plongements archimédiens de $k$. Le *discriminant* $\mathcal{D}_k$ d'un corps de nombres $k$ est habituellement défini par

$$\mathcal{D}_k \quad := \quad \det\left((\sigma_i\omega_j)_{1\leq i,j\leq d}\right)^2. \tag{4.4}$$

$\mathcal{D}_k$ ne dépend pas de la base choisie. En effet, deux $\mathbb{Z}$-bases peuvent être envoyée l'une sur l'autre à l'aide d'un matrice entière de déterminant $\pm 1$. En prenant le carré du déterminant dans la définition, on obtient bien une valeur indépendante de la base. Le nombre $\mathcal{D}_k$ est alors un élément de $\mathbb{Z}$, qui peut tout à fait être négatif (si $k$ possède des plongements complexes). On préférera pour notre part travailler avec sa valeur absolue

$$\mathscr{D}_k \quad := \quad |\mathcal{D}_k|\,, \tag{4.5}$$

qu'on appelera également *discriminant* de $k$. Sans autre précision, par « discriminant de $k$ » on entendra donc cette variante de la définition standard.

**Remarque 4.16.** Il serait tentant d'utiliser la terminologie « discriminant absolu » pour faire référence à $\mathscr{D}_k$, afin de le distinguer de $\mathcal{D}_k$. On verra cependant en §4.6 que les adjectifs « absolu / relatif » doivent être à propos du discriminant réservé pour une autre signification.

**4.17 Interprétation géométrique.** La première interprétation pour $\mathscr{D}_k$ que nous donnons est de nature géométrique, et se base sur l'inclusion $\mathscr{O}_k \subset k_\infty$ rappelée au paragraphe §4.3. Supposons pour simplifier que $k$ soit totalement réel. Les colonnes de la matrice $(\sigma_i\omega_j)$ apparaissant dans (4.4) correspondent en fait à $\omega_1, \ldots, \omega_d$, vus comme vecteurs de $k_\infty$ écrits en base canonique. La valeur absolue du déterminant de cette matrice, égale à $\sqrt{\mathscr{D}_k}$, donne donc le volume du domaine fondamental de $\mathscr{O}_k$ dans $k_\infty$. Le volume est ici entendu avec la normalisation suivante : les vecteurs de la base canonique ont longueur 1.

**Remarque 4.18.** Lorsque $k$ n'est pas totalement réel cette interprétation n'est plus directement correcte. La normalisation du volume sur $k_\infty$ à choisir pour interpréter $\sqrt{\mathscr{D}_k}$ comme le covolume de $\mathscr{O}_k$ n'est alors plus si évidente. Elle demande en effet pour chaque facteur $\mathbb{C}$ dans $k_\infty$ d'attribuer la valeur 2 (et non 1) à la surface déterminée par les deux vecteurs de la base canonique de $\mathbb{C}$ (i.e. 1 et $i$). Le lecteur s'en convaincra en analysant le cas de $k = \mathbb{Q}(i)$, pour lequel $\mathscr{D}_k = 4$ et $\mathscr{O}_k = \mathbb{Z}[i]$.

**4.19 Interprétation algébrique.** La deuxième signification du discriminant que nous donnons est algébrique. Elle est facile à présenter, mais nettement plus difficile à prouver. Nous avons évoqué au paragraphe §4.4 la notion de ramification d'un nombre premier $p$ dans l'extension $k|\mathbb{Q}$. Or les nombres premiers ramifiés dans $k|\mathbb{Q}$ sont exactement ceux qui divisent $\mathscr{D}_k$ (c'est un cas particulier du théorème 4.22 que nous énonçons plus bas). Notons que si nous qualifions cette propriété d' « algébrique », elle est en fait plus précisément exprimée par une analogie avec la géométrie algébrique, cf. [Neu99, Ch. III §2]. Une conséquence, qu'on obtient habituellement par d'autres chemins moins ardus, est la suivante : il n'existe qu'un nombre fini de nombres premiers ramifié dans l'extension $k|\mathbb{Q}$.

## §4.6 Extensions relatives

Nous avons porté notre attention pour l'instant sur les extensions finies de $\mathbb{Q}$. Soit $\ell$ un corps de nombres qui contient un autre corps de nombres $k$. Il vaut alors également la peine de considérer $\ell$ sous l'angle de l'extension $\ell|k$. Pour $k \neq \mathbb{Q}$ on parlera d'une extension *relative*, par opposition à l'extension $\ell|\mathbb{Q}$ qui est dite *absolue*. Certains concepts énoncés jusqu'à maintenant pour le cas absolu se généralisent ici pour l'étude de $\mathscr{O}_\ell$ comme un $\mathscr{O}_k$-module (plutôt que comme un $\mathbb{Z}$-module). Ce paragraphe présentera surtout une généralisation adéquate du discriminant.

Tout comme les idéaux premiers $\mathfrak{p}$ de $\mathscr{O}_k$ se trouvent chacun « au-dessus » d'un nombre premier $p \in \mathbb{Z}$, on peut obtenir les idéaux premiers $\mathfrak{P}$ de $\mathscr{O}_\ell$ en énumérant les idéaux qui divisent les idéaux $\mathfrak{p}\mathscr{O}_\ell$. De façon similaire au cas absolu

on utilise la notation $\mathfrak{P}|\mathfrak{p}$ dans la situation où $\mathfrak{P}$ apparaît dans la factorisation de $\mathfrak{p}\mathscr{O}_\ell$ dans $\mathscr{O}_\ell$. La division est bien sûr transitive : si $\mathfrak{P}|\mathfrak{p}$ et $\mathfrak{p}|p$, alors $\mathfrak{P}|p$.

Comme $\mathscr{O}_k$ n'est pas forcément un anneau principal (si $h_k \neq 1$), l'idée de la preuve de la proposition 4.6 n'est pas applicable. Ainsi nous ne pouvons garantir que $\mathscr{O}_\ell$ soit libre sur $\mathscr{O}_k$ et la notion de discriminant relatif ne peut se définir de façon tout-à-fait analogue à ce qui a été fait en §4.5 pour le cas absolu. Nous utilisons ici les notations $t := [\ell : k]$ et $\sigma_i : \ell \to \overline{k}$ pour les $t$ $k$-monomorphismes associés à l'extension $\ell|k$.

**Définition 4.20.** Soit $\mathfrak{d}_{\ell|k}$ l'idéal dans $\mathscr{O}_k$ engendré par tous les éléments de la forme

$$\det\Big((\sigma_i a_j)_{1\leq i,j\leq t}\Big)^2,$$

où $a_1, \ldots, a_t$ sont des éléments de $\mathscr{O}_\ell$ linéairement indépendants sur $k$. L'idéal $\mathfrak{d}_{\ell|k}$ est appelé *discriminant relatif* de l'extension $\ell|k$. De façon similaire à ce qui apparaît en §4.5, on utilisera également (et même de préférence) la désignation *discriminant relatif* pour référer au nombre entier :

$$\mathscr{D}_{\ell|k} \quad := \quad \mathcal{N}_{k|\mathbb{Q}}(\mathfrak{d}_{\ell|k})$$

Le calcul du discriminant relatif $\mathscr{D}_{\ell|k}$ suit du calcul des discriminants absolus [Neu99, Ch. III (2.10)] :

**Proposition 4.21.** *Pour l'extension de corps de nombres $\ell|k$, le discriminant relatif peut se calculer par :*

$$\mathscr{D}_{\ell|k} \quad = \quad \frac{\mathscr{D}_\ell}{\mathscr{D}_k{}^{[\ell:k]}}.$$

En comparaison avec le cas $k = \mathbb{Q}$, la généralisation que constitue le discriminant relatif perd l'interprétation géométrique expliquée en §4.5. Par contre l'interprétation « algébrique » de 4.19 est encore valable [Neu99, Ch. III (2.12)] :

**Théorème 4.22.** *Soit $\mathfrak{p}$ un idéal premier dans $\mathscr{O}_k$. Alors la factorisation de $\mathfrak{p}$ en idéaux premiers :*

$$\mathfrak{p}\mathscr{O}_\ell \quad = \quad \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_\alpha^{e_\alpha}$$

*possède au moins un facteur redondant (i.e. $\exists\ e_i > 1$) exactement lorsque $\mathfrak{p}$ divise $\mathfrak{d}_{\ell|k}$.*

Le contenu de §4.4 se généralise au cas des extensions relatives, et on utilise une notation et un vocabulaire similaire. Ainsi on désigne par $e_{\mathfrak{P}|\mathfrak{p}}$ la multiplicité du facteur $\mathfrak{P}$ dans la factorisation de l'idéal $\mathfrak{p}$ dans $\mathscr{O}_\ell$, appelé *indice de ramification de $\mathfrak{P}$ dans $\ell|k$*. De même on notera par $f_{\mathfrak{P}|\mathfrak{p}} := [\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}]$ le *degré d'inertie de $\mathfrak{P}$ dans $\ell|k$*. $\mathfrak{P}$ est dit *ramifié dans $\ell|k$* si $e_{\mathfrak{P}|\mathfrak{p}} > 1$. L'idéal $\mathfrak{p}$ est lui-même *ramifié dans $\ell|k$* s'il existe un tel facteur $\mathfrak{P}|\mathfrak{p}$ ramifié. On dit que $\mathfrak{p}$ est *inerte dans $\ell|k$* si $\mathfrak{p}\mathscr{O}_\ell$ est un idéal premier de $\mathscr{O}_\ell$. Toutes ces notions généralisent les définitions 4.13 et 4.15. La proposition 4.14 se généralise également : pour chaque idéal premier $\mathfrak{p}$ de $\mathscr{O}_k$, on a l'égalité :

$$\sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}} \quad = \quad [\ell : k]. \tag{4.6}$$

## §4.7 Fonctions zêta et fonctions $L$

Ce paragraphe présente brièvement certaines fonctions analytiques liées aux extensions de corps de nombres : les *fonctions zêta* et *fonctions L*. Elles apparaissent dans l'expression du volume des quotients arithmétiques (notamment dans les théorèmes 1.3 et 1.4). On réfère à [Lan86, Ch. VIII] pour une exposition plus détaillée de ces fonctions.

Pour un corps de nombres $k$, on définit sur le demi-plan complexe $\mathrm{Re}(s) > 1$ la fonction donnée par

$$\zeta_k(s) \quad := \quad \prod_{\mathfrak{p}} \frac{1}{1 - \mathcal{N}_{k|\mathbb{Q}}(\mathfrak{p})^{-s}},$$

où l'indice $\mathfrak{p}$ parcourt tous les idéaux premiers de $\mathscr{O}_k$. Pour $k = \mathbb{Q}$, on obtient la fonction $\zeta$ de Riemann sous sa forme produit due à Euler : $\zeta_{\mathbb{Q}} = \zeta$. Tout comme pour la fonction zêta de Riemann, la fonction $\zeta_k$ se prolonge vers une fonction analytique sur $\mathbb{C} \smallsetminus \{1\}$. Cet aspect analytique ne jouera cependant aucun rôle dans cette thèse : nous n'évaluerons $\zeta_k$ que sur des entiers $\geq 2$.

Soit $\ell$ un second corps de nombres qui contient $\ell$. Selon l'égalité (4.6) un idéal premier $\mathfrak{p}$ de $\mathscr{O}_k$ se factorise en au plus $[\ell : k]$ idéaux premiers de $\mathscr{O}_\ell$. En ajoutant à ceci que pour $\mathfrak{P}|\mathfrak{p}$ on a $\mathcal{N}_{\ell|\mathbb{Q}}(\mathfrak{P}) \geq \mathcal{N}_{k|\mathbb{Q}}(\mathfrak{p})$, on voit facilement que pour $s > 1$ :

$$\zeta_\ell(s) \quad \leq \quad \zeta_k(s)^{[\ell:k]}. \tag{4.7}$$

Pour le reste de ce paragraphe on suppose que l'extension $\ell|k$ est quadratique, i.e. $[\ell : k] = 2$. Dans ce cas on considère la fonction :

$$L_{\ell|k} \quad = \quad \zeta_\ell / \zeta_k, \tag{4.8}$$

qui s'écrit donc comme

$$L_{\ell|k}(s) \quad = \quad \prod_{\mathfrak{p}} \left( \left(1 - \mathcal{N}_{k|\mathbb{Q}}(\mathfrak{p})^{-s}\right) \prod_{\mathfrak{P}|\mathfrak{p}} \frac{1}{1 - \mathcal{N}_{k|\mathbb{Q}}(\mathfrak{P})^{-s}} \right). \tag{4.9}$$

Comme $\ell|k$ est quadratique il y a selon (4.6) pour l'idéal premier $\mathfrak{p}$ de $\mathscr{O}_k$ exactement trois possibilités de factorisation dans $\mathscr{O}_\ell$ en idéaux $\mathfrak{P}|\mathfrak{p}$ :

- $\mathfrak{p}$ est inerte : $\mathfrak{p} = \mathfrak{P}$.
- $\mathfrak{p}$ est ramifé : $\mathfrak{p} = \mathfrak{P}^2$.
- $\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2$ pour deux idéaux disctincts $\mathfrak{P}_i|\mathfrak{p}$. On dit dans ce cas que $\mathfrak{p}$ est *décomposé dans* $\ell|k$ .

En analysant ces trois possibilités, on observe à partir de (4.9) que la fonction $L_{\ell|k}$ prend la forme :

$$L_{\ell|k}(s) \quad = \quad \prod_{\mathfrak{p} \text{ décomposé}} \frac{1}{1 - \mathcal{N}_{k|\mathbb{Q}}(\mathfrak{p})^{-s}} \prod_{\mathfrak{p} \text{ inerte}} \frac{1}{1 + \mathcal{N}_{k|\mathbb{Q}}(\mathfrak{p})^{-s}}, \tag{4.10}$$

avec $\mathfrak{p}$ qui parcourt les idéaux premiers de $\mathscr{O}_k$ non ramifiés dans $\ell|k$.

**Remarque 4.23.** Les fonctions $L$ sont habituellement introduites de façon différente (et plus générale), la relation (4.8) n'étant qu'une proprieté valable dans le cas particulier d'une extension $\ell|k$ quadratique [Lan86, Ch.XII §1].

## §4.8 Groupe des unités

On conclut ce chapitre en explicitant la structure du *groupe des unités* $\mathscr{O}_k^\times$ de l'anneau des entiers algébriques $\mathscr{O}_k$. On utilisera la notation suivante pour ce groupe :

$$U_k \quad := \quad \mathscr{O}_k^\times. \tag{4.11}$$

Remarquons qu'un élément $x$ de $\mathscr{O}_k$ est dans $U_k$ exactement lorsque $(x) = \mathscr{O}_k$. On peut interpréter cela en disant que pour $x \in U_k$ la factorisation de $(x)$ en idéaux premiers est un produit vide (i.e l'indice $\alpha$ dans le théorème 4.1 vaudrait 0).

On notera par $\mu(k)$ le groupe multiplicatif des racines de l'unité dans $k$. Il s'agit d'un groupe cyclique fini. Comme d'habitude $(r, s)$ désigne la signature de $k$. La structure de $U_k$ est alors donnée par le fameux théorème [Neu99, Ch. I (7.4)] :

**Théorème 4.24** (des unités de Dirichlet)**.** *Il existe un isomorphisme :*

$$U_k \quad \cong \quad \mu(k) \times \mathbb{Z}^{r+s-1}.$$

**Définition 4.25.** Une base sur $\mathbb{Z}$ de $U_k$ est appelée *système d'unités fondamentales* de $k$.

# Chapitre 5. Complétions de corps de nombres

Chaque plongement archimédien $\sigma : k \to \mathbb{C}$ d'un corps de nombres $k$ nous donne une extension transcendante $\mathbb{C}|k$ (si $\sigma$ est complexe) ou $\mathbb{R}|k$ (si $\sigma$ est réel). D'autres extensions transcendantes de $k$ sont intéressantes en théorie des nombres. Celles-ci sont étroitement liées aux idéaux premiers de $\mathscr{O}_k$. Nous avons ainsi un moyen de réunir les paragraphes §4.3 et §4.4 sous un même langage. Cette approche donne une autre vision du problème de l'étude de $(k, \mathscr{O}_k)$. Cette vision est à la base d'une étude efficace des sous-groupes arithmétiques, en particulier pour le problème du calcul de volume.

Notre présentation du sujet est plus concrète que le traitement donné dans [Neu99], et à cet égard il est peut-être plus convenable de se référer à [Lan86]. Dans tout ce chapitre $k$ désigne un corps de nombres.

## §5.1 Valeurs absolues et complétions

**Définition 5.1.** Une *valeur absolue* sur $k$ est une application

$$\begin{aligned} \|\cdot\|_v \quad : \quad & k \to \mathbb{R}_{\geq 0} \\ & x \mapsto \|x\|_v \end{aligned}$$

respectant les propriétés suivantes ($\forall\, x, y \in k$) :

1. $\|x\|_v = 0 \iff x = 0$.
2. $\|x \cdot y\|_v = \|x\|_v \cdot \|y\|_v$.
3. $\|x + y\|_v \leq \|x\|_v + \|y\|_v$.

Utiliser un indice (ici $v$) dans la notation des valeurs absolues permettra de les distinguer entre elles. Cela sera utile lorsque nous considérerons plusieurs valeurs absolues simultanément sur $k$.

**Remarque 5.2.** La notation $|\cdot|$ est généralement préférée à $\|\cdot\|$. Nous réserverons cependant le symbole $|\cdot|$ pour une certaine classe de « valeurs absolues » sur les corps de nombres, normalisées d'une manière particulière.

Les propriétés de la définition 5.1 font de $(k, \|\cdot\|_v)$ un corps topologique, grâce à la métrique donnée par $d(x, y) := \|x - y\|_v$. Un exemple évident de valeur absolue est la valeur absolue usuelle $|\cdot|$ sur $\mathbb{Q}$, que nous noterons désormais par $\|\cdot\|_\infty$. Comme espace métrique, $(\mathbb{Q}, \|\cdot\|_\infty)$ n'est pas complet. Par un processus de complétion on en obtient les nombres réels $\mathbb{R}$. Nous expliquons dans ce qui suit que cette idée reste valable en général.

Pour une valeur absolue $\|\cdot\|_v$ quelconque sur $k$, dénotons par $\mathfrak{S}$ l'anneau des suites de Cauchy (les opérations $+$ et $\cdot$ étant effectuées terme à terme entre

deux suites) et par $\mathfrak{S}_0$ l'idéal de $\mathfrak{S}$ constitué des *suites nulles* (i.e. des suites qui convergent vers 0). On peut vérifier que $\mathfrak{S}_0$ est un idéal maximal, ce qui fait de $\mathfrak{S}/\mathfrak{S}_0$ un corps, que nous noterons par $k_v$. En associant à chaque élément $x \in k$ la suite constante $(x)_{n\geq 0} \in \mathfrak{S}$, on voit $k$ comme sous-corps de $k_v$. On peut de plus étendre la valeur absolue $\|\cdot\|_v$ à ce corps en définissant pour une suite $(x_n) \in \mathfrak{S}$ :

$$\|(x_n)\|_v := \lim_{n\to\infty} \|x_n\|_v .$$

Tous les éléments d'une même classe modulo $\mathfrak{S}_0$ ont alors même limite et cette limite existe toujours, la suite $(\|x_n\|_v)$ étant une suite de Cauchy dans $\mathbb{R}_{\geq 0}$. On a alors [Neu99, Ch. II §4] :

**Proposition 5.3.** *Le corps $k_v = \mathfrak{S}/\mathfrak{S}_0$ muni de la valeur absolue $\|\cdot\|_v$ est complet. De plus $k$ est dense dans $k_v$.*

On appellera le corps topologique $k_v$ le *complété* de $k$ par rapport à la valeur absolue $\|\cdot\|_v$. On dit aussi que $k$ est obtenu par *complétion* par rapport à $\|\cdot\|_v$. On peut montrer que ce complété est (à $k$-isomorphisme près) l'unique extension de $k$ sur lequel $\|\cdot\|_v$ est prolongée de façon à obtenir les propriétés de la proposition 5.3.

Supposons être en présence d'une extension finie de corps $\ell|k$. Lorsque $\|\cdot\|_w$ est une valeur absolue de $\ell$ qui étend la valeur absolue $\|\cdot\|_v$ sur $k$, on utilisera la notation suivante au niveau des indices :

$$w|v. \tag{5.1}$$

Dans ce cas, le complété $\ell_w$ contient de manière évidente $k_v$. Etant fixé une valeur absolue $\|\cdot\|_v$ sur $k$, on définit l'anneau

$$\ell_v \quad := \quad \prod_{w|v} \ell_w, \tag{5.2}$$

le produit parcourant tous les complétés liées à des extensions distinctes $\|\cdot\|_w$ de $\|\cdot\|_v$. Les corps $\ell$ et $k_v$ seront alors considérés comme inclus diagonalement dans $\ell_v$.

**Remarque 5.4.** On définit habituellement $\ell_v$ comme le produit tensoriel

$$\ell \otimes_k k_v,$$

puis on montre l'existence d'un isomorphisme canonique entre ce produit tensoriel et la forme plus explicite donnée par (5.2). Pour $k_v = \mathbb{R}$, le paragraphe suivant montrera que c'est justement la situation de la proposition 3.13 (où $k$ correspond à $\mathbb{Q}$ et $\ell$ à $k$).

Cette remarque permet de constater le résultat suivant :

**Proposition 5.5.** *On a l'égalité :*

$$[\ell : k] \quad = \quad \sum_{w|v} [\ell_w : k_v].$$

## §5.2 Complétions archimédiennes

Pour la notation introduite en §5.1 on a $\mathbb{Q}_\infty = \mathbb{R}$. La valeur absolue $\|\cdot\|_\infty$ correspond à la valeur absolue usuelle sur $\mathbb{R}$, et celle-ci s'étend à la valeur absolue (ou *module*) définie usuellement sur $\mathbb{C}$. On notera également par $\|\cdot\|_\infty$ cette extension sur tout $\mathbb{C}$. Pour chaque plongement archimédien $k \to \mathbb{C}$, on considère la valeur absolue définie par

$$\|x\|_\sigma \quad := \quad \|\sigma x\|_\infty \quad (x \in k). \tag{5.3}$$

On a donc $\sigma|\infty$ selon la notation (5.1). Le complété $k_\sigma$ d'un corps de nombres obtenu grâce à une telle valeur absolue sera dit *archimédien*. On remarque que pour deux plongements archimédiens conjugués $\sigma$ et $\overline{\sigma}$, on a $\|\cdot\|_\sigma = \|\cdot\|_{\overline{\sigma}}$. Si $(r, s)$ est la signature du corps $k$, il existe alors exactement $r + s$ complétés archimédiens de $k$. Ils sont décrits par la proposition suivante [Lan86, Ch. II §1] :

**Proposition 5.6.**

1. *Si $\sigma$ est réel, alors $k_\sigma$ est isomorphe (comme anneau topologique) à $\mathbb{R}$. La structure de $k$-algèbre sur $k_\sigma$ correspond à la structure de $k$-algèbre sur $\mathbb{R}$ donnée par l'inclusion $\sigma(k) \subset \mathbb{R}$.*
2. *Si $\sigma$ est complexe, alors $k_\sigma$ est isomorphe à $\mathbb{C}$. La structure de $k$-algèbre sur $k_\sigma$ correspond à la structure de $k$-algèbre sur $\mathbb{C}$ donnée par l'inclusion $\sigma(k) \subset \mathbb{C}$ (ou de façon équivalente par l'inclusion $\overline{\sigma}(k) \subset \mathbb{C}$).*

Cette proposition permet de voir que l'espace vectoriel réel $k_\infty$ défini selon (5.2) par :

$$k_\infty \quad = \quad \prod_{\sigma|\infty} k_\sigma, \tag{5.4}$$

correspond bien à l'espace $k_\infty$ qui a été défini en (4.3). On préférera désormais travailler avec l'écriture plus concise donnée par (5.4).

**Remarque 5.7.** L'espace $k_\infty$ ne contient qu'un seul facteur direct pour chaque plongement complexe. Ceci tient dans la définition (5.2), où l'on parcourt l'ensemble des complétions liées à des valeurs absolues distinctes (deux plongements conjugués donnant même valeur absolue et ainsi en quelque sorte une redondance d'information). Il est intéressant de constater que ce même fait pouvait se justifier dans l'exemple 4.11 de façon différente. Ces deux interprétations sont en fait liées par la remarque 5.4 : $\mathscr{O}_k$ est discret dans $k \otimes_k \mathbb{R}$, et ce dernier espace est isomorphe au produit $\prod_{\sigma|\infty} k_v$.

## §5.3 Complétions $\mathfrak{p}$-adiques

Aux complétions archimédiennes d'un corps de nombres s'ajoutent un autre type de complétions, qui apparaît sans doute comme plus exotique lors d'une première rencontre. Fixons pour l'instant un idéal premier $\mathfrak{p}$ de $\mathscr{O}_k$. Un tel choix détermine une application :

$$\tilde{v}_\mathfrak{p} \quad : \quad k^\times \to \mathbb{Z}, \tag{5.5}$$

définie comme suit : $\tilde{v}_{\mathfrak{p}}(x)$ est la multiplicité de l'idéal $\mathfrak{p}$ dans la factorisation en idéaux premiers de l'idéal $(x)$. Par exemple, si $\mathfrak{p}$ est au-dessus du nombre premier $p$ (i.e. $\mathfrak{p}|p$), alors $\tilde{v}_{\mathfrak{p}}(p)$ est égal à $e_{\mathfrak{p}}$, l'indice de ramification de $\mathfrak{p}$ dans $k|\mathbb{Q}$. L'application $\tilde{v}_{\mathfrak{p}}$ est ce que l'on appelle une *valuation* de $k$. Cette valuation est *normalisée*, dans le sens où $\tilde{v}_{\mathfrak{p}}(k^\times) = \mathbb{Z}$.

A partir de la valuation normalisée $\tilde{v}_{\mathfrak{p}}$ on définit la *valeur absolue* $\mathfrak{p}$*-adique*, comme suit : $\|0\|_{\mathfrak{p}} := 0$ et pour $x \in k^\times$ :

$$\|x\|_{\mathfrak{p}} \quad := \quad \left(\frac{1}{p^{1/e_{\mathfrak{p}}}}\right)^{\tilde{v}_{\mathfrak{p}}(x)}$$

où $\mathfrak{p}$ divise $p$ et $e_{\mathfrak{p}}$ est l'indice de ramification de $\mathfrak{p}$. A chaque idéal premier $\mathfrak{p}$ de $\mathscr{O}_k$ est ainsi associé une valeur absolue sur $k$ et par conséquent un complété $k_{\mathfrak{p}}$. Un corps obtenu par pareille complétion d'un corps de nombres est appelé *corps de nombres* $\mathfrak{p}$*-adiques* ou plus brièvement *corps* $\mathfrak{p}$*-adique* (le « $\mathfrak{p}$ » étant dans cette terminologie un symbole fixe). Ces corps sont des exemples de corps dits *locaux*.

**Exemple 5.8.** Considérons le cas $k = \mathbb{Q}$. Soit $p$ un nombre entier premier et notons par $v_p := \tilde{v}_{(p)}$ sa valuation normalisée associée. On a ici $e_{(p)} = 1$. On note par $\|\cdot\|_p$ la *valeur absolue p-adique* correspondante. Le corps des *nombres p-adiques* $\mathbb{Q}_p$ peut s'identifier avec l'ensemble des séries de Laurent en $p$ avec des coefficients dans l'anneau $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$. Le livre [Gou97] donne une très bonne introduction à l'étude des nombres $p$-adiques.

On revient à la situation d'une extension $k|\mathbb{Q}$. Si $\mathfrak{p} \subset \mathscr{O}_k$ est au-dessus de $p$, alors on constate que la valeur absolue $\|\cdot\|_{\mathfrak{p}}$ sur $k$ étend la valeur absolue $p$-adique $\|\cdot\|_p$ définie sur $\mathbb{Q}$. La notation $\mathfrak{p}|p$ possède alors une double interprétation : d'une part au sens de la division d'idéaux vue en §4.4, et d'autre part dans le sens donné en (5.1). On peut en fait voir que plus généralement, pour une extension de corps de nombres $\ell|k$, si $\mathfrak{P}$ est un idéal premier de $\mathscr{O}_\ell$ et $\mathfrak{p}$ un idéal premier de $\mathscr{O}_k$ alors on a aussi cette double signification pour l'écriture $\mathfrak{P}|\mathfrak{p}$.

La valeur absolue $\mathfrak{p}$-adique possède une inégalité triangulaire plus forte que celle donnée dans la définition 5.1. En effet pour deux éléments $x, y \in k$, on a :

$$\|x + y\|_{\mathfrak{p}} \quad \leq \quad \max\left\{\|x\|_{\mathfrak{p}}, \|y\|_{\mathfrak{p}}\right\}. \tag{5.6}$$

Cette propriété, souvent qualifiée d'*ultramétrique*, reste valable pour la valeur absolue étendue sur le complété $k_{\mathfrak{p}}$. Un corps dans lequel (5.6) est valable est dit *non archimédien*. Le sous-ensemble de $k_{\mathfrak{p}}$ donné par

$$\mathscr{O}_{\mathfrak{p}} \quad := \quad \left\{x \in k_{\mathfrak{p}} \;\middle|\; \|x\|_{\mathfrak{p}} \leq 1\right\} \tag{5.7}$$

est donc non seulement fermé pour la multiplication (comme ce serait le cas pour n'importe quelle valeur absolue), mais également pour l'addition. Cela fait de $\mathscr{O}_{\mathfrak{p}}$ un sous-anneau de $k_{\mathfrak{p}}$, qu'on appelle *anneau des entiers* $\mathfrak{p}$*-adiques*. Clairement on a $\mathscr{O}_k \subset \mathscr{O}_{\mathfrak{p}}$ ; plus précisément on peut voir que $\mathscr{O}_{\mathfrak{p}}$ est l'adhérence de $\mathscr{O}_k$ dans $k_{\mathfrak{p}}$. De plus, $x \in k$ est entier algébrique exactement lorsqu'il appartient à $\mathscr{O}_{\mathfrak{p}}$ pour tous les idéaux premiers $\mathfrak{p}$. Cela explique la terminologie introduite. La définition (5.7) de $\mathscr{O}_{\mathfrak{p}}$ est analogue à celle du disque unité fermé dans $\mathbb{C}$ (ou de l'intervalle $[-1, 1]$ dans $\mathbb{R}$). Une ressemblance entre ces deux situations apparaît bel et bien au travers du résultat suivant [Neu99, Ch. II (5.1)] :

**Proposition 5.9.** *L'anneau topologique $\mathscr{O}_\mathfrak{p}$ est compact. En conséquence le corps $k_\mathfrak{p}$ est localement compact.*

Par contre une différence essentielle avec le cas archimédien apparaît : $\mathscr{O}_\mathfrak{p}$ est ouvert dans $k_\mathfrak{p}$.

**Exemple 5.10.** Si le corps $\mathbb{Q}_p$ peut s'écrire comme l'ensemble des séries de Laurent en $p$, son sous-anneau compact $\mathbb{Z}_p$ des *entiers p-adiques* correspond lui aux séries entières en $p$ à coefficients $a_i$ dans le corps fini $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. L'application

$$\begin{array}{ccc} \mathbb{Z}_p & \to & \mathbb{F}_p \\ \sum_{i=0}^{\infty} a_i p^i & \mapsto & a_0 \end{array}$$

est alors un homomorphisme qui généralise la réduction modulo $p$ définie sur $\mathbb{Z}$.

L'homomorphisme de réduction du dernier exemple se généralise pour le corps de nombres $k$. Pour chaque idéal premier $\mathfrak{p}$ de $\mathscr{O}_k$, on a un homomorphisme dit *de réduction modulo* $\mathfrak{p}$ :

$$\mathscr{O}_\mathfrak{p} \quad \to \quad \mathbb{F}_\mathfrak{p}, \tag{5.8}$$

qui restreint à $\mathscr{O}_k$ correspond à la projection naturelle $\mathscr{O}_k \to \mathscr{O}_k/\mathfrak{p}$.

Si $K|k_\mathfrak{p}$ est une extension finie, la valuation $\tilde{v}_\mathfrak{p}$ s'étend en fait de façon unique comme valuation (pas nécessairement normalisée) sur $K^\times$. On dit alors que l'extension $K|k_\mathfrak{p}$ est *non ramifiée* si cette extension de $\tilde{v}_\mathfrak{p}$ reste normalisée, i.e. si $\tilde{v}_\mathfrak{p}(K^\times) = \mathbb{Z}$. La terminologie s'explique naturellement : si $\mathfrak{P}$ est un idéal premier de $\mathscr{O}_\ell$ (pour une extension $\ell|k$) tel que $\mathfrak{P}|\mathfrak{p}$, alors $\ell_\mathfrak{P}|k_\mathfrak{p}$ est non ramifiée exactement lorsque $\mathfrak{P}$ n'est pas ramifié dans l'extension $\ell|k$. De manière analogue à la définition d'une clôture algébrique d'un corps, il existe pour $k_\mathfrak{p}$ une *extension maximale non ramifiée* notée $\hat{k}_\mathfrak{p}$ et qui contient toutes les extensions finies non ramifiées de $k_\mathfrak{p}$. Le corps $\hat{k}_\mathfrak{p}$ possède une métrique naturelle, mais il n'est plus localement compact. Il existe une définition d'un sous-anneau $\hat{\mathscr{O}}_\mathfrak{p}$ d'*entiers* de $\hat{k}_\mathfrak{p}$, pour lequel le quotient $\hat{k}_\mathfrak{p}/\hat{\mathscr{O}}_\mathfrak{p}$ est isomorphe à la clôture algébrique $\overline{\mathbb{F}}_\mathfrak{p}$ de $\mathbb{F}_\mathfrak{p}$. Le corps $\hat{k}_\mathfrak{p}$ n'est pas $\mathfrak{p}$-adique, mais reste un exemple de corps local.

## §5.4 Places d'un corps de nombres

Pour le corps de nombres $k$ notons par $V_\mathrm{f} = V_\mathrm{f}(k)$ l'ensemble des idéaux premiers de $\mathscr{O}_k$. On va considérer dans la suite $V_\mathrm{f}$ comme un ensemble d'indices $v$ pour lesquels le complété $k_v$ est défini. De manière analogue, soit $V_\infty = V_\infty(k)$ l'ensemble d'indices $\{\sigma\}$ tel que $k_\sigma$ parcourt tous les complétés archimédiens de $k$ ($V_\infty$ est donc en bijection avec $\{[\sigma] \mid \sigma$ plongement archimédien$\}$). On note alors par $V = V(k)$ la réunion de ces deux ensembles : $V := V_\infty \cup V_\mathrm{f}$. Un élément de $V$ est une *place* du corps $k$. On dit que la place $v \in V$ est *finie* si $v \in V_\mathrm{f}$, et *infinie* si $v \in V_\infty$.

**Remarque 5.11.** L'ensemble $V$ des places de $k$ peut être défini plus subtilement comme un ensemble de classes d'équivalence de valeur absolues sur $k$, deux valeurs absolues étant définies équivalentes lorsqu'elles induisent la même topologie sur $k$. On peut en effet montrer que les complétions archimédiennes et $\mathfrak{p}$-adiques donnent à isomorphisme près tous les complétés possibles de $k$.

Pour chaque place $v \in V$ on a un corps localement compact $k_v$. Si la place $v$ est finie, on dispose de plus du sous-anneau compact $\mathscr{O}_v$, ainsi que de l'homomorphisme $\mathscr{O}_v \to \mathbb{F}_v$ de réduction modulo $v$ ; $k_v$ est inclus dans son extension maximale non ramifiée $\hat{k}_v$. On note encore par $\tilde{v}$ la valuation normalisée définie en (5.5) par la place finie $v$. On a donc par définition $\tilde{v}(k^\times) = \mathbb{Z}$.

Sur chaque complété $k_v$ ($v \in V$) on a bien sûr la valeur absolue $\|\cdot\|_v$. On aura cependant avantage à renormaliser cette valeur absolue comme suit :

$$|\cdot|_v \quad := \quad \begin{cases} \|\cdot\|_v & \text{si } v \in V_\infty \text{ est réelle ;} \\ \|\cdot\|_v^2 & \text{si } v \in V_\infty \text{ est complexe ;} \\ \|\cdot\|_{\mathfrak{p}}^{e_\mathfrak{p} f_\mathfrak{p}} & \text{si } v = \mathfrak{p} \in V_{\mathrm{f}}, \end{cases} \tag{5.9}$$

où $e_\mathfrak{p}$ désigne l'indice de ramification de $\mathfrak{p}$ dans $k|\mathbb{Q}$ et $f_\mathfrak{p}$ est son degré d'inertie. On appellera $|\cdot|_v$ la *valeur absolue normalisée* sur $k_v$. Il s'agit d'une application continue sur $k_v$.

**Remarque 5.12.** Pour $v \in V_\infty$ complexe la valeur absolue normalisée $|\cdot|_v$ n'est pas une valeur absolue au sens de la définition 5.1 : l'inégalité triangulaire n'est plus respectée. Dans les autres cas il s'agit bien de valeurs absolues, et la topologie que $|\cdot|_v$ induit sur $k_v$ correspond à la topologie induite par $\|\cdot\|_v$.

La raison que nous invoquons dans un premier temps pour justifier cette renormalisation des valeurs absolues est qu'elle permet la validité du résultat suivant :

**Proposition 5.13** (Formule du produit)**.** *Pour $x \in k^\times$, on a :*

$$\prod_{v \in V} |x|_v \quad = \quad 1,$$

*avec $|x|_v = 1$ pour presque tous les $v \in V$.*

Idée de la preuve. Pour $k = \mathbb{Q}$ la formule est facile à voir. Pour une extension $k|\mathbb{Q}$ non triviale on va se ramener au cas de $\mathbb{Q}$. Pour cela on utilise le fait que pour $v \in V(\mathbb{Q})$ et $x \in k$, on a :

$$\left|N_{k|\mathbb{Q}}(x)\right|_v \quad = \quad \prod_{w|v} |x|_w \,, \tag{5.10}$$

où $w \in V(k)$. C'est facile à voir pour $v = \infty$. Pour $v = p$, il s'agit essentiellement d'une reformulation de la proposition 4.14. On a alors :

$$\begin{aligned} 1 \quad &= \quad \prod_{v \in V(\mathbb{Q})} \left|N_{k|\mathbb{Q}}(x)\right|_v \\ &= \quad \prod_{v \in V(\mathbb{Q})} \prod_{w|v} |x|_w \\ &= \quad \prod_{w \in V(k)} |x|_w \,. \end{aligned}$$

□

Il existe une justification plus subtile pour l'introduction de la normalisation $|\cdot|_v$. Pour le voir on fixe une mesure de Haar $\mu$ sur $(k_v, +)$. Un élément $a \in k_v^\times$ détermine une mesure de Haar $\mu_a$ définie par :

$$\mu_a(F) \quad := \quad \mu(aF)$$

et $\mu_a$ doit nécessairement être un multiple de $\mu$. On observe alors qu'en fait $\mu_a = |a|_v \, \mu$. Ceci permet de voir que $|\cdot|_v$ peut être définie par la seule considération de $k_v$ comme corps topologique.

**5.14 Mesure de Haar normalisée sur $k_v$.** Nous fixons à présent pour chaque $v \in V$ une normalisation $\nu_v$ de la mesure de Haar sur $k_v$. Pour $v \in V_\infty$ réel, on prend la mesure standard de Lebesgue : $\nu_v([0,1]) := 1$. Pour $v \in V_\infty$ complexe on choisit $\nu_v$ comme dans la remarque 4.18 : $\nu_v([0,1] \times [0,i]) := 2$. Pour $v \in V_\mathrm{f}$ la normalisation la plus naturelle consiste à prendre $\nu_v(\mathscr{O}_v) := 1$.

Pour les places infinies, cette normalisation de la mesure est celle qui permet d'exprimer le covolume de $\mathscr{O}_k$ en fonction du discriminant (cf. 4.17). Si on considère la mesure produit $\nu_\infty := \prod_{v \in V_\infty} \nu_v$ sur $k_\infty$, on a en effet :

$$\nu_\infty(k_\infty / \mathscr{O}_k) \quad = \quad \sqrt{\mathscr{D}_k}. \tag{5.11}$$

## §5.5 Théorie adélique

Afin de considérer tous les complétés $k_v$ d'un corps $k$ en même temps, on peut travailler avec le produit $\prod_{v \in V} k_v$. Mais on perd alors un avantage que possédait chacun des $k_v$ : ce produit n'est plus localement compact. Nous voulons définir ici un anneau regroupant tous les $k_v$ tout en restant localement compact. Pour cela, notons d'abord qu'un élément $x \in k$ possède la propriété suivante : $x \in \mathscr{O}_v$ pour presque tous les $v \in V_\mathrm{f}$. Il existe donc un ensemble fini $S \subset V$ contenant $V_\infty$ et suffisamment grand pour que $x \in k$ appartienne à l'anneau :

$$\mathbb{A}_S \quad := \quad \prod_{v \in S} k_v \times \prod_{v \notin S} \mathscr{O}_v,$$

$k$ étant vu comme plongé diagonalement dans $\prod_{v \in V} k_v$. Pour chaque $S \subset V$ fini contenant $V_\infty$, on munit $\mathbb{A}_S$ de la topologie produit : $\mathbb{A}_S$ est alors localement compact. Chacun des $\mathbb{A}_S$ est un sous-ensemble du même ensemble $\prod_{v \in V} k_v$, ce qui permet de définir

$$\mathbb{A} = \mathbb{A}(k) \quad := \quad \bigcup_S \mathbb{A}_S,$$

la réunion étant indexée par tous les ensembles finis $S \subset V$ contenant $V_\infty$. On montre facilement que $\mathbb{A}$ est fermé pour l'addition et la multiplication. Si l'on munit $\mathbb{A}$ de la topologie engendrée par la topologie de chacun des $\mathbb{A}_S$, on a que $\mathbb{A}$ est un anneau topologique qui est localement compact et qui contient $k$ diagonalement. C'est l'anneau recherché. Remarquons encore qu'un ouvert de $\mathbb{A}$ est formé d'une infinité de facteurs de la forme $\mathscr{O}_v$.

**Définition 5.15.** L'anneau topologique $\mathbb{A}$ est appelé *anneau des adèles* de $k$. Un *adèle* de $k$ est donc un élément de $\mathbb{A}$.

Les adèles permettent une formulation élégante de nombreuses propriétés qui apparaissent en théorie de nombres. Fortement lié à la proposition 4.10, se retrouve le résultat suivant :

**Théorème 5.16.** *$k$ est discret dans $\mathbb{A}$.*

On définit l'anneau $\mathbb{A}_{\mathrm{f}} = \mathbb{A}_{\mathrm{f}}(k)$ des *adèles finis* de $k$ en ne considérant que les places finies :

$$\mathbb{A}_{\mathrm{f}} \quad := \quad \mathbb{A} \cap \prod_{v \in V_{\mathrm{f}}} k_v.$$

On a alors la décomposition en produit :

$$\mathbb{A} \quad = \quad k_\infty \times \mathbb{A}_{\mathrm{f}} \tag{5.12}$$

Selon le contexte, on considère $k$ comme plongé diagonalement dans $k_\infty$, $\mathbb{A}_{\mathrm{f}}$ ou tout $\mathbb{A}$. On connaît déjà les propriétés du plongement de $k$ dans $\mathbb{A}$. Le plongement de $k$ dans $\mathbb{A}_f$ présente lui un aspect topologique nouveau :

**Théorème 5.17** (d'approximation)**.** *$k$ est dense dans $\mathbb{A}_{\mathrm{f}}$.*

Ce théorème est essentiellement la formulation adélique d'un résultat fort connu : le théorème du reste chinois [Neu99, Ch. I (3.6)].

Considérons à présent la mesure de Haar $\nu_{\mathbb{A}}$ sur $\mathbb{A}$ donnée par le produit des mesures de Haar $\nu_v$ sur $k_v$ ($v \in V$) définies en 5.14. Le calcul de la mesure d'un ouvert $U$ de $\mathbb{A}$ revient à un calcul d'un produit fini de mesures, comme $U$ doit s'écrire comme un produit $U = U' \times \prod_{v \notin S} \mathscr{O}_v$, et que ce dernier facteur possède mesure 1. Le théorème d'approximation nous permet le calcul suivant :

**Proposition 5.18.** *La mesure $\nu_{\mathbb{A}}(\mathbb{A}/k)$ vaut $\sqrt{\mathscr{D}_k}$.*

Preuve. On va noter ici par $P$ l'ouvert de $\mathbb{A}_{\mathrm{f}}$ défini par $P := \prod_{v \in V_{\mathrm{f}}} \mathscr{O}_v$. Par densité de $k$ on a $k \cdot P = \mathbb{A}_{\mathrm{f}}$, et donc

$$\mathbb{A} \quad = \quad k \cdot (k_\infty \times P).$$

Si on note $P_\infty := k_\infty \times P$, on a donc un isomorphisme :

$$\mathbb{A}/k \quad \cong \quad P_\infty/(k \cap P_\infty).$$

Or $k \cap P_\infty = \mathscr{O}_k$ (plongé diagonalement dans $\mathbb{A}$). On obtient donc $\nu_{\mathbb{A}}(\mathbb{A}/k) = \nu_{\mathbb{A}}(P_\infty/\mathscr{O}_k)$, et comme $\nu_v(\mathscr{O}_v) = 1$ pour $v \in V_{\mathrm{f}}$ cette mesure correspond à la mesure donnée par (5.11). □

# Chapitre 6. Arithmétique des groupes algébriques

Ce chapitre expose la « généralisation » au cas des groupes algébriques semi-simples de certains résultats de la théorie des nombres (qui correspond au cas du groupe additif $\mathbf{G}_{\mathrm{a}}$). On utilisera pour cela une formulation adélique. Une référence très complète sur ce sujet est le chapitre 5 de [PR94].

On désignera tout au long du chapitre par $G$ un $k$-groupe algébrique semi-simple connexe, avec $k$ un corps de nombres. Pour chaque place $v \in V$, on considère le groupe $G(k_v)$ muni de la *topologie métrique*, i.e. la topologie qui provient de la valeur absolue $\|\cdot\|_v$ sur $k_v$.

## §6.1 Groupes sur les corps complets

Rappelons que la proposition 3.13 donne une identification entre le groupe $\mathbf{R}_{k|\mathbb{Q}}(G)(\mathbb{R})$ et un groupe $G_\infty$ qui y a été introduit. La théorie exposée au chapitre 5 nous permet de raccourcir l'écriture (3.4) plutôt lourde qui fût nécessaire pour définir $G_\infty$. En effet, si $\sigma$ est une place réelle, la proposition 5.6 montre que $G^\sigma(\mathbb{R})$ n'est autre que $G(k_\sigma)$ ; de même pour $\sigma$ complexe on a un isomorphisme entre $G^\sigma(\mathbb{C})$ et $G(k_\sigma)$. Clairement les facteurs de $G_\infty$ sont indexés par les places infinies de $k$, et on peut ainsi écrire :

$$G_\infty \quad = \quad \prod_{v \in V_\infty} G(k_v). \tag{6.1}$$

Cette écriture pour $G_\infty$, nettement plus agréable, sera utilisée par la suite.

Lorsque le groupe $G$ est muni d'un plongement matriciel dans $\mathrm{GL}_N$, on peut définir pour chaque place finie $v \in V_{\mathrm{f}}$ le groupe :

$$G(\mathscr{O}_v) \quad := \quad G(k_v) \cap \mathrm{GL}_N(\mathscr{O}_v). \tag{6.2}$$

Tout comme pour les sous-groupes arithmétiques, le sous-groupe $G(\mathscr{O}_v)$ varie avec le choix du plongement matriciel. On fixe pour toute la suite du chapitre un plongement de $G$. Les résultats présentés seront indépendants de ce plongement.

## §6.2 Le groupe adélique

De façon similaire à la définition de l'anneau des adèles $\mathbb{A}$, on peut définir le groupe

$$G_{\mathbb{A}} \quad := \quad \bigcup_S G_S,$$

appelé *groupe adélique* de $G$, comme réunion dans $\prod_{v\in V} G(k_v)$ des groupes

$$G_S \quad = \quad \prod_{v\in S} G(k_v) \times \prod_{v\notin S} G(\mathscr{O}_v),$$

lorsque $S$ parcourt les sous-ensembles finis de $V$ qui contiennent $V_\infty$. Tout comme pour $\mathbb{A}$, on obtient une topologie sur $G_\mathbb{A}$ qui en fait un groupe topologique localement compact. Il est alors facile de constater :

**Proposition 6.1.** *A isomorphisme près, le groupe topologique $G_\mathbb{A}$ ne dépend pas du plongement matriciel choisi pour $G$.*

Tout comme les adèles possèdent la décomposition $\mathbb{A} = k_\infty \times \mathbb{A}_\mathrm{f}$, il nous sera utile de considérer le groupe

$$G_{\mathbb{A}_\mathrm{f}} \quad := \quad G_\mathbb{A} \cap \prod_{v\in V_\mathrm{f}} G(k_v), \tag{6.3}$$

qui muni de la topologie adéquate permet d'écrire $G_\mathbb{A} = G_\infty \times G_{\mathbb{A}_\mathrm{f}}$. Le groupe $G(k)$ est vu plongé diagonalement dans $G_\infty$, $G_{\mathbb{A}_\mathrm{f}}$, ou $G_\mathbb{A}$. Il suit immédiatement de 5.16 que $G(k)$ est discret dans $G_\mathbb{A}$.

Le théorème d'approximation 5.17 n'est pas valable pour un groupe algébrique quelconque. On a en effet le résultat suivant :

**Théorème 6.2** (Approximation forte)**.** *Pour le groupe semi-simple $G$, on a que $G(k)$ est dense dans $G_{\mathbb{A}_\mathrm{f}}$ si et seulement si $G$ est simplement connexe.*

Ce théorème donne donc une importance considérable aux groupes simplement connexes. Cela explique notre volonté au paragraphe §3.4 de ramener la définition des réseaux arithmétiques à la considération de groupes simplement connexes. La partie « $\Leftarrow$ » du théorème d'approximation forte constitue l'un des résultats les plus difficiles que nous utilisons dans cette thèse. Sa démonstration utilise en effet des connaissances profondes sur les groupes semi-simples. Plusieurs auteurs (Eichler, Kneser, Platonov, etc.) ont contribué à établir le résultat. Dans [PR94, §7.4 : page 432] on trouve un aperçu historique du sujet.

## §6.3 Théorie de Tamagawa

Par compacité locale, le groupe adélique $G_\mathbb{A}$ possède une mesure de Haar, définie à un facteur près. Il existe une normalisation canonique de cette mesure, que nous présentons maintenant. Nous laissons le lecteur à la consultation de [Wei82] pour les détails. Nous supposerons ici $G$ connexe, de dimension $\dim(G) =: n$.

Considérons une forme multilinéaire alternée $\omega(e)$ définie sur le $k$-espace vectoriel $(\mathcal{T}_eG)_k$, i.e.

$$\omega(e) \quad \in \quad \bigwedge{}^d \, (\mathcal{T}_eG)_k^*,$$

pour un certain entier $d \geq 1$. Par extension, on peut également voir $\omega(e)$ comme une forme définie sur le $\overline{k}$-espace vectoriel $\mathcal{T}_eG$. Pour chaque $g \in G$, l'application $L_g : x \to gx$ de $G$ vers $G$ transporte alors $\omega(e)$ vers une $\overline{k}$-forme multilinéaire

alternée $\omega(g)$ définie sur $\mathcal{T}_g G$. Si $g \in G(k)$, la forme $\omega(g)$ peut aussi être vue comme une $k$-forme sur $(\mathcal{T}_g G)_k$. Nous avons ainsi une application

$$\omega \quad : \quad g \mapsto \omega(g)$$

définie sur tout $G$, appelée *forme extérieure invariante* (définie sur $k$). Une telle forme non nulle qui est de degré maximal (i.e. $d = n$) est appelée *forme de Tamagawa* (définie sur $k$).

**Remarque 6.3.** En remplaçant $k$ par $\mathbb{R}$ dans ce qui précède on retrouve la notion de forme différentielle invariante à gauche sur $G(\mathbb{R})$. Par intégration d'une telle forme on sait qu'on obtient une mesure de Haar sur $G(\mathbb{R})$.

L'intégration de formes différentielles sur $G(\mathbb{R})$ peut être généralisée pour donner à partir d'une forme de Tamagawa, sur chaque $G(k_v)$ une mesure de Haar. Voici l'idée de cette construction. Soit $\omega$ une forme de Tamagawa sur le $k$-groupe $G$. Localement $\omega$ peut s'écrire sous la forme bien familière :

$$\omega \quad = \quad f \, dx_1 \wedge \cdots \wedge dx_n, \tag{6.4}$$

où $x_1, \ldots, x_n$ sont les coordonnées d'une « carte rationnelle ». Si $A$ est un sous-ensemble de $G(k_v)$ qui est recouvert par cette carte $\phi = (x_1, \ldots, x_n)$, alors la mesure de Haar $\omega_v$ appliquée sur $A$ est donnée par :

$$\omega_v(A) \quad = \quad \int_{\phi(A)} |f|_v \, dx_1 \cdots dx_n, \tag{6.5}$$

où dans cette intégrale $dx_i$ renvoie à la mesure normalisée $\nu_v$ sur $k_v$ telle que choisie en 5.14. $\omega_v(A)$ est indépendant du choix d'une carte, et par recollement cela détermine bien une mesure de Haar $\omega_v$ définie sur tout $G(k_v)$.

Tout comme l'ensemble des mesures $\nu_v$ ($v \in V$) définissait la mesure $\nu_{\mathbb{A}}$ sur $\mathbb{A}$, les mesures $\omega_v$ définissent une mesure de Haar $\omega_{\mathbb{A}}$ sur $G_{\mathbb{A}}$, donnée par le produit.

**Proposition 6.4.** *La mesure $\omega_{\mathbb{A}}$ ne dépend pas du choix de la forme de Tamagawa $\omega$ sur $G$.*

Preuve. Comme une forme de Tamagawa $\omega$ est de degré maximal et invariante à gauche, elle est déterminée par un seul paramètre (un élément de $k^\times$) qui correspond à $\omega(e)$. Toute autre mesure de Tamagawa sur $G$ est donc de la forme $a\omega$, pour un $a \in k^\times$. Mais par (6.5) on a clairement $(a\omega)_v = |a|_v \, \omega_v$ et l'indépendance de $\omega_{\mathbb{A}}$ suit alors de la formule du produit (proposition 5.13). □

**Définition 6.5.** La mesure $\omega_{\mathbb{A}}$ sur $G_{\mathbb{A}}$ est la *mesure de Tamagawa* de $G$. Le nombre

$$\omega_{\mathbb{A}}\left(G_{\mathbb{A}}/G(k)\right) \cdot \mathscr{D}_k^{-\dim G/2}$$

est appelé *nombre de Tamagawa* de $G$.

**Théorème 6.6.** *Si $G$ est simplement connexe, alors son nombre de Tamagawa vaut* 1.

La démonstration de ce théorème nécessite un traitement au cas par cas, avec des efforts considérables. Pour les cas des groupes « classiques » (cf. 7.19), la démonstration du théorème est le sujet de [Wei82]. On lira [PR94, §5.3 : page 263] pour un historique de ce théorème. Notons encore que le nombre de Tamagawa d'un groupe non simplement connexe se déduit à partir de ce théorème.

## §6.4 Collections cohérentes et mesure

Remarquons qu'un sous-groupe $U < G_{\mathbb{A}_\mathrm{f}}$ définit canoniquement un sous-groupe de $G(k)$ : en effet, $G(k)$ se plonge diagonalement dans $G_{\mathbb{A}_\mathrm{f}}$ et $U \cap G(k)$ détermine alors un sous-groupe de $G(k)$. Ce sous-groupe peut à son tour se voir plongé dans $G_\infty$ de façon diagonale. En exemple, on a l'écriture du sous-groupe arithmétique $G(\mathscr{O}_k)$ comme l'intersection :

$$G(\mathscr{O}_k) \quad = \quad G(k) \cap \prod_{v \in V_\mathrm{f}} G(\mathscr{O}_v).$$

On fait remarquer ici que chaque $G(\mathscr{O}_v)$ est ouvert et compact dans $G(k_v)$. Nous allons généraliser en construisant d'autres sous-groupes arithmétiques de $G(k)$ à partir d'un produit dans $G_{\mathbb{A}_\mathrm{f}}$. Pour cela définissons :

**Définition 6.7.** Une collection $\mathscr{P} = (P_v)_{v \in V_\mathrm{f}}$ de sous-groupes $P_v \subset G(k_v)$ $(v \in V_\mathrm{f})$ est dite *cohérente* si chacun des $P_v$ est compact et si le produit $\prod_{v \in V_\mathrm{f}} P_v$ est ouvert dans $G_{\mathbb{A}_\mathrm{f}}$.

Par définition de la topologie sur $G_{\mathbb{A}_\mathrm{f}}$, que le produit $\prod P_v$ soit ouvert signifie que chacun des $P_v$ est ouvert et que de plus $P_v = G(\mathscr{O}_v)$ pour presque tous les $v$.

**Proposition 6.8.** *Soit $\mathscr{P} = (P_v)_{v \in V_\mathrm{f}}$ une collection cohérente de sous-groupes $P_v \subset G(k_v)$. Alors le groupe*

$$\Lambda_{\mathscr{P}} \quad := \quad G(k) \cap \prod_{v \in V_\mathrm{f}} P_v \tag{6.6}$$

*est un sous-groupe arithmétique de $G(k)$.*

Preuve. Notons $\Lambda := \Lambda_{\mathscr{P}}$ et $\Gamma := G(\mathscr{O}_k) \cap \Lambda$. De plus notons par $\Gamma_v$ le sous-groupe $G(\mathscr{O}_v) \cap P_v$ dans $G(k_v)$. Il s'agit d'un sous-groupe ouvert de $G(k_v)$. Comme $P_v$ est compact on a que l'indice $[P_v : \Gamma_v]$ est fini pour tous les $v \in V_\mathrm{f}$. De plus $P_v = \Gamma_v$ pour presque tous les $v$. Comme $\Lambda = G(k) \cap \prod_v P_v$ et $\Gamma = G(k) \cap \prod_v \Gamma_v$, l'indice $[\Lambda : \Gamma]$ est borné par $\prod_{v \in V_\mathrm{f}} [P_v : \Gamma_v]$ et est donc fini. De manière analogue on montre que $[G(\mathscr{O}_k) : \Gamma]$ est fini. Ainsi $G(\mathscr{O}_k)$ et $\Lambda_{\mathscr{P}}$ sont commensurables. □

**Proposition 6.9.** *Supposons que $G$ soit simplement connexe. Si $\mathscr{P}$ et $\mathscr{P}'$ sont deux collections cohérentes pour le groupe $G$ telles que $\Lambda_{\mathscr{P}} = \Lambda_{\mathscr{P}'}$, alors $\mathscr{P} = \mathscr{P}'$.*

Preuve. Soit $\mathscr{P} = (P_v)$ la collection cohérente qui détermine $\Lambda_{\mathscr{P}}$. Par le théorème d'approximation forte, $G(k)$ est dense dans $G_{\mathbb{A}_\mathrm{f}}$. En intersectant avec l'ouvert $\prod_v P_v$ on voit que $\Lambda_{\mathscr{P}}$ est dense dans $\prod_v P_v$, et en projetant sur chaque facteur : $\Lambda_{\mathscr{P}}$ est dense dans chaque $P_v$. Ainsi la collection $(P_v)$ se retrouve à partir de $\Lambda_{\mathscr{P}}$ en prenant son adhérence dans chaque $G(k_v)$. □

Pour un sous-groupe arithmétique donné par une collection cohérente, la question du calcul de son covolume peut s'envisager. Un début de solution est en effet donné par ce lemme :

**Lemme 6.10.** *Supposons que $G$ soit simplement connexe. Soit $\mathscr{P} = (P_v)_{v\in V_\mathrm{f}}$ une collection cohérente et soit $\Lambda_\mathscr{P} < G(k)$ le sous-groupe arithmétique associé. Pour une forme de Tamagawa $\omega$ sur $G$, on note par $\omega_\infty$ la mesure produit $\prod_{v|\infty}\omega_v$. On a alors :*

$$\omega_\infty(G_\infty/\Lambda_\mathscr{P}) \quad = \quad \mathscr{D}_k^{\dim G/2}\prod_{v\in V_\mathrm{f}}\omega_v(P_v)^{-1}.$$

Idée de la preuve. Comme $G$ est simplement connexe on peut utiliser l'approximation forte. Si l'on note $P := \prod_{v\in V_\mathrm{f}} P_v$, on peut donc montrer de manière analogue au cas $\mathbb{A}/k$ (voir preuve de la proposition 5.18) qu'on a un isomorphisme :

$$G_\mathbb{A}/G(k) \quad \cong \quad (G_\infty \times P)/\Lambda_\mathscr{P}.$$

La mesure induite par $\omega_\mathbb{A}$ de ce quotient donne $\mathscr{D}_k^{\dim G/2}$ selon le théorème 6.6. De l'autre côté on a :

$$\omega_\mathbb{A}\left((G_\infty \times P)/\Lambda_\mathscr{P}\right) \quad = \quad \omega_\infty(G_\infty/\Lambda_\mathscr{P})\cdot\prod_{v\in V_\mathrm{f}}\omega_v(P_v),$$

d'où le résultat. □

Nous mettons en garde le lecteur sur les limites de ce résultat à ce stade. Notre mise en garde porte sur trois niveaux :

- On sera intéressé à calculer le covolume d'un sous-groupe dans $G_\mathcal{S}$ et non pas dans $G_\infty$ (voir §3.4).
- La mesure $\omega_\infty$ n'est pas a priori (ni même a posteriori en fait) celle qui intéresse le géomètre. Contrairement à $\omega_\mathbb{A}$, la mesure $\omega_\infty$ dépend du choix de $\omega$.
- Cette formule donne un résultat concret à la condition que l'on puisse calculer les mesures $\omega_v(P_v)$ pour chaque $v \in V_\mathrm{f}$.

Ce dernier point amène à se poser la question de la description des sous-groupes ouverts et compacts de $G(k_v)$, ces derniers pouvant apparaître comme les membres $P_v$ de la collection cohérente $\mathscr{P}$. Une description explicite d'une classe importante de ces sous-groupes passera par la théorie présentée dans le chapitre 8. La compréhension de ce chapitre est elle-même conditionnée aux connaissances présentées dans le chapitre 7.

# Chapitre 7. Structure des groupes semi-simples

Ce chapitre expose les éléments importants de structure des groupes semi-simples. Cette structure se base sur l'étude de certains sous-groupes qu'on appelle *tores*. Dans ce chapitre la théorie absolue (structure des groupes sur un corps algébriquement clos) précédera la théorie relative (sur un corps quelconque). Nous ne donnerons presque aucune preuve : les résultats présentés font partie d'une riche théorie, qui se construit à l'aide de connaissances en géométrie algébrique bien plus larges que celles présentées en §2.2. Les références données au début du chapitre 2 restent valables ici. Le corps $k$ suivra les conventions données en §2.1.

## §7.1 Tores des groupes semi-simples

**Définition 7.1.** Un *tore (algébrique)* est un groupe algébrique isomorphe à un produit $(\mathbf{G}_{\mathrm{m}})^n$ pour un certain entier $n > 0$. Si $G$ est un groupe algébrique, alors un *tore de* $G$ sera un sous-groupe fermé de $G$ qui est un tore.

**Définition 7.2.** Un *caractère* d'un tore $T$ est un homomorphisme algébrique

$$\chi : T \to \mathbf{G}_{\mathrm{m}}.$$

Nous notons par $\mathbf{X}(T)$ le groupe abélien des caractères de $T$, et la loi de groupe de $\mathbf{X}(T)$ sera notée de façon additive. Ainsi $0 \in \mathbf{X}(T)$ correspond à l'homomorphisme $t \mapsto 1$ ($\forall\, t \in T$).

Nous travaillons dans ce paragraphe avec un groupe algébrique connexe semi-simple $G$ (défini sur un corps algébriquement clos). Fixons un tore $T$ dans $G$ (qui existe nécessairement) et considérons l'opération adjointe de $T$ sur $\mathfrak{g}$ (cf. (2.7)). Dans la suite nous utiliserons la notation simplifiée $\mathbf{X} := \mathbf{X}(T)$. Pour un caractère $\alpha \in \mathbf{X}$ on définit le sous-espace vectoriel de $\mathfrak{g}$ suivant :

$$\mathfrak{g}_\alpha \quad := \quad \{X \in \mathfrak{g} \mid \mathrm{Ad}(t)X = \alpha(t)X \;\forall\, t \in T\} \tag{7.1}$$

**Définition 7.3.** Un caractère $\alpha \in \mathbf{X}$ pour lequel $\mathfrak{g}_\alpha$ est non nul est appelé *poids* de $T$ dans $G$. Un poids non nul (on rappelle que $\mathbf{X}$ est noté additivement) est une *racine* de $T$ dans $G$. L'ensemble des racines de $T$ dans $G$ est désigné par $\Phi(G, T)$.

Comme $T$ est un groupe abélien on obtient :

**Proposition 7.4.** *L'espace* $\mathfrak{g}$ *possède la décomposition en somme directe :*

$$\mathfrak{g} \quad = \quad \mathfrak{g}_0 \oplus \bigoplus_\alpha \mathfrak{g}_\alpha,$$

*l'indice* $\alpha$ *parcourant les éléments de* $\Phi(G, T)$

Notons par $N_G(T)$ et $Z_G(T)$ le normalisateur et le centralisateur de $T$ dans $G$. Ce sont des sous-groupes fermés. On a le théorème suivant [Hum75, 16.3 et 22.3] :

**Théorème 7.5.** *Soit $T$ un tore du groupe semi-simple connexe $G$. On a que $N_G(T)^\circ = Z_G(T)$.*

Ce théorème permet de constater que le groupe

$$W(G,T) \quad := \quad N_G(T)/Z_G(T) \tag{7.2}$$

est fini (cf. proposition 2.38).

Chaque tore de $G$ est inclus dans un *tore maximal*, i.e. un tore qui n'est pas strictement inclus dans un autre tore de $G$. La propriété fondamentale des tores maximaux de $G$ est la suivante :

**Théorème 7.6.** *Tous les tores maximaux de $G$ sont conjugués dans $G$.*

Ce théorème montre que la dimension des tores maximaux de $G$ est invariante. De plus le groupe $W(G,T)$ est à isomorphisme près indépendant du choix d'un tore maximal $T$.

**Définition 7.7.** On définit le *rang (absolu)* de $G$ comme la dimension des tores maximaux de $G$. Pour un tore maximal $T \subset G$, le groupe fini $W := W(G,T)$ défini par (7.2) est appelé *groupe de Weyl (absolu)* de $G$.

**Remarque 7.8.** On peut en fait montrer qu'un tore maximal dans un groupe connexe est égal à son propre centralisateur. Ceci donne en particulier la formule simplifiée pour le groupe de Weyl absolu de $G$ :

$$W(G,T) = N_G(T)/T.$$

## §7.2 Système de racines des groupes semi-simples

Tout comme pour les groupes de Lie semi-simples, la structure des groupes algébriques semi-simples s'étudie grâce à la notion suivante :

**Définition 7.9.** Soit E un espace vectoriel réel de dimension finie. Un *système de racines* de E est un sous-ensemble $\Phi \subset$ E satisfaisant :

(R1) $\Phi$ est fini, engendre l'espace E sur $\mathbb{R}$ et ne contient pas 0.

(R2) Si $\alpha \in \Phi$, il existe une application linéaire (en fait unique) $\tau_\alpha$ telle que :
- $\tau_\alpha(\alpha) = -\alpha$
- $\tau_\alpha$ fixe un sous-espace de E de codimension 1.
- $\tau_\alpha(\Phi) = \Phi$.

(R3) Pour $\alpha, \beta \in \Phi$, le vecteur $\tau_\alpha(\beta) - \beta$ est un multiple entier de $\alpha$.

Avant de voir comment les systèmes de racines interviennent dans la théorie des groupes algébriques, nous passons en revue les concepts associés à la notion de système de racines.

**7.10 Rang.** La dimension de E est le *rang* de $\Phi$.

**7.11 Nombres de Cartan.** Il existe un produit scalaire $(\cdot,\cdot)$ sur E pour lequel les $\tau_\alpha$ sont des transformations orthogonales de E. On note :

$$<\alpha,\beta> \quad := \quad 2\frac{(\alpha,\beta)}{(\beta,\beta)},$$

et ces nombres (entiers) sont appelé *nombres de Cartan*. On montre que les seules valeurs possibles pour ces nombres sont $0, \pm 1, \pm 2$ et $\pm 3$.

**7.12 Base.** Une *base* de $\Phi$ est un sous-ensemble $\Delta \subset \Phi$ pour lequel chaque $\alpha \in \Phi$ possède une unique expression

$$\alpha \quad = \quad \sum_{\alpha_i \in \Delta} c_i \alpha_i,$$

avec des coefficients entiers $c_i$ de même signe. On peut montrer que tout système de racines possède une base. Il est clair que la cardinalité d'une base de $\Phi$ est égale au rang de $\Phi$.

**7.13 Groupe de Weyl.** Le sous-groupe fini de GL(E) engendré par les applications $\tau_\alpha$ ($\alpha \in \Phi$) est appelé *groupe de Weyl* de $\Phi$. De façon équivalente on peut définir ce groupe comme le groupe des isométries (par rapport au produit scalaire $(\cdot,\cdot)$) qui stabilisent $\Phi$. Il s'agit d'un *groupe de Coxeter* fini, dont un système de générateurs est donné par l'ensemble

$$S \quad = \quad \{\tau_\alpha \mid \alpha \in \Delta\}, \tag{7.3}$$

où $\Delta$ désigne une base de $\Phi$. On va supposer dans cette thèse que le lecteur possède une certaine familiarité avec les groupes de Coxeter. Au besoin il peut consulter [Hum90].

**7.14 Type.** Soit E′ un second espace vectoriel et $\Phi'$ un système de racines de E′. Alors $\Phi$ et $\Phi'$ sont dits *isomorphes* s'il existe un isomorphisme $\theta : \mathrm{E} \to \mathrm{E}'$ qui envoie $\Phi$ sur $\Phi'$ et tel que $<\theta(\alpha),\theta(\beta)>=<\alpha,\beta>$ pour tout $\alpha,\beta \in \Phi$. Un *type* sera une classe d'isomorphisme de système de racines.

**7.15 Système réduit.** Le système $\Phi$ est dit *réduit* lorsque la propriété suivante est respectée : $\forall\ \alpha,\beta \in \Phi$, on a :

$$\alpha = c\beta \quad \Longrightarrow \quad c = \pm 1.$$

**7.16 Système irréductible.** $\Phi$ est appelé *irréductible* s'il ne peut se partitionner en deux sous-ensembles orthogonaux entre eux.

**7.17 Diagramme de Dynkin.** On associe à un système de racines réduit $\Phi$ son *diagramme de Dynkin* comme suit : étant fixé une base $\Delta \subset \Phi$, on fait correspondre à chaque élément de $\Delta$ un noeud (sommet d'un graphe). Les deux

noeuds correspondant à $\alpha, \beta \in \Delta$ sont joints par une arête simple, double ou triple en fonction de l'égalité $<\alpha, \beta><\beta, \alpha> = 1, 2$ ou 3. Quand ce nombre vaut 0 les noeuds sont laissés disjoints (c'est la situation où $\alpha$ et $\beta$ sont orthogonaux). Cela couvre toutes les situations. De plus si $\alpha$ et $\beta$ sont joints mais n'ont pas la même longueur (par rapport au produit scalaire $(\cdot, \cdot)$ sur E), on fait pointer une flèche vers le noeud correspondant au vecteur le plus court. Ce diagramme ne dépend pas de la base choisie. $\Phi$ est irréductible si et seulement si son diagramme de Dynkin est connexe.

**7.18 Graphe de Coxeter.** Au diagramme de Dynkin de $\Phi$ est associé un graphe de Coxeter [Hum90] qu'on dira *sous-jacent*. Celui-ci est déterminé comme suit. On garde les mêmes noeuds et on oublie l'orientation des arêtes. A une arête simple on associe l'arête de poids 3 (poids généralement omis), à une arête double l'arête de poids 4, et à une arête triple on associe une arête de poids 6. Contrairement à certains usages dans la littérature, nous noterons toujours les graphes de Coxeter à l'aide de poids et non de traits doublés ou triplés. On évite ainsi la confusion avec les diagrammes de Dynkin (un trait triple pour un graphe de Coxeter fait souvent référence à une arête de poids 5 et non 6). Le graphe de Coxeter sous-jacent au diagramme de Dynkin du système $\Phi$ correspond en fait au graphe du groupe de Weyl de $\Phi$.

**7.19 Classification.** Les différents types de système de racines réduits et irréductibles sont classifiés par leurs diagrammes de Dynkin. On dénote ces types par une lettre majuscule indicée par un nombre qui correspond au rang. Nous listons dans la figure 7.1 les types correspondants aux symboles $\mathrm{A} - \mathrm{D}$, et qu'on appelle *types classiques*. Outre ceux-ci, il existe exactement cinq autres types irréductibles réduits, qu'on appelle *types exceptionnels*. Ils sont désignés par les symboles $\mathrm{E}_6, \mathrm{E}_7, \mathrm{E}_8, \mathrm{F}_4$ et $\mathrm{G}_2$. Les types réduits non irréductibles s'obtiennent comme produit des types irréductibles, et on les notera grâce au symbole du produit cartésien (e.g. $\mathrm{A}_4 \times \mathrm{G}_2$).

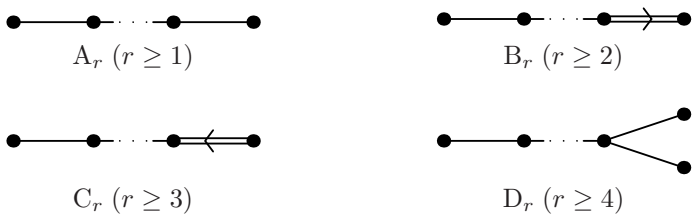



FIG. 7.1 – Types classiques

Le lien entre systèmes de racines et groupes algébriques est contenu dans le résultat suivant :

**Théorème 7.20.** *Soit $G$ un groupe semi-simple connexe et $T$ un tore maximal dans $G$. L'ensemble $\Phi(G,T)$ est un système réduit de racines dans $\mathrm{E} := \mathbf{X}(T)\otimes_{\mathbb{Z}} \mathbb{R}$, dont le groupe de Weyl coïncide avec $W(G,T)$ (le groupe de Weyl de $G$ tel que défini en 7.7). De plus $G$ est absolument simple si et seulement si $\Phi(G,T)$ est irréductible.*

On fait remarquer ici que $\mathbf{X}(T)$ est un groupe abélien libre d'un rang égal à la dimension de $T$. Cette dimension vaut donc la dimension de l'espace E et les deux notions de rang pour $G$ et pour $\Phi(G,T)$ coïncident. Par conjugaison des tores maximaux, le système de racines $\Phi(G,T)$ ne dépend (à isomorphisme près) pas du choix particulier de $T$. Il n'y a donc aucune ambiguïté à définir le *type (absolu)* du groupe semi-simple $G$ comme le type de $\Phi(G,T)$. Il s'agit ainsi d'un invariant des groupes algébriques semi-simples. La plupart du temps un tore maximal $T$ sera fixé une fois pour toute dans $G$, et dans ce cas nous utiliserons les notations simplifiées :

$$\Phi := \Phi(G,T) \tag{7.4}$$
$$W := W(G,T) \tag{7.5}$$

L'identification de $W$ avec le groupe de Weyl de $\Phi$ mentionnée dans le théorème 7.20 est bien canonique : un élément $w \in W$ représenté par $n \in N_G(T)$ transforme $\mathbf{X}(T)$, et par extension l'espace E, en envoyant $\alpha \in \mathbf{X}(T)$ sur le caractère :

$$w(\alpha) \quad : \quad t \in T \mapsto \alpha(ntn^{-1}). \tag{7.6}$$

L'opération de $W$ sur E ainsi définie correspond alors à celle du groupe de Weyl de $\Phi(G,T)$. On peut vérifier que $W$ stabilise $\Phi(G,T)$.

**Remarque 7.21.** Dans le cas absolu le type constitue un invariant très fort : à quelques exceptions près qui n'apparaissent qu'en caractéristique positive, le type caractérise complètement les classes d'isogénie des groupes algébriques semi-simples (sur un corps algébriquement clos). De plus si l'on ajoute au type un second invariant, appelé le *groupe fondamental*, on obtient une classification complète des groupes algébriques semi-simples défini sur un corps algébriquement clos. On peut aussi affirmer que le type classifie à isomorphisme près les groupes algébriques semi-simples simplement connexe (sur un corps algébriquement clos).

**Exemple 7.22.** Le groupe $\mathrm{SL}_2$ est de type $\mathrm{A}_1$.

**Exemple 7.23.** Le type du groupe $\mathrm{Spin}_f$ (resp. $\mathrm{SO}_f$) varie en fonction de la dimension $n$ de la forme quadratique $f$. Pour $n \geq 5$ la parité de la dimension est déterminante : si $n = 2r+1 \geq 5$ alors $\mathrm{Spin}_f$ (resp. $\mathrm{SO}_f$) est de type $\mathrm{B}_r$, et pour $n = 2r \geq 8$ il est de type $\mathrm{D}_r$. En basses dimensions on a la description suivante. Pour $n = 3$ le type de $\mathrm{Spin}_f$ (resp. $\mathrm{SO}_f$) est $\mathrm{A}_1$, ce qui implique que $\mathrm{Spin}_f \cong \mathrm{SL}_2$. Pour $n = 4$ le type de $\mathrm{Spin}_f$ (resp. $\mathrm{SO}_f$) est réductible et vaut $\mathrm{A}_1 \times \mathrm{A}_1$ (cf. exemple 2.37). Pour cette raison on définit souvent le type $\mathrm{D}_2$ par $\mathrm{D}_2 := \mathrm{A}_1 \times \mathrm{A}_1$. De façon similaire on peut définir $\mathrm{D}_3 := \mathrm{A}_3$, ce type étant celui de $\mathrm{Spin}_f$ (resp. $\mathrm{SO}_f$) pour $f$ de dimension $n = 6$.

## §7.3 Système de Tits

Un concept important lié à la théorie des groupes algébriques semi-simples est celui de « système de Tits » [Hum75, §29]. Un premier type de système de Tits sera associé à n'importe quel groupe semi-simple, dans la seconde moitié du présent paragraphe. Au chapitre suivant, un second type de système de Tits apparaîtra lorsque nous traiterons des groupes définis sur un corps $\mathfrak{p}$-adique. C'est ce second aspect qui motive notre besoin d'exposer les systèmes de Tits, les idées qui concluent ce paragraphe jouant un rôle moins fondamental pour la suite de notre exposé. Elles ont toutefois le mérite de préparer le lecteur au chapitre suivant. Cette dichotomie entre le cas général (on parlera de *théorie classique*) et le cas $\mathfrak{p}$-adique (*théorie locale*) nous pousse à travailler avec une définition abstraite. C'est pourquoi nous insistons sur le fait que dans ce qui suit, le terme « groupe » désigne un groupe abstrait.

**Définition 7.24.** Soit $B$ et $N$ deux sous-groupes du groupe $G$ qui engendrent celui-ci et tels que $T := B \cap N$ est normal dans $N$. Soit encore $S$ un ensemble de générateurs du groupe $W := N/T$. Le quadruplet $(G, B, N, S)$ est appelé *système de Tits* s'il respecte les axiomes suivants :

(T1) $BsBwB \subset BwB \cup BswB$, pour chaque $s \in S$ et $w \in W$.

(T2) Pour $s \in S$, on a : $sBs^{-1} \not\subset B$.

On dit également dans ce cas que $(B, N)$ est une BN-*pair* de $G$.

Dans ce cadre axiomatique on peut montrer que $(W, S)$ doit être un système de Coxeter. D'autre part, la seule considération de la propriété (T1) montre que pour chaque sous-ensemble $I \subset S$, si $W_I$ désigne le sous-groupe de $W$ engendré par $I$, alors

$$P_I \quad := \quad BW_IB \tag{7.7}$$

est un sous-groupe de $G$. C'est essentiellement l'étude des sous-groupes de la forme $P_I$ (et de leurs conjugués) qui retiendra notre attention par la suite. Leur rôle prépondérant sera expliqué par les propriétés suivantes :

**Théorème 7.25.** *Soit $(G, B, N, S)$ un système de Tits.*

1. *Chaque sous-groupe de $G$ contenant $B$ est de la forme $P_I$ pour un $I \subset S$.*
2. *Soient $I, J \subset S$. Alors $P_I$ est conjugué à $P_J$ si et seulement si $I = J$ (et dans ce cas on a donc même $P_I = P_J$). De plus $P_I \subset P_J$ implique $I \subset J$.*

Considérons un sous-groupe $P < G$ qui contient un conjugué de $B$, i.e.

$$\exists\, g \in G \ \text{ tel que } \ g^{-1}Bg \subset P.$$

La première assertion du théorème montre que $P$ est conjugué à un sous-groupe $P_I$ (pour un certain $I \subset S$), et par la deuxième partie du théorème le sous-ensemble $I$ est uniquement déterminé par $P$ (c'est-à-dire indépendant l'élément $g$).

**Définition 7.26.** Soit $(G, B, N, S)$ un système de Tits, et soit $P < G$ un sous-groupe contenant un conjugué de $B$. Le sous-ensemble $I \subset S$ attribué à $P$ comme ci-dessus est appelé le *type* de $P$. Il existe donc $2^{\#S}$ types distincts pour le système $(G, B, N, S)$.

**Remarque 7.27.** Les sous-groupes contenant un conjugué de $B$ sont connus dans ce cadre axiomatique sous le nom de « sous-groupes paraboliques » de $G$. Cette désignation dépend bien entendu du système de Tits que l'on construit dans $G$. Nous réserverons (dans la définition 7.30) le terme *parabolique* à la première variante de système de Tits que nous verrons. Dans le cas $\mathfrak{p}$-adique, ces sous-groupes « paraboliques » possèdent une appellation propre que le lecteur reconnaîtra toutefois inspirée de l'appellation classique (cf. définition 8.1).

Nous revenons à présent à la situation des groupes algébriques. Les groupes semi-simples contiennent en plus des tores, un autre type de sous-groupes d'importance fondamentale, que nous définissons ici.

**Définition 7.28.** Un *sous-groupe de Borel* d'un groupe algébrique $G$ est un sous-groupe fermé, connexe et résoluble, maximal dans $G$ pour ces propriétés.

Tout comme les tores maximaux, on peut montrer que les sous-groupes de Borel d'un groupe algébrique sont tous conjugués entre eux. Si $T$ est un tore maximal de $G$, celui-ci étant par définition connexe, fermé et résoluble, il doit exister un sous-groupe de Borel $B$ contenant $T$. Voici alors le système de Tits classique dans un groupe algébrique semi-simple [Hum75, 29.1] :

**Théorème 7.29.** *Soit $G$ un groupe algébrique semi-simple, $T$ un tore maximal de $G$ contenu dans le sous-groupe de Borel $B$. Posons $N := N_G(T)$ et (en adéquation avec l'usage jusqu'ici : cf. remarque 7.8) notons $W := N/T$. Soit $(W, S)$ un système de Coxeter pour $W$ (dont l'existence découle du théorème 7.20). Alors $(G, B, N, S)$ est un système de Tits.*

**Définition 7.30.** Un sous-groupe d'un groupe algébrique semi-simple est dit *parabolique* s'il contient un sous-groupe de Borel.

Le théorème 7.29 permet d'appliquer nos connaissances sur les systèmes de Tits, et de décrire les sous-groupes paraboliques de $G$ à l'aide du type. On peut en déduire par exemple que les sous-groupes paraboliques sont des sous-groupes fermés. Fixons une base $\Delta$ de $\Phi(G, T)$. Ce choix d'une base détermine (cf. 7.13) un système de Coxeter $(W, S)$ avec :

$$S \quad := \quad \{\tau_\alpha \mid \alpha \in \Delta\}\,.$$

Plutôt que de décrire les sous-groupes paraboliques à l'aide de $S$, nous utilisons la bijection canonique $\alpha \mapsto \tau_\alpha$ entre $\Delta$ et $S$. Par *type* d'un sous-groupe parabolique $P \subset G$ nous entendrons donc le sous-ensemble de $\Delta$ en bijection canonique avec le type de $P$ au sens de la définition 7.26 (qui est un sous-ensemble de $S$).

## §7.4 Groupes semi-simples réels

Soit $\mathscr{G}$ un groupe de Lie réel et $\mathfrak{g}$ son algèbre de Lie. La théorie des groupes de Lie semi-simples associe à l'algèbre complexifiée $\mathfrak{g}_\mathbb{C} := \mathfrak{g} \otimes \mathbb{C}$ un système de racines [OV94, Ch. 3 : 1.3]. Cela définit le *type* du groupe de Lie $\mathscr{G}$. Le type des groupes algébriques est en fait une généralisation du type des groupes de Lie :

**Proposition 7.31.** *Soit $G$ un $\mathbb{R}$-groupe semi-simple. Le type absolu de $G$ (comme groupe algébrique sur $\mathbb{C}$) et le type de $G(\mathbb{R})$ (comme groupe de Lie) coïncident.*

Même en se restreignant aux cas des groupes de Lie de la forme $G(\mathbb{R})$ pour un $\mathbb{R}$-groupe $G$ simplement connexe, le type n'est pas suffisant pour la classification des groupes semi-simples. Ce n'est en effet pas le même cas de figure que celui de remarque 7.21 : $\mathbb{R}$ n'est pas algébriquement clos. La structure réel de l'algèbre complexifiée contient elle suffisamment d'information :

**Proposition 7.32.** *Soient $G$ et $H$ deux $\mathbb{R}$-groupes semi-simples simplement connexes. Si les algèbres de Lie $\mathfrak{g}_{\mathbb{R}}$ et $\mathfrak{h}_{\mathbb{R}}$ sont isomorphes, alors $G$ et $H$ sont $\mathbb{R}$-isomorphes.*

Le type permet (comme le suggère la remarque 7.21) une classification des groupes de Lie complexes simplement connexes. On sera pour notre part surtout intéressé au résultat similaire pour les groupes compacts, qu'on formule comme suit [OV94, Ch. 4 §1-2] :

**Théorème 7.33.** *Soit $G$ un $\mathbb{R}$-groupe semi-simple simplement connexe. Alors il existe une unique (à $\mathbb{R}$-isomorphisme près) $\mathbb{R}$-forme $G_{\mathrm{u}}$ de $G$ telle que $G_{\mathrm{u}}(\mathbb{R})$ est compact.*

Le $\mathbb{R}$-groupe $G_{\mathrm{u}}$ est appelée *forme compacte réelle* de $G$. Comme $\mathbb{R}$-forme de $G$, le groupe $G_{\mathrm{u}}$ doit être de même type absolu et être simplement connexe. En fixant un isomorphisme (sur $\mathbb{C}$) entre $G$ et $G_{\mathrm{u}}$, on peut voir $G_{\mathrm{u}}(\mathbb{R})$ comme un sous-groupe compact maximal de $G(\mathbb{C})$.

**Exemple 7.34.** La forme compacte réelle du groupe $\mathrm{Spin}_{(n,1)}$ est le $\mathbb{R}$-groupe $\mathrm{Spin}_{n+1}$, dont les points réels $\mathrm{Spin}(n+1) := \mathrm{Spin}_{n+1}(\mathbb{R})$ forment un revêtement double (et bien surjectif) du groupe orthogonal $\mathrm{SO}(n+1)$.

## §7.5 Tores rationnels des groupes semi-simples

Tout comme pour la structure absolue, la structure relative des groupes semi-simples s'étudie grâce à la notion de tore. C'est pourquoi nous commençons par quelques définitions concernant les tores dans le cas relatif.

**Définition 7.35.** Un $k$-tore de dimension $n$ est dit *déployé* (sur $k$) s'il est $k$-isomorphe à $(\mathbf{G}_{\mathrm{m}})^n$. On parlera aussi de tore $k$-déployé. A l'opposé, un $k$-tore qui ne possède aucun sous-tore $k$-déployé est dit *$k$-anisotrope*.

**Exemple 7.36.** Soit $\ell|k$ une extension de corps. On considère le $k$-homomorphisme

$$N_{\ell|k} \quad : \quad \mathbf{R}_{\ell|k}(\mathbf{G}_{\mathrm{m}}) \to \mathbf{G}_{\mathrm{m}} \tag{7.8}$$

qui associe à un élément de $\mathbf{R}_{\ell|k}(\mathbf{G}_{\mathrm{m}})$ son déterminant ($\mathbf{R}_{\ell|k}(\mathbf{G}_{\mathrm{m}})$ étant écrit comme un groupe de matrices de taille $[\ell : k] \times [\ell : k]$). Si l'on restreint cette application à $\ell^\times \cong \mathbf{R}_{\ell|k}(\mathbf{G}_{\mathrm{m}})(k)$ on obtient la norme $N_{\ell|k}$ telle que donnée

dans la définition 4.7. Cette application étendue à $\mathbf{R}_{\ell|k}(\mathbf{G}_{\mathrm{m}})$ sera également appelée *norme*. On définit alors le $k$-sous-groupe

$$\mathbf{R}^{(\mathbf{1})}_{\ell|k}(\mathbf{G}_{\mathrm{m}}) \quad < \quad \mathbf{R}_{\ell|k}(\mathbf{G}_{\mathrm{m}}) \tag{7.9}$$

comme le noyau de $N_{\ell|k}$. Tous les tores $k$-anisotropes de dimension 1 sont alors de la forme $\mathbf{R}^{(\mathbf{1})}_{\ell|k}(\mathbf{G}_{\mathrm{m}})$ pour une extension quadratique $\ell|k$ [Vos98, 4.9].

On va considérer dès maintenant un $k$-groupe semi-simple connexe $G$. Le groupe $G$ est dit *anisotrope* s'il ne possède aucun tore $k$-déployé. Si $G$ n'est pas anisotrope il existe dans $G$ des $k$-tores déployés qui sont maximaux pour cette propriété. On les appellera brièvement *$k$-tores déployés maximaux*. On prendra garde à ne pas confondre « tore déployé maximal » et « tore maximal déployé ». On dispose de la généralisation suivante du théorème 7.6 [Bor91, 20.9] :

**Théorème 7.37.** *Tous les $k$-tores déployés maximaux sont conjugués entre eux par un élément de $G(k)$. De plus chaque tore déployé maximal est inclus dans un tore maximal défini sur $k$ (pas forcément déployé).*

Ce théorème permet d'envisager des résultats de structure similaires au cas absolu en considérant les tores déployés de $G$. On a en effet [Bor91, §21] :

**Théorème 7.38.** *Supposons que $G$ n'est pas anisotrope, et soit ${}_kT$ un $k$-tore déployé maximal de $G$. L'ensemble $\Phi(G, {}_kT)$ est un système de racines (pas nécessairement réduit), indépendant (à isomorphisme près) du choix de ${}_kT$.*

**Définition 7.39.** Nous notons par ${}_k\Phi := \Phi(G, {}_kT)$ le système de racines associé à un $k$-tore déployé maximal de $G$. Son type est appelé *type de $G$ relatif à $k$*. Le *rang relatif* de $G$ est défini comme le rang de ${}_k\Phi$, ou de manière équivalente comme la dimension de ${}_kT$. Le groupe de Weyl de ${}_k\Phi$ correspond au groupe fini

$${}_kW := N_G({}_kT)/Z_G({}_kT),$$

appelé *groupe de Weyl de $G$ relatif à $k$*.

## §7.6 Indice de Tits

On va supposer (ce n'est pas une restriction majeure) que le $k$-groupe $G$ est absolument simple. Le théorème 7.37 nous permet de choisir un $k$-tore maximal $T$ de $G$ qui contient ${}_kT$. L'inclusion ${}_kT \subset T$ induit alors une application

$$j \quad : \quad \Phi \to {}_k\Phi \cup \{0\}\,. \tag{7.10}$$

Etant donnée une base ${}_k\Delta$ de ${}_k\Phi$, il est alors possible (cf. [Bor91, 21.8]) de choisir une base $\Delta$ de $\Phi$ pour laquelle

$$j(\Delta \smallsetminus \Delta^0) \quad = \quad {}_k\Delta,$$

où $\Delta^0$ désigne le sous-ensemble (éventuellement vide) de $\Delta$ constitué des éléments dont l'image par $j$ est nulle.

Les fibres de l'application $j$ au-dessus de ${}_k\Delta$ se décrivent alors comme orbites d'une certaine opération de $\mathrm{Gal}(\overline{k}|k)$ sur $\Delta$. Nous décrivons ici cette opération. Dans ce qui suit par « sous-groupe parabolique maximal » on entend un sous-groupe parabolique maximal différent de $G$. Un tel sous-groupe parabolique $P \subset G$ est nécessairement de type $\Delta \smallsetminus \{\alpha\}$, pour un $\alpha \in \Delta$. Supposons que $P$ contienne le sous-groupe de Borel $B$, et soit $\sigma \in \mathrm{Gal}(\overline{k}|k)$. Le sous-groupe conjugué ${}^\sigma B$ est également un sous-groupe de Borel, et le sous-groupe ${}^\sigma P$ est alors lui-même parabolique maximal. Nous notons par $\Delta \smallsetminus \{\sigma(\alpha)\}$ son type. Cette attribution

$$\sigma \quad : \quad \alpha \mapsto \sigma(\alpha) \tag{7.11}$$

donne l'opération de $\mathrm{Gal}(\overline{k}|k)$ sur $\Delta$ annoncée : deux éléments de $\Delta \smallsetminus \Delta^0$ ont même image par $j$ si et seulement s'ils sont conjugués par cette opération.

L'opération de $\mathrm{Gal}(\overline{k}|k)$ sur $\Delta$ est en fait assez rigide : $\sigma \in \mathrm{Gal}(\overline{k}|k)$ doit opérer sur $\Delta$ comme une symétrie du diagramme de Dynkin qui représente $\Delta$. On note par $\mathrm{Aut}(\Delta)$ ce groupe des symétries du diagramme de Dynkin. En particulier pour les types $\mathrm{B}_r$ et $\mathrm{C}_r$ on a $\mathrm{Aut}(\Delta) = \{1\}$, et donc $\mathrm{Gal}(\overline{k}|k)$ opère trivialement sur $\Delta$.

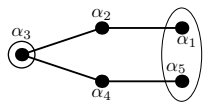
La structure du $k$-groupe $G$ est alors partiellement captée par une représentation graphique qui décrit le sous-ensemble $\Delta^0$ et l'opération $\mathrm{Gal}(\overline{k}|k) \to \mathrm{Aut}(\Delta)$ sur le diagramme de Dynkin de $\Delta$. On appelle ainsi *indice (de Tits)* de $G$ par rapport à $k$ le diagramme de Dynkin de $\Delta$ qu'on dessine avec les adaptation suivantes :

- les noeuds qui sont conjugué par $\mathrm{Gal}(\overline{k}|k)$ sont placés proches les uns des autres ;
- les orbites de l'opération de $\mathrm{Gal}(\overline{k}|k)$ sur $\Delta \smallsetminus \Delta^0$ sont entourées.

Les entourages de l'indice correspondent par l'application $j$ donc aux éléments de ${}_k\Delta$. Les noeuds qui ne sont pas entourés correspondent eux aux éléments de $\Delta^0$.

**Remarque 7.40.** Notre définition de l'indice contient moins d'information que la définition usuelle [Tit66, 2.3], qui donne toute l'opération de $\mathrm{Gal}(\overline{k}|k)$ sur $\Delta$. Il est cependant assez fréquent de confondre cette version plus forte de l'indice avec sa représentation graphique.

**Exemple 7.41.** L'indice donné par




correspond à un groupe de type absolu $\mathrm{A}_5$, pour lequel $\Delta^0 = \{\alpha_2, \alpha_4\}$ et sur lequel $\mathrm{Gal}(\overline{k}|k)$ induit une opération non triviale sur $\Delta$.

Dans l'article [Tit66] Tits utilise la notion d'indice pour donner une classification des groupes semi-simples dans le cas relatif. Contrairement au cas absolu, le corps $k$ joue un rôle important dans cette classification : certains indices qui apparaissent avec certains corps peuvent être absent avec d'autres corps. Dans ce même article [Tit66] la notation ${}^a\mathrm{X}_{r,l}^{(d)}$ est proposée pour faire référence aux différents indices des groupes absolument simples. Ici X doit être remplacé par

le type absolu (A − G) du groupe $G$, $r$ désigne le rang de $G$, $l$ le rang $k$-relatif et $a$ est l'ordre de l'image de $\mathrm{Gal}(\overline{k}|k)$ dans $\mathrm{Aut}(\Delta)$. Enfin le $d$ correspond à un certain invariant définit au cas par cas pour chaque type. On peut se contenter de le voir comme un nombre qui permet de lever les éventuelles ambiguïtés. On peut très bien utiliser la notation de façon partielle pour décrire non pas un seul indice, mais une famille d'indices d'invariants donnés ; par exemple nous n'utiliserons pas l'invariant $d$, qu'on laissera donc tomber dans la notation des indices. De même on notera ${}^a\mathrm{X}_r$ pour décrire tous les indices avec X, $a$ et $r$ fixés, et $l$ quelconque. On dira que $G$ est de *type* ${}^a\mathrm{X}_{r,l}$ (resp. ${}^a\mathrm{X}_r$) si son indice appartient à cette famille. Un groupe $G$ qui possède l'indice de l'exemple 7.41 est ainsi de type ${}^2\mathrm{A}_{5,2}$ (et donc plus généralement de type ${}^2\mathrm{A}_5$).

**Définition 7.42.** Soit $G$ de type ${}^a\mathrm{X}_r$. On dit que $G$ est une *forme interne* ou *est de type interne* si $a = 1$. Dans le cas contraire on dit que $G$ est une *forme externe* ou *est de type externe*.

Nous verrons au paragraphe §7.8 une explication plus détaillée de la signification pour $G$ d'être une formes interne (ou externe). Si $\mathrm{Aut}(\Delta)$ est trivial alors $G$ est nécessairement une forme interne.

**Remarque 7.43.** Pour $G$ absolument simple (i.e. de type absolu irréductible) on a, à la seule exception du type $\mathrm{D}_4$, que $\mathrm{Aut}(\Delta)$ possède un ordre d'au plus 2 et que dans ces cas les formes externes correspondent au type ${}^2\mathrm{X}_r$. Par contre pour le type $\mathrm{D}_4$ le groupe $\mathrm{Aut}(\Delta)$ est isomorphe au groupe symétrique d'ordre 6, et à côté des types ${}^1\mathrm{D}_4$ et ${}^2\mathrm{D}_4$ apparaissent les types ${}^3\mathrm{D}_4$ et ${}^6\mathrm{D}_4$. $G$ est appelé *forme trialitaire* s'il est d'un de ces deux derniers types. On utilisera souvent la notation ${}^{3,6}\mathrm{D}_4$ pour regrouper les deux types trialitaires.

## §7.7 Groupes déployés et quasi-déployés

On continue à désigner par $G$ un $k$-groupe semi-simple. Les notations des deux paragraphes précédents seront utilisées sans autre précision.

**Définition 7.44.** $G$ est dit *$k$-déployé* (ou *déployé sur $k$*) s'il possède un tore maximal qui est défini sur $k$ et déployé (i.e $\exists\ {}_kT = T$). Lorsque le corps de définition $k$ est clairement établi par le contexte, on parlera simplement d'un groupe déployé.

S'il est déployé, $G$ est nécessairement une forme interne et son indice s'obtient de façon triviale à partir du diagramme de Dynkin de $\Phi(G,T)$ : chaque noeud est entouré (comme $\Delta^0 = \emptyset$), seul dans son orbite. Si $G$ est absolument simple, il est déployé exactement lorsque qu'il est de type ${}^1\mathrm{X}_{r,r}$. En se restreignant aux groupes déployés, le type retrouve autant d'importance que dans le cas absolu :

**Théorème 7.45.** *Il existe une $k$-forme $G^{\mathrm{s}}$ du groupe $G$ qui est déployée, et celle-ci est unique à $k$-isomorphisme près.*

On peut affaiblir quelque peu la condition de la définition 7.44 :

**Définition 7.46.** Le groupe $G$ est dit *quasi-déployé* (sur $k$) si $\Delta^0 = \emptyset$.

On passe du cas quasi-déployé au cas déployé en observant l'opération

$$\mathrm{Gal}(\overline{k}|k) \quad \to \quad \mathrm{Aut}(\Delta)$$

discutée en §7.6. Le noyau de cette opération est un sous-groupe de $\mathrm{Gal}(\overline{k}|k)$ d'indice $a$, où $G$ quasi-déployé est ici supposé être de type ${}^a\mathrm{X}_r$. A ce sous-groupe correspond donc une extension galoisienne $L|k$ de degré $a$ pour laquelle $G|L$ est déployé. Si $G$ quasi-déployé est une forme interne, alors $G$ est déjà déployé sur $k$. Le corps $L$ sera appelé *corps de déploiement* de $G$.

**Remarque 7.47.** Le corps de déploiement $L$ du groupe quasi-déployé $G$ est minimal, dans la sens suivant : si $K|k$ est une extension de corps pour laquelle $G|K$ est déployé, alors il doit exister une inclusion $L \hookrightarrow K$.

## §7.8 Automorphismes et formes internes

Par *automorphisme* du groupe algébrique $G$, on entend ici un isomorphisme algébrique de $G$ vers $G$. On notera par $\mathrm{Aut}(G)$ le groupe des automorphismes de $G$. Si $G$ est défini sur $k$, on peut se restreindre au sous-groupe $\mathrm{Aut}_k(G)$ des $k$-automorphismes. Nous avons déjà rencontré en §2.9 un sous-groupe de $\mathrm{Aut}(G)$ : le groupe adjoint $\overline{G}$, décrivant les automorphismes internes de $G$. On rappelle (cf. proposition 2.39) que lorsque $G$ est défini sur $k$, on a $\mathrm{Aut}_k(G) \cap \overline{G} = \overline{G}(k)$. Le groupe $\mathrm{Aut}(G)$ possède la description suivante [Hum75, 27.4] :

**Théorème 7.48.** *Soit $G$ semi-simple et soit $\Delta$ une base du système de racines (absolu) de $G$. Alors* $\mathrm{Aut}(G) \cong \mathrm{Aut}(\Delta) \ltimes \overline{G}$.

**Définition 7.49.** Soit $G$ un $k$-groupe semi-simple et $H$ une $k$-forme de $G$. On dit que $H$ est une $k$-forme *interne* de $G$ s'il existe un isomorphisme $\phi : G \to H$ tel que pour chaque $\sigma \in \mathrm{Gal}(\overline{k}|k)$ l'isomorphisme $\phi^{-1} \circ {}^\sigma\phi$ est interne, i.e. $\phi^{-1} \circ {}^\sigma\phi \in \overline{G}$ .

Si le contexte ne permet aucune ambiguïté pour le corps $k$ dont il est question, on parlera brièvement de *forme interne* d'un groupe donné. Cette définition généralise en quelque sorte la définition 7.42 : « forme interne » au sens de la définition 7.42 correspond à « forme interne de la $k$-forme déployée $G^{\mathrm{s}}$ ». L'unicité de la forme déployée apparaît pour les formes quasi-déployées lorsqu'on se restreint aux formes internes d'un groupe donné. Plus précisément, on a le théorème [Spr98, 16.4.9] :

**Théorème 7.50.** *Soit $G$ un $k$-groupe semi-simple. Il existe alors une $k$-forme interne de $G$ qui est quasi-déployée, et celle-ci est unique à $k$-isomorphisme près.*

La *forme interne quasi-déployée* du $k$-groupe $G$ sera notée $G'$. La relation « être forme interne de » est une relation d'équivalence qui partitionne l'ensemble des $k$-formes d'un groupe semi-simple donné en classes disjointes. Chacune de ces classes contient alors exactement un groupe quasi-déployé. Une classe particulière est celle de la forme déployée du groupe.

**Remarque 7.51.** Soit $L$ le corps de déploiement de la forme interne quasi-déployée $G'$ de $G$. Alors $L$ est le corps minimal (au sens de la remarque 7.47) pour lequel $G|L$ devient une forme interne.

**Exemple 7.52.** Soit $f$ et $g$ deux formes quadratiques de dimension $n \geq 5$. Si $n$ est impair, alors $\mathrm{Spin}_f$ (resp. $\mathrm{SO}_f$) est de type B, et $\mathrm{Spin}_f$ (resp. $\mathrm{SO}_f$) est nécessairement une forme interne. Si $n$ est pair alors $\mathrm{Spin}_f$ (resp. $\mathrm{SO}_f$) est une forme interne de $\mathrm{Spin}_g$ (resp. $\mathrm{SO}_g$) exactement lorsque $f$ et $g$ possèdent le même discriminant (modulo $(k^\times)^2$) (cf. [Spr98, 17.3]).

**Remarque 7.53.** On rappelle ici la définition du *discriminant* $\mathrm{d}(f)$ d'une forme quadratique $f$. A équivalence près $f$ peut s'écrire sous forme diagonale :

$$f(x_1, \ldots, x_n) \quad = \quad a_1 x_1^2 + \cdots + a_n x_n^2.$$

On considère alors $\mathrm{d}(f) := \prod_{i=1}^n a_i$ comme élément dans le quotient $k^\times/(k^\times)^2$. Il s'agit d'un invariant de l'espace quadratique $\mathbf{V}_f$. Il existe d'autres normalisations du discriminant, mais le contenu de l'exemple 7.52 reste invariant.

On termine par énoncer un résultat très facile à voir :

**Proposition 7.54.** *Soit $G$ un $k$-groupe et $H$ une forme interne de $G$. Alors leurs centres $Z_G$ et $Z_H$ sont isomorphes sur $k$.*

## §7.9 Groupes sur les corps finis

Nous terminons ce chapitre par le traitement des groupes algébriques définis sur des corps finis. De tels groupes apparaîtrons lorsque l'on abordera au chapitre suivant les groupes semi-simples définis sur des corps $\mathfrak{p}$-adiques. On désignera ici par $\mathbb{F}_q$ le corps fini à $q$ éléments.

**Théorème 7.55.** *Tout $\mathbb{F}_q$-groupe $G$ semi-simple et connexe est quasi-déployé.*

**Théorème 7.56.** *Si $\pi : G \to H$ est une $\mathbb{F}_q$-isogénie entre deux $\mathbb{F}_q$-groupes algébriques connexes, alors $G(\mathbb{F}_q)$ et $H(\mathbb{F}_q)$ possèdent le même ordre.*

Ces deux théorèmes sont corollaires d'un même théorème dû à Lang [PR94, §6.2]. Ils montrent que le type suffit avec le corps de déploiement $L$ à déterminer l'ordre de $G(\mathbb{F}_q)$ pour $G$ semi-simple connexe. Or $L$ est uniquement déterminé par son ordre, et donc par le degré $[L : \mathbb{F}_q]$. En particulier le tableau 7.1 (recopié à partir de [Ono66, table 1]) présente une liste complète des ordres de $G(\mathbb{F}_q)$ pour $G$ connexe d'un type classique (non trialitaire) irréductible.

On sera aussi intéressé à l'ordre du tore anisotrope de l'exemple 7.36. On place ce calcul facile dans la proposition qui suit. On observe que là aussi le corps $\ell$, qui prend dans cette situation le rôle du corps de déploiement, n'influence pas la cardinalité.

**Proposition 7.57.** *Soit le $\mathbb{F}_q$-tore $T := \mathbf{R}^{(\mathbf{1})}_{\ell|\mathbb{F}_q}(\mathbf{G}_\mathrm{m})$ de dimension 1 (i.e. $\ell|\mathbb{F}_q$ est une extension quadratique, ou de manière équivalente $\ell = \mathbb{F}_{q^2}$). Alors l'ordre de $T(\mathbb{F}_q)$ vaut $q + 1$.*

PREUVE. On a l'isomorphisme

$$\mathbf{R}_{\ell|\mathbb{F}_q}(\mathbf{G}_{\mathrm{m}})(\mathbb{F}_q) \quad \cong \quad \mathbf{G}_{\mathrm{m}}(\ell),$$

qui montre que ce premier groupe possède un ordre égal à $q^2-1$ (qui est la cardinalité de $\ell^\times$). Or selon [PR94, §6.2 : Corollary 2] la norme $N_{\ell|\mathbb{F}_q}$ est surjective pour les corps finis. Par définition $T(\mathbb{F}_q)$ est le noyau de la norme, restreinte à $\mathbf{R}_{\ell|\mathbb{F}_q}(\mathbf{G}_{\mathrm{m}})(\mathbb{F}_q)$. Comme le groupe image $\mathbf{G}_{\mathrm{m}}(\mathbb{F}_q) = \mathbb{F}_q^\times$ est d'ordre $q-1$, on obtient le résultat :

$$\#T(\mathbb{F}_q) \;=\; \frac{q^2-1}{q-1} \;=\; q+1.$$

□

| type de $G$ | cardinalité de $G(\mathbb{F}_q)$ |
|---|---|
| ${}^1\mathrm{A}_r$ $(r \geq 1)$ | $q^{r(r+1)/2}\prod_{j=1}^{r}(q^{j+1}-1)$ |
| ${}^2\mathrm{A}_r$ $(r \geq 2)$ | $q^{r(r+1)/2}\prod_{j=1}^{r}(q^{j+1}-(-1)^{j+1})$ |
| $\mathrm{B}_r$ ou $\mathrm{C}_r$ $(r \geq 2)$ | $q^{r^2}\prod_{j=1}^{r}(q^{2j}-1)$ |
| ${}^1\mathrm{D}_r$ $(r \geq 4)$ | $q^{r(r-1)}(q^r-1)\prod_{j=1}^{r-1}(q^{2j}-1)$ |
| ${}^2\mathrm{D}_r$ $(r \geq 4)$ | $q^{r(r-1)}(q^r+1)\prod_{j=1}^{r-1}(q^{2j}-1)$ |

TAB. 7.1 – Ordres des groupes classiques semi-simples sur $\mathbb{F}_q$

# Chapitre 8. Eléments de la théorie de Bruhat-Tits

L'étude des groupes algébriques semi-simples définis sur un corps $\mathfrak{p}$-adique, ou plutôt l'étude des points rationnels de tels groupes, apparaît comme cas particulier d'un vaste programme réalisé principalement par Bruhat et Tits et publié sur plusieurs années [BT72] [BT84] [BT87]. Nous présentons ici certains éléments de cette théorie. L'ampleur du sujet, mais aussi sa complexité, nous contraint à renoncer à faire figurer les définitions précises de plusieurs concepts fondamentaux qui interviennent. A côté de [BT72] et [BT84], la référence standard sur le sujet est le survol donné par [Tit79], qui contient notamment une précieuse partie de classification. Notre discussion s'inspire également de [PR94, §3.4].

Dans ce chapitre $G$ désignera toujours un groupe absolument simple, défini sur un corps $\mathfrak{p}$-adique $k_v$. On suppose que $G$ n'est pas anisotrope. De plus, même si cela n'est pas une restriction impérative dans la théorie de Bruhat-Tits, nous supposerons $G$ simplement connexe, ce qui simplifie grandement la discussion. On considère $G(k_v)$ avec sa topologie induite par la topologie métrique sur $k_v$. Notre principal but, motivé par la discussion menée en §6.4, est de comprendre la description de certains sous-groupes compacts de $G(k_v)$ que permet la théorie de Bruhat-Tits. Ce chapitre comporte plusieurs exemples qui seront utilisés plus tard.

## §8.1 Système de Tits affine dans $G(k_v)$

Le système de Tits attribué par le théorème 7.29 pour chaque groupe semi-simple est habituellement qualifié de *sphérique* : le groupe de Coxeter d'un tel système étant fini, il opère comme groupe de réflexions sur une sphère. Un système de Tits sera dit *affine* lorsque son groupe de Coxeter opère comme groupe infini discret de réflexions sur un espace euclidien. Rappelons que ces groupes de Coxeter, eux-mêmes dit *affines*, apparaissent essentiellement tous en lien avec les systèmes de racines [Hum90, Ch. 4]. A chaque système de racines $\Phi$ réduit et irréductible est associé un groupe de Coxeter affine qui dépend à isomorphisme près uniquement du type de $\Phi$. Ce groupe est un produit semi-direct entre le groupe de Weyl de $\Phi$ et un groupe de translations. Le graphe de Coxeter de ce groupe affine s'obtient en ajoutant un noeud au graphe de Coxeter sous-jacent au diagramme de Dynkin de $\Phi$. Pour fixer les idées nous donnons dans la figure 8.1 pour chaque type classique le graphe de Coxeter du groupe affine associé. On y a surmonté du label « 0 » le noeud rajouté au graphe du groupe sphérique.

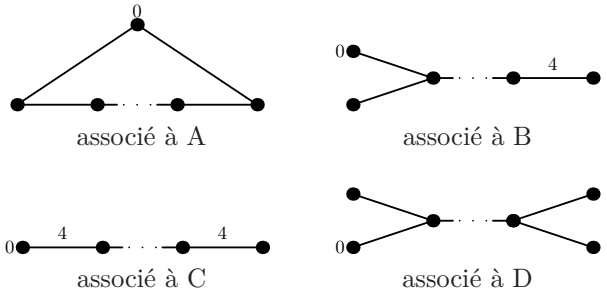



FIG. 8.1 – Groupes de Coxeter affines associés aux types classiques

Choisissons un $k_v$-tore déployé maximal de $G$, que nous noterons par $T$ afin de ne pas surcharger la notation (ce tore serait noté ${}_{k_v}T$ si l'on suivait §7.5). Ce tore n'est pas nécessairement maximal, $k_v$ n'étant pas algébriquement clos. Soit $Z = Z_G(T)$ (resp. $N = N_G(T)$) le centralisateur (resp. normalisateur) de $T$. On définit en plus le sous-groupe de $Z(k_v)$ suivant :

$$Z_c \quad := \quad \left\{ x \in Z(k_v) \mid a(x) \in \mathscr{O}_v^\times \ \ \forall a \in \mathbf{X}_{k_v}(Z) \right\}, \tag{8.1}$$

où $\mathbf{X}_{k_v}(Z)$ désigne le groupe abélien des *caractères $k_v$-rationnels* de $Z$, i.e. des $k_v$-homomorphismes $Z \to \mathbf{G}_{\mathrm{m}}$. Le groupe $Z_c$ n'est pas le groupe des points rationnels d'un sous-groupe algébrique de $Z$. Il s'agit du sous-groupe compact maximal de $Z$. Le groupe

$$\widetilde{W} \quad := \quad N(k_v)/Z_c \tag{8.2}$$

est alors une extension du groupe $W := {}_{k_v}W$, celui-ci pouvant en fait s'écrire comme quotient des $k_v$-points : $W \cong N(k_v)/Z(k_v)$. Il est possible de voir que $\widetilde{W}$ est en fait un groupe de Coxeter affine. Si $S \subset N(k_v)$ est un ensemble de générateurs de $W$, alors il existe $s_0 \in N(k_v)$ tel que $(\widetilde{W}, \widetilde{S})$ est un système de Coxeter affine, avec $\widetilde{S} := S \cup \{s_0\}$.

La théorie de Bruhat-Tits montre l'existence d'un sous-groupe $\widetilde{B} \subset G(k_v)$ compact et ouvert, tel que :

$$\widetilde{B} \cap N(k_v) \quad = \quad Z_c. \tag{8.3}$$

$$\left(G(k_v), \widetilde{B}, N(k_v), \widetilde{S}\right) \text{ est un système de Tits .} \tag{8.4}$$

Le sous-groupe $\widetilde{B}$, ainsi que chacun de ses conjugués dans $G(k_v)$ est appelé *sous-groupe d'Iwahori*. Ces sous-groupes tiennent ici le rôle que prenaient les sous-groupes de Borel dans le cas classique. La définition 7.26 attribue un *type* $I \subset \widetilde{S}$ à chaque sous-groupe de $G(k_v)$ contenant un sous-groupe d'Iwahori. Un groupe de type $I \subset \widetilde{S}$ est par définition conjugué au groupe $P_I = \widetilde{B}\widetilde{W}_I\widetilde{B}$ et, pour autant que $I \neq \widetilde{S}$, le groupe $\widetilde{W}_I$ est fini (sous l'hypothèse que $G$ est absolument simple), ce qui fait de $P_I$ un sous-groupe compact et ouvert de $G(k_v)$.

**Définition 8.1.** Un sous-groupe $P \subsetneq G(k_v)$ qui contient un sous-groupe d'Iwahori est appelé *sous-groupe parahorique* de $G(k_v)$. (On rappelle que ici $G$ est supposé simplement connexe.)

**Remarque 8.2.** Notre choix de noter les « objets affines » par des symboles surmontés d'un « tilde » $\widetilde{\ }$ , inspiré de la notation usuelle pour les types affines, se différencie de la notation de [Tit79], où ${}^v\tilde{W}$ correspond à notre $W$. Nous mettons en garde le lecteur contre d'autres différences entre notre notation et celles des références citées . Nous profitons encore d'insister sur le fait que les notations $W$ et $\widetilde{W}$ indiquent des objets qui dépendent du corps $k_v$.

## §8.2 Appartements de $G(k_v)$

On notera ici par $V$ l'espace vectoriel réel

$$V \quad := \quad \mathbf{X}_*(T) \otimes_{\mathbb{Z}} \mathbb{R}, \tag{8.5}$$

où $\mathbf{X}_*(T)$ désigne le groupe abélien des *cocaractères* de $T$, c'est-à-dire le groupe des homomorphismes algébriques $\mathbf{G}_{\mathrm{m}} \to T$. L'espace dual $V^*$ de $V$ s'identifie alors avec $\mathbf{X}(T) \otimes_{\mathbb{Z}} \mathbb{R}$ de la façon suivante : si $a \in \mathbf{X}(T)$ et $\lambda \in \mathbf{X}_*(T)$ on pose $a(\lambda) := n$, où $a \circ \lambda : \mathbf{G}_{\mathrm{m}} \to \mathbf{G}_{\mathrm{m}}$ est l'homomorphisme algébrique $x \mapsto x^n$ (tout homomorphisme $\mathbf{G}_{\mathrm{m}} \to \mathbf{G}_{\mathrm{m}}$ doit être de cette forme pour un certain entier $n \in \mathbb{Z}$). Le système de racines $\Phi := {}_{k_v}\Phi$ relatif à $T$ sera alors vu comme un ensemble de fonctions linéaires sur $V$. De plus, le groupe $W$ opère sur $V$ comme groupe fini de réflexions, l'opération étant donnée par la conjugaison.

Le groupe $\widetilde{W}$ opère quant à lui de façon canonique sur $V$ comme groupe de transformations affines. Chaque réflexion de $\widetilde{W}$ fixe un hyperplan affine appelé *mur*. L'opération de $\widetilde{W}$ partitionne ainsi l'espace $V$ en un complexe simplicial (chaque simplexe étant délimité par des murs) que nous noterons par $\mathscr{A}$ et qui est appelé *appartement* (par rapport à $T$). Comme ensemble $V$ et $\mathscr{A}$ coïncident. Si on le munit d'un produit scalaire invariant par $W$, l'espace $V$ peut être vu comme la réalisation géométrique du complexe $\mathscr{A}$, et nous utiliserons la notation $\mathscr{A}_{\mathbb{R}}$ par la suite pour désigner $V$ vu comme espace métrique. Un simplexe maximal dans $\mathscr{A}$ sera appelé une *chambre* de l'appartement. Il s'agit d'un partie compacte de $\mathscr{A}_{\mathbb{R}}$. L'appartement peut est recouvert par l'ensemble de ses chambres.

## §8.3 L'immeuble affine

A tout système de Tits est associé un objet de nature géométrique appelé *immeuble* [AB08]. Dans le cas de $G(k_v)$, la considération de l'immeuble conduit à une preuve fort élégante du corollaire 8.5 qui apparaît plus bas, raison pour laquelle nous introduisons cette notion. La construction de l'immeuble de $G(k_v)$ peut se faire de façon « abstraite » par la seule considération de son système de Tits (8.4) (une fois l'existence du sous-groupe $\widetilde{B}$ admis). Cette approche, bien qu'envisagée dans la théorie de Bruhat-Tits [BT72], peut être remplacée par une construction plus concrète de l'immeuble de $G(k_v)$, qui consiste à recoller les appartements dont il est question en §8.2.

A chaque $k_v$-tore déployé maximal de $G(k_v)$ est associé un appartement. Par le théorème 7.37 chacun de ces tores peut s'écrire comme conjugué $gTg^{-1}$ du tore fixé $T$, pour un élément $g \in G(k_v)$. On peut voir l'*immeuble affine* de

$G(k_v)$, noté $\mathscr{I}$, comme un certain complexe simplicial muni d'une opération de $G(k_v)$ pour laquelle

$$\mathscr{I} = \bigcup_{g \in G(k_v)} g\mathscr{A}, \tag{8.6}$$

et $g\mathscr{A}$ s'identifie avec l'appartement associé au tore $gTg^{-1}$. Si l'on considère $\mathscr{A}_{\mathbb{R}}$ plutôt que $\mathscr{A}$, on peut aussi considérer la réalisation géométrique $\mathscr{I}_{\mathbb{R}}$ de $\mathscr{I}$. Signalons que la réunion (8.6) n'est pas disjointe. L'immeuble possède la propriété suivante : pour chaque $x, y \in \mathscr{I}_{\mathbb{R}}$ il existe un appartement contenant $x$ et $y$. La réalisation géométrique $\mathscr{I}_{\mathbb{R}}$ possède alors une structure d'espace métrique complet, donné par le recollement des métriques de chaque appartement. L'opération de $G(k_v)$ sur $\mathscr{I}_{\mathbb{R}}$ est continue pour cette métrique.

Grâce à l'immeuble $\mathscr{I}$ nous pouvons donner une caractérisation des sous-groupes d'Iwahori. Une chambre C d'un appartement $g\mathscr{A}$ sera également appelée *chambre* lorsque considérée comme sous-ensemble de $\mathscr{I}$. Il faut relever qu'une chambre C de l'immeuble est chambre de plusieurs appartements à la fois. Notons par $G(k_v)^{\mathrm{C}}$ le sous-groupe de $G(k_v)$ qui laisse C fixe. Un sous-groupe de $G(k_v)$ est un sous-groupe d'Iwahori précisément lorsqu'il est de la forme $G(k_v)^{\mathrm{C}}$, avec C une chambre de $\mathscr{I}$.

**Exemple 8.3.** Lorsque le groupe $G$ est de $k_v$-rang égal à 1, il est possible de visualiser l'immeuble affine de $G(k_v)$. Dans ce cas il s'agit en effet d'un arbre [Tit79, 2.7]. Considérons par exemple $\mathrm{SL}_2$ (qui possède un rang égal à 1) comme groupe défini sur $\mathbb{Q}_2$. L'immeuble affine de $\mathrm{SL}_2(\mathbb{Q}_2)$ correspond à l'arbre suivant :

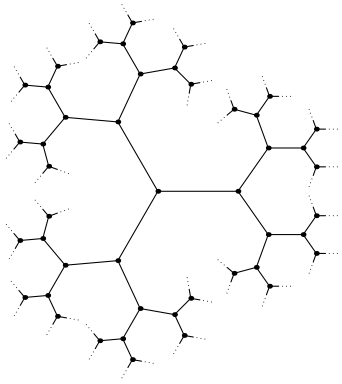


FIG. 8.2 – Immeuble affine de $\mathrm{SL}_2(\mathbb{Q}_2)$

Chaque chambre correspond à un segment . C'est uniquement par commodité que les chambres apparaissent de tailles différentes dans la figure 8.2 : considérées comme parties d'espace métrique, toutes les chambres ont la même longueur. Chaque appartement de l'immeuble correspond à une branche sans extrémité :



Un appartement est donc bien un complexe simplicial obtenu en partitionnant l'espace vectoriel réel de dimension 1. On voit que l'immeuble est un recollement de tous les appartements, et qu'une chambre donnée est contenue dans une infinité d'appartements.

Les travaux de Bruhat et Tits montrent le résultat suivant :

**Théorème 8.4** (Point fixe de Bruhat-Tits)**.** *Tout groupe compact d'isométries de $\mathscr{I}_{\mathbb{R}}$ fixe un point.*

IDÉE DE LA PREUVE. Même si l'immeuble $\mathscr{I}$ est qualifié d'*affine* (voir même souvent d'*euclidien* dans la littérature), l'espace métrique $\mathscr{I}_{\mathbb{R}}$ est plutôt « hyperbolique » : il s'agit d'un espace CAT(0) (on peut en particulier le voir sur l'exemple de la figure 8.2). Ceci permet de montrer que chaque sous-ensemble compact (ou plus généralement borné) de $\mathscr{I}_{\mathbb{R}}$ contient un point unique qui lui sert de centre (pour une certaine définition appropriée de la notion de « centre »). Soit alors $H$ un groupe compact d'isométries de $\mathscr{I}_{\mathbb{R}}$. Pour $x \in \mathscr{I}_{\mathbb{R}}$ l'orbite $Hx$ est compacte et possède ainsi un centre, qui doit être fixé par $H$. Le lecteur peut se référer à [AB08, §11.2 - §11.3] pour les détails. □

**Corollaire 8.5.** *Chaque sous-groupe compact de $G(k_v)$ est contenu dans un sous-groupe parahorique. Ainsi les sous-groupes compacts maximaux de $G(k_v)$ sont les sous-groupes parahoriques maximaux.*

PREUVE. Soit $H \subset G(k_v)$ un sous-groupe compact. Par le théorème 8.4, $H$ fixe un point $x \in \mathscr{I}_{\mathbb{R}}$, ce qui montre que $H \subset G(k_v)^x$ (le stabilisateur de $x$). Mais $G(k_v)^{\mathrm{C}} \subset G(k_v)^x$, où C est une chambre contenant $x$. Comme $G(k_v)^{\mathrm{C}}$ est un sous-groupe d'Iwahori, le sous-groupe $G(k_v)^x$ est donc bien parahorique. □

## §8.4 Diagramme de Dynkin local

Nous utilisons ici les notations de §8.1 associée au groupe $G|k_v$. Tout hyperplan affine de $\mathscr{A}_{\mathbb{R}}$ s'écrit sous la forme

$$H_\alpha \quad = \quad \alpha^{-1}(0),$$

où $\alpha : \mathscr{A}_{\mathbb{R}} \to \mathbb{R}$ est une fonction affine, i.e une fonction de la forme $x \mapsto Ax + s$, où la fonction $A$ (appelée *partie vectorielle* de $\alpha$) est linéaire et $s \in \mathbb{R}$. Soit $\widetilde{\Phi}$ l'ensemble des fonctions affines $\alpha$ pour lesquelles $H_\alpha$ est un mur. La partie vectorielle d'un élément de $\widetilde{\Phi}$ est alors un élément de $\Phi$. L'ensemble $\widetilde{\Phi}$ est un *système de racines affines* ou *échelonnage*. Un tel système est décrit par son *diagramme (de Dynkin) local*. Il s'agit d'un diagramme qui s'obtient à partir d'une « base » $\widetilde{\Delta} \subset \widetilde{\Phi}$ du système. Le diagramme ne dépend que du groupe $G|k_v$. Dans [Tit79, §4] apparaît une liste des diagrammes de Dynkin locaux en fonction du type de $G$ relatif à $k_v$. Nous aurons besoin par la suite d'utiliser cette classification.

Les diagrammes de Dynkin locaux possèdent la même allure que les diagrammes de Dynkin vu en 7.17. Les différences sont les suivantes :

- les noeuds du diagramme local sont donné par des traits plutôt que par des cercles pleins. Ceci présente l'avantage d'éviter tout confusion entre cas local et cas classique.
- En plus des arêtes simples, doubles et triples, un quatrième type d'arêtes peut apparaître, représentées par un trait accentué : ⟝. Ce type d'arêtes correspond au poids $\infty$ dans le graphe de Coxeter sous-jacent au diagramme.

– Les noeuds des diagrammes locaux sont souvent surmontés de labels qui possèdent des significations diverses. Ces labels incluent des nombres entiers, ainsi que des croix : $\times$. Nous n'aurons pas besoin des ces deux types de labels, et nous les omettrons dans nos diagrammes. Un troisième type de labels, notés « $s$ » ou « $hs$ », sera expliqué dans la remarque 8.20.

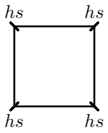
Le fait important qu'il nous faut retenir concernant les diagrammes de Dynkin locaux est donné dans la proposition que voici [Tit79, §1] :

**Proposition 8.6.** *Le graphe de Coxeter sous-jacent au diagramme local de $\widetilde{\Phi}$ correspond au graphe du groupe $\widetilde{W}$.*

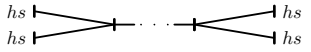
Nous allons noter par $\Delta_v$ le diagramme de Dynkin local du groupe $G$ sur $k_v$. Cette proposition permet d'identifier les noeuds de $\Delta_v$ avec l'ensemble $\widetilde{S}$ des générateurs du groupe $\widetilde{W}$. Si $r_v$ est le $k_v$-rang de $G$, alors $\Delta_v$ comprend exactement $r_v + 1$ noeuds. L'omission du noeud correspondant au générateur $s_0 \in \widetilde{S}$ donne un diagramme de Dynkin dont le graphe de Coxeter sous-jacent est celui du groupe de Weyl relatif $W = {}_{k_v}W$. Cette proposition permettra surtout de voir les types des sous-groupes parahoriques directement sur le diagramme : chaque type correspond à un sous-ensemble $I$ de noeuds de $\Delta_v$, ce que l'on abrège par $I \subset \Delta_v$.

Voici quelques exemples de diagrammes de Dynkin locaux. Ils apparaissent tous dans [Tit79, 4.2].

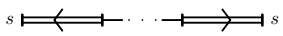
**Exemple 8.7.** Si $G$ est déployé sur $k_v$ et de type $\mathrm{A}_3$, alors $\Delta_v$ est donné par :




**Exemple 8.8.** Si $G$ est déployé sur $k_v$ et de type $\mathrm{D}_r$ (avec $r \geq 4$), alors $\Delta_v$ est donné par :




**Exemple 8.9.** Supposons que $G$ soit de type $\mathrm{D}_r$ (avec $r \geq 3$) et qu'il soit quasi-déployé sur $k_v$, mais ne se déploie pas sur l'extension maximale non ramifiée $\hat{k}_v$. Si $r = 4$ on suppose encore que $G$ n'est pas une forme trialitaire (ceci impose à $G$ d'avoir un $k_v$-rang égal à $r - 1$). Alors $\Delta_v$ est donné par :




Le graphe de Coxeter sous-jacent à $\Delta_v$ est le graphe du groupe affine lié au type sphérique $\mathrm{C}_{r-1}$ (cf. figure 8.1).

## §8.5 Indice de Tits local

On va plus loin dans l'analyse de la structure de $G|k_v$ en associant à chaque groupe un « indice de Tits local ». La théorie de Bruhat-Tits fait appel à l'extension maximale non ramifiée $\hat{k}_v|k_v$ (plutôt que la clôture algébrique) pour passer au cas « absolu ». On peut en effet analyser la structure de $G$ sur $\hat{k}_v$ selon les mêmes principes qu'exposés jusqu'ici pour $k_v$.

**Remarque 8.10.** Le groupe $G$ est nécessairement quasi-déployé sur $\hat{k}_v$ [Tit79, 1.10.4].

Considérons un $\hat{k}_v$-tore déployé maximal $\widehat{T}$ de $G$ qui contient le $k_v$-tore $T$. En appliquant la théorie sur $\widehat{T}$ plutôt que sur $T$ on obtient un appartement $\widehat{\mathscr{A}}$, dont l'ensemble des points fixés par $\mathrm{Gal}(\hat{k}_v|k_v)$ s'identifie avec l'appartement $\mathscr{A}$ associé à $T$. Ceci associe un système de racines affines relatif à $\widehat{T}$ caractérisé par son diagramme de Dynkin local $\widehat{\Delta}_v$. Le groupe $\mathrm{Gal}(\hat{k}_v|k_v)$ opère alors sur les noeuds de $\widehat{\Delta}_v$ et, de manière similaire au cas classique les orbites de cette opération s'identifient avec les noeuds de $\Delta_v \cup \{0\}$.

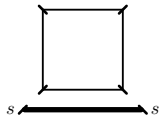
**Remarque 8.11.** Contrairement au cas classique où l'ensemble $\Delta^0$ apparaît fréquemment, dans le cas local, à la seule exception près du type nommé ${}^dA_{2d-1}$ dans [Tit79, 4.3], chaque noeud de $\widehat{\Delta}_v$ est « projeté » sur un noeud de $\Delta_v$.

L'*indice (de Tits) local* de $G$ (relatif à $k_v$) s'obtient en plaçant le diagramme $\Delta_v$ sous $\widehat{\Delta}_v$, en mettant les éléments de $\widehat{\Delta}_v$ d'une même orbite, ainsi que le noeud de $\Delta_v$ correspondant, dans le même alignement. Dans [Tit79, §4] se retrouve alors pour chaque type de $k_v$-groupe son indice local associé. En voici quelques exemples, qui seront utiles dans la suite de cette thèse.

**Exemple 8.12.** Si $G|k_v$ est déployé, son indice local correspond simplement à deux copies de son diagramme local. Dans ce cas on se contente en pratique de représenter l'indice local par une seule copie du diagramme local. C'est la situation des exemples 8.7 et 8.8.

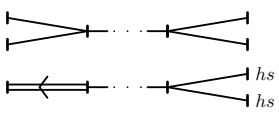
**Exemple 8.13.** Si comme dans l'exemple 8.9 le groupe $G$ possède un $k_v$-rang égal au $\hat{k}_v$-rang, alors l'indice local est trivial (dans le même sens que dans l'exemple 8.12). Une seule copie du diagramme local sera là aussi nécessaire.

**Exemple 8.14.** L'indice local d'un groupe $G$ de type ${}^1\mathrm{A}_{3,1}$ est de la forme :




Les éléments de $\widehat{\Delta}_v$ sur des sommets opposés sont donc dans la même orbite.

**Exemple 8.15.** On suppose que $G$ soit du type ${}^2\mathrm{D}_{r,r-1}$ (avec $r \geq 4$) et que $G$ soit déployé sur $\hat{k}_v$. Alors l'indice local de $G$ vaut :



## §8.6 Sous-groupes spéciaux et hyperspéciaux

Considérons le diagramme local $\Delta_v$ associé au groupe $G$ sur $k_v$.

**Définition 8.16.** Un noeud du diagramme de Dynkin $\Delta_v$ est dit *spécial* si lorsque on soustrait ce noeud à $\Delta_v$ on obtient un diagramme dont le graphe de Coxeter sous-jacent est le graphe du groupe de Weyl $W = {}_{k_v}W$. Soit $\alpha$ un noeud spécial de $\Delta_v$. Les sous-groupes parahoriques de $G(k_v)$ de type $I = \Delta_v \smallsetminus \{\alpha\}$ sont eux-mêmes dits *spéciaux*.

Nous avons vu en §8.1 que le graphe de Coxeter de $\widetilde{W}$ s'obtient en ajoutant un noeud (qui correspond au générateur $s_0$) au graphe de $W$. Comme le graphe de $\widetilde{W}$ est sous-jacent à $\Delta_v$ il existe donc au moins un noeud spécial sur $\Delta_v$.

Un sous-groupe parahorique spécial est clairement maximal. Mais en général il existe plusieurs noeuds $\alpha$ de $\Delta_v$ qui ne sont pas spéciaux, et pour chacun de ceux-ci correspond un sous-groupe parahorique maximal de type $\Delta_v \smallsetminus \{\alpha\}$ qui n'est pas spécial. Une propriété importante des sous-groupes spéciaux est liée à la question du volume [BP89, A.5] :

**Proposition 8.17.** *Supposons fixée sur $G(k_v)$ une mesure de Haar. Chaque sous-groupe parahorique de $G(k_v)$ qui est de volume maximal est spécial.*

**Définition 8.18.** Supposons $G|\hat{k}_v$ déployé. Dans ce cas un noeud de $\Delta_v$ sera appelé *hyperspécial* si l'orbite qui lui correspond dans $\widehat{\Delta}_v$ sur l'indice local est constituée d'un seul noeud spécial. De façon similaire à ce qui est fait dans la définition 8.16 on peut alors appliquer cette dénomination pour certains sous-groupes parahoriques de $G(k_v)$.

Comme la terminologie le fait penser, tout sous-groupe hyperspécial est spécial [Tit79, 1.10.2]. Lorsque $\Delta_v$ possède des noeuds hyperspéciaux, on a un raffinement de la proposition 8.17 : les sous-groupes parahoriques de volumes maximaux dans $G(k_v)$ sont hyperspéciaux [Tit79, 3.8.2]. Sous certaines conditions on peut prouver l'existence de sous-groupes parahoriques hyperspéciaux [Tit79, 1.10.2] :

**Proposition 8.19.** *Si $G|k_v$ est quasi-déployé et $G|\hat{k}_v$ est déployé, alors $\Delta_v$ possède au moins un noeud hyperspécial.*

**Remarque 8.20.** Sur le diagramme local $\Delta_v$ un noeud spécial (mais pas hyperspécial) est noté d'un label « $s$ », tandis qu'un noeud hyperspécial est noté avec le label « $hs$ ».

## §8.7 Structure des sous-groupes parahoriques

Nous examinons ici un aspect structural des sous-groupes parahoriques, qui permettra le calcul de volume présenté au chapitre 9. Un sous-groupe parahorique $P \subset G(k_v)$, à l'instar du sous-groupe $Z_c$, n'est pas formé par les points rationnels d'un $k_v$-sous-groupe de $G$. La théorie de Bruhat-Tits permet pourtant d'attribuer une structure algébro-géométrique à $P$. Pour cela nous devons faire appel à la notion de schéma en groupes affines (à laquelle le lecteur trouvera une introduction dans [Wat79]). En effet, notre définition de groupe algébrique

(définition 2.12) nécessite de travailler avec des objets (variétés) définis sur un corps. Un *schéma en groupes affines lisse* peut être vu comme une généralisation de la notion de groupe algébrique linéaire qui permet (entre autres) de traiter avec des objets définis sur un anneau (commutatif et avec élément identité). Par exemple sur $\mathrm{SL}_n|\mathbb{Q}$ peut être mis une structure de schéma en groupes défini sur $\mathbb{Z}$, dont les points rationnels sont alors $\mathrm{SL}_n(\mathbb{Z})$. Plus généralement, si $\mathcal{G}$ est un schéma en groupes affines lisse défini sur un anneau $R$, alors est défini son groupe des points $R$-rationnels $\mathcal{G}(R)$. Une propriété essentielle dans théorie de Bruhat-Tits est donnée dans la proposition suivante [Tit79, 3.4.1] :

**Proposition 8.21.** *Chaque sous-groupe parahorique $P$ de $G(k_v)$ s'écrit sous la forme :*

$$P \quad = \quad \mathcal{G}_P(\mathscr{O}_v),$$

*où $\mathcal{G}_P$ est un schéma en groupes affines lisse défini sur $\mathscr{O}_v$ qui est défini canoniquement (à isomorphisme près).*

Cette proposition nous a placé dans la délicate situation consistant à parler de schéma en groupes, sans avoir défini ou expliqué en détails cette notion. Fort heureusement il y a un échappatoire : en utilisant l'application $\mathscr{O}_v \to \mathbb{F}_v$ de réduction modulo $v$ (cf. (5.8)) nous obtenons une application surjective :

$$\mathcal{G}_P(\mathscr{O}_v) \quad \to \quad \overline{\mathcal{G}}_P(\mathbb{F}_v), \tag{8.7}$$

où $\overline{\mathcal{G}}_P$ est un groupe algébrique défini sur le corps $\mathbb{F}_v$, et défini canoniquement à partir de $\mathcal{G}_P$. Sous notre hypothèse que $G$ est simplement connexe, on a que $\overline{\mathcal{G}}_P$ est connexe.

Le $\mathbb{F}_v$-groupe $\overline{\mathcal{G}}_P$ possède une décomposition en produit semi-direct

$$\overline{\mathcal{G}}_P \quad = \quad \overline{\mathcal{G}}_P^{\mathrm{red}} \cdot \overline{U}_P,$$

où $\overline{U}_P$ est le *radical unipotent* de $\overline{\mathcal{G}}_P$ [Bor91, 11.21] et $\overline{\mathcal{G}}_P^{\mathrm{red}}$ est un $\mathbb{F}_v$-sous-groupe connexe défini canoniquement à isomorphisme près. Ce groupe $\overline{U}_P$ n'aura pas d'importance pour nous par la suite. Le groupe $\overline{\mathcal{G}}_P^{\mathrm{red}}$ est un groupe *réductif*, c'est-à-dire qu'il peut s'écrire comme *produit presque direct* (i.e $\overline{\mathcal{G}}_P^{\mathrm{ss}} \cap \overline{T}_P$ est fini) :

$$\overline{\mathcal{G}}_P^{\mathrm{red}} \quad = \quad \overline{\mathcal{G}}_P^{\mathrm{ss}} \cdot \overline{T}_P, \tag{8.8}$$

où $\overline{\mathcal{G}}_P^{\mathrm{ss}}$ est un groupe sur $\mathbb{F}_v$ semi-simple, et $\overline{T}_P$ est soit le groupe trivial $\{1\}$, soit un $\mathbb{F}_v$-tore. Le *rang* (absolu) de $\overline{\mathcal{G}}_P^{\mathrm{red}}$, défini comme la dimension des tores maximaux de $\overline{\mathcal{G}}_P^{\mathrm{red}}$, s'obtient ainsi en additionnant $\dim(\overline{T})$ avec le rang absolu de $\overline{\mathcal{G}}_P^{\mathrm{ss}}$. Nous résumons dans la proposition suivante les éléments de structure concernant $\overline{\mathcal{G}}_P^{\mathrm{red}}$ dont nous aurons besoin :

**Proposition 8.22.** *Soit $P \subset G(k_v)$ un sous-groupe parahorique de type $I \subset \Delta_v$. Alors :*

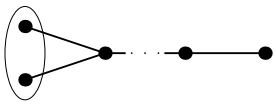
1. *Le rang absolu de $\overline{\mathcal{G}}_P^{\mathrm{red}}$ est égal au $\hat{k}_v$-rang de $G$.*
2. *Le $\mathbb{F}_v$-rang de $\overline{\mathcal{G}}_P^{\mathrm{red}}$ est égal au $k_v$-rang de $G$.*
3. *L'indice de Tits du groupe $\overline{\mathcal{G}}_P^{\mathrm{ss}}|\mathbb{F}_v$ s'obtient à l'aide de l'indice local de la manière suivante : pour chaque élément de $\Delta_v \smallsetminus I$, on retire l'orbite qui lui correspondant sur $\widehat{\Delta}_v$ (ainsi que les arêtes partant de cette orbite). L'indice de Tits de $\overline{\mathcal{G}}_P^{\mathrm{ss}}$ est donné alors par ce qui reste de ce diagramme, sur lequel on trace les orbites données par l'indice local.*

Ces éléments de structure apparaissent avec une plus grande précision dans [Tit79, 3.5]. Il est à noter que la remarque 8.11 assure le fait que $\overline{\mathcal{G}}_P^{\mathrm{ss}}$ est bien quasi-déployé, comme l'impose le théorème 7.55.

**Exemple 8.23.** Soit $G$ comme dans l'exemple 8.7. Alors n'importe quel sous-groupe parahorique maximal de $G(k_v)$ est de type $\Delta_v \smallsetminus \{\alpha\}$, où $\alpha$ est nécessairement un noeud hyperspécial. Pour tous ces sous-groupes $P$ maximaux, on a $\overline{\mathcal{G}}_P^{\mathrm{red}} = \overline{\mathcal{G}}_P^{\mathrm{ss}}$, et ce $\mathbb{F}_v$-groupe semi-simple est de type ${}^1\mathrm{A}_3$. De même si $G$ est comme dans l'exemple 8.8, il existe exactement quatre types de sous-groupes hyperspéciaux, pour lesquels $\overline{\mathcal{G}}_P^{\mathrm{red}} = \overline{\mathcal{G}}_P^{\mathrm{ss}}$ est de type ${}^1\mathrm{D}_r$.

**Exemple 8.24.** On suppose ici que $G$ est comme dans l'exemple 8.9, et soit $\alpha \in \Delta_v$ l'un des deux sommets spéciaux. Soit $P$ un sous-groupe parahorique de type $\Delta_v \smallsetminus \{\alpha\}$. On a $\overline{\mathcal{G}}_P^{\mathrm{red}} = \overline{\mathcal{G}}_P^{\mathrm{ss}}$, et ce groupe possède un rang absolu de $r-1$. Le $\mathbb{F}_v$-rang de $\overline{\mathcal{G}}_P^{\mathrm{ss}}$ correspond à son rang absolu : $\overline{\mathcal{G}}_P^{\mathrm{ss}}$ est déployé. Il s'agit d'un groupe de type ${}^1\mathrm{B}_{r-1}$.

**Exemple 8.25.** Soit $G$ comme dans l'exemple 8.15, $\alpha \in \Delta_v$ l'un des deux noeuds hyperspéciaux, et soit $P$ un sous-groupe parahorique de type $\Delta_v \smallsetminus \{\alpha\}$. En retirant le noeud $\alpha$ et son noeud correspondant dans $\widehat{\Delta}_v$ au diagramme local, on obtient l'indice de Tits de $\overline{\mathcal{G}}_P^{\mathrm{ss}} = \overline{\mathcal{G}}_P^{\mathrm{red}}$ :



Le groupe $\overline{\mathcal{G}}_P^{\mathrm{ss}}$ est donc ici de type ${}^2\mathrm{D}_r$.

**Exemple 8.26.** Soit $G$ comme dans l'exemple 8.14 et $P \subset G(k_v)$ un sous-groupe parahorique maximal. L'indice de Tits du groupe $\overline{\mathcal{G}}_P^{\mathrm{ss}}$ s'obtient en retirant un des deux sommets du diagrammes  ainsi que les deux sommets de son orbite correspondante dans $\widehat{\Delta}_v$, i.e. les deux sommets dans son alignement. On trouve que $\overline{\mathcal{G}}_P^{\mathrm{ss}}$ possède un indice de Tits donné par :

Ainsi $\overline{\mathcal{G}}_P^{\mathrm{ss}}$ est de type absolu $\mathrm{A}_1 \times \mathrm{A}_1$ ; il est déployé sur l'extension quadratique de $\mathbb{F}_v$, sans être déployé sur $\mathbb{F}_v$. Comme $\overline{\mathcal{G}}_P^{\mathrm{red}}$ est de $\hat{k}_v$-rang égal à 3 et que $\overline{\mathcal{G}}_P^{\mathrm{ss}}$ possède lui un $\hat{k}_v$-rang de 2, on voit que le $\mathbb{F}_v$-groupe $\overline{T}_P$ est un tore anisotrope de dimension 1.

## §8.8 Conjugaison des sous-groupes parahoriques

Il est clair, par la définition du type (définition 7.26), que lorsque l'on conjugue un sous-groupe parahorique $P$ par un élément $g \in G(k_v)$ on ne change pas son type. Par contre si $\phi \in \mathrm{Aut}_{k_v}(G)$ désigne un $k_v$-automorphisme de $G$ plus général, le sous-groupe parahorique $\phi(P)$ ne doit pas forcément avoir le même type que $P$. En particulier, le groupe $\overline{G}(k_v)$ des automorphismes internes définis sur $k_v$ (cf. §2.9) permute les types de sous-groupes parahoriques. Cela induit une opération de $\overline{G}(k_v)$ sur le diagramme de Dynkin local $\Delta_v$. Plus précisément, $\overline{G}(k_v)$ opère sur $\Delta_v$ par symétries qui conservent les arêtes ainsi que les labels. On dénote par $\mathrm{Aut}(\Delta_v)$ ce groupe des symétries, et on a donc un homomorphisme :

$$\overline{G}(k_v) \quad \to \quad \mathrm{Aut}(\Delta_v),$$

dont le noyau contient $\pi(G(k_v))$.

# Chapitre 9. La formule du volume de Prasad

L'outil central qui est utilisé pour obtenir les théorèmes 1.3 et 1.4 est une formule de volume pour les sous-groupes arithmétiques des groupes semi-simples, développée par Prasad [Pra89]. Cette formule fait un usage intensif de certains éléments de la théorie de Bruhat-Tits, aussi bien dans sa démonstration que dans son application.

## §9.1 Conventions sur le groupe $G$

Nous allons travailler dans ce chapitre (et dans les suivants) avec un groupe algébrique $G$ défini sur un corps de nombres $k$, avec $G$ supposé absolument simple et simplement connexe. La matière exposée au chapitre 3 doit suffire à expliquer ces restrictions.

Comme d'habitude $V = V_\infty \cup V_\mathrm{f}$ désigne l'ensemble des places (infinies et finies) de $k$, et $\mathcal{S} \subset V_\infty$ est l'ensemble des places $v \in V_\infty$ telles que $G(k_v)$ est non compact. On suppose que $\mathcal{S} \neq \emptyset$, c'est-à-dire que le groupe $G_\infty$ n'est pas compact. Le groupe

$$G_\mathcal{S} \quad := \quad \prod_{v \in \mathcal{S}} G(k_v) \tag{9.1}$$

et ses sous-groupes arithmétiques seront l'objet de notre attention. On rappelle que $G(k)$ s'y plonge diagonalement et que $G_\infty$ se projette sur $G_\mathcal{S}$ (avec noyau compact). On note par $\mathrm{C} := Z_G$ le centre (algébrique) de $G$. Le centre de $G_\mathcal{S}$, noté $\mathcal{Z}$, peut s'écrire comme

$$\mathcal{Z} \quad = \quad \prod_{v \in \mathcal{S}} \mathrm{C}(k_v). \tag{9.2}$$

## §9.2 Sous-groupes arithmétiques principaux

La formule de Prasad ne permet pas de traiter n'importe quel sous-groupe arithmétique dans $G_\mathcal{S}$. Nous commençons ici par définir les sous-groupes entrant dans son champ d'application. On rappelle qu'une collection cohérente $\mathscr{P}$ de sous-groupes de $G(k_v)$ (avec $v$ qui parcourt $V_\mathrm{f}$) détermine un sous-groupe arithmétique dans $G(k)$ (proposition 6.8).

**Définition 9.1.** Soit $\Lambda$ un sous-groupe arithmétique de $G(k)$. Supposons qu'il existe une collection cohérente $\mathscr{P} = (P_v)_{v \in V_\mathrm{f}}$ telle que pour chaque $v \in V_\mathrm{f}$ le sous-groupe $P_v$ est un sous-groupe parahorique de $G(k_v)$, et pour laquelle

$\Lambda_{\mathscr{P}} = \Lambda$ (avec $\Lambda_{\mathscr{P}}$ donné par (6.6)). Alors le sous-groupe arithmétique $\Lambda$ est dit *principal*.

On voit grâce à la proposition 6.9 qu'un sous-groupe arithmétique principal $\Lambda \subset G$ détermine uniquement la collection cohérente qui le définit. Si $(P_v)$ désigne cette collection cohérente, nous notons par $\theta_v \subset \Delta_v$ le type du sous-groupe parahorique $P_v$ tel que défini en §8.1. Ainsi pour chaque $v \in V_{\mathrm{f}}$ le type $\theta_v$ dépend uniquement de $\Lambda$, et on définit la collection

$$\theta \quad := \quad (\theta_v)_{v \in V_{\mathrm{f}}} \tag{9.3}$$

comme étant le *type global* du sous-groupe principal $\Lambda$.

Une collection quelconque de types $\theta = (\theta_v)$ n'est pas forcément le type global d'un sous-groupe principal de $G(k)$. Une condition nécessaire est donnée dans le lemme qui suit, dont la démonstration apparaît dans [Tit79, 3.9.1] :

**Lemme 9.2.** *Soit $\Lambda$ un sous-groupe arithmétique principal de $G$ et soit $\mathscr{P} = (P_v)_{v \in V_{\mathrm{f}}}$ sa collection cohérente associée. Alors $P_v$ est hyperspécial pour presque tous les $v \in V_{\mathrm{f}}$.*

**Remarque 9.3.** Si pour un nombre fini de places $v \in V_{\mathrm{f}}$ on remplace le sous-groupe parahorique $P_v$ de la collection cohérente $\mathscr{P}$ par un autre sous-groupe parahorique contenant le même sous-groupe d'Iwahori que $P_v$, on obtient une collection également cohérente. Par cette procédure de modification on construit une infinité de sous-groupes arithmétiques principaux de $G(k)$ (tous commensurables).

Une condition nécessaire pour la validité du lemme 9.2 est l'existence de sous-groupes parahoriques hyperspéciaux dans presque tous les $G(k_v)$. Nous allons expliquer ici comment cette condition peut se vérifier. Au vu de la proposition 8.19, il suffit voir que pour presque toutes les places $v \in V_{\mathrm{f}}$, on a que $G|k_v$ est quasi-déployé avec $G|\hat{k}_v$ déployé. Une partie du chemin est alors accomplie par le résultat suivant, démontré par exemple dans [PR94, theorem 6.7] :

**Théorème 9.4.** *$G|k_v$ est quasi-déployé pour presque tous les $v \in V_{\mathrm{f}}$.*

Il faut encore voir que l'ensemble de places

$$\mathscr{R} \quad := \quad \left\{ v \in V_{\mathrm{f}} \;\middle|\; G|\hat{k}_v \text{ n'est pas déployé} \right\} \tag{9.4}$$

est fini. Cela suit à l'aide du théorème 4.22 de la description alternive de $\mathscr{R}$ donnée dans la proposition :

**Proposition 9.5.** *Soit $L$ le corps de déploiement de la forme interne quasi-déployé $G'$ de $G$. L'ensemble $\mathscr{R}$ peut alors se décrire comme l'ensemble des places de $V_{\mathrm{f}}$ qui sont ramifiées dans $L|k$.*

Idée de la preuve. A l'aide des remarques 8.10 et 7.47, on voit que $G|\hat{k}_v$ n'est pas déployé si et seulement si il n'existe pas d'inclusion de $L$ dans $\hat{k}_v$. Or on peut observer grâce à la discussion sur la ramification en fin de §5.3, que ceci arrive exactement lorsque $v$ n'est pas ramifié dans $L|k$. □

## §9.3 La mesure normalisée $\mu$

Nous introduisons ici une normalisation particulière de la mesure de Haar sur $G_\infty$. Soit $v \in V_\infty$ une place fixée. Si $v$ est réelle on peut identifier $k_v$ avec $\mathbb{R}$ et ainsi considérer la forme réelle compacte $G_{\mathrm{u}}$ de $G|k_v$. Une mesure de Haar sur $G(k_v)$ correspond (de manière unique) à une forme multilinéaire alternée de degré maximal sur $\mathfrak{g}_{k_v}$. Cette forme s'étend canoniquement à une forme sur $\mathfrak{g}_{k_v} \otimes \mathbb{C}$, et cela détermine une forme multilinéaire alternée de degré maximal sur l'algèbre de Lie de $G_{\mathrm{u}}(\mathbb{R})$ (comme $G_{\mathrm{u}}(\mathbb{R})$ s'identifie avec un sous-groupe de $G(\mathbb{C})$). Pour $v \in V_\infty \setminus \mathcal{S}$ on a $G(k_v) = G_{\mathrm{u}}(\mathbb{R})$, et cette procédure est triviale. Ainsi à chaque mesure de Haar sur $G(k_v)$ correspond une unique mesure de Haar sur $G_{\mathrm{u}}(\mathbb{R})$, et on notera ces deux mesures par le même symbole. Pour $v$ réelle, on introduit alors la mesure de Haar $\mu_v$ sur $G(k_v)$, définie par

$$\mu_v(G_{\mathrm{u}}(\mathbb{R})) \quad = \quad 1. \tag{9.5}$$

Pour $v$ complexe on fait la même chose en prenant la forme réelle compacte du groupe $\mathbf{R}_{k_v|\mathbb{R}}(G)$. Il s'agit du produit direct de deux copies de l'unique groupe réel compact de même type que $G$. Pour chaque place complexe $v$ cela détermine alors également une mesure $\mu_v$, qui attribue la valeur 1 à ce groupe produit de deux facteurs compacts.

On prend alors comme mesure sur $G_\infty$ le produit des mesures $\mu_v$ :

$$\mu_\infty \quad := \quad \prod_{v \in V_\infty} \mu_v. \tag{9.6}$$

Cette normalisation est particulièrement adaptée pour traiter le covolume dans $G_{\mathcal{S}}$. En effet, pour la mesure restreinte

$$\mu_{\mathcal{S}} \quad := \quad \prod_{v \in \mathcal{S}} \mu_v, \tag{9.7}$$

et pour un sous-groupe discret $\Lambda \subset G(k)$ (qu'on voit comme sous-groupe de $G_\infty$, resp. de $G_{\mathcal{S}}$, par plongement diagonal) on a l'égalité :

$$\mu_{\mathcal{S}}(G_{\mathcal{S}}/\Lambda) \quad = \quad \mu_\infty(G_\infty/\Lambda).$$

Cela suit facilement du fait que pour les facteurs compacts $G(k_v)$ on a par définition de $\mu$ : $\mu_v(G(k_v)) = 1$.

Signalons encore que $\mu_{\mathcal{S}}$ peut aussi se voir comme mesure de Haar sur $G_{\mathcal{S}}/\mathcal{Z}$. Les algèbres de Lie de $G_{\mathcal{S}}$ et $G_{\mathcal{S}}/\mathcal{Z}$ s'identifient en effet canoniquement, et donc la forme multilinéaire altérnée qui détermine $\mu_{\mathcal{S}}$ donne également naissance à une mesure de Haar sur $G_{\mathcal{S}}/\mathcal{Z}$. Là aussi on utisera la même notation $\mu_{\mathcal{S}}$ pour la mesure sur le quotient. Si un sous-groupe arithmétique $\Gamma$ dans $G_{\mathcal{S}}$ contient le centre $\mathcal{Z}$, alors son quotient par $\mathcal{Z}$ est un réseau arithmétique de $\mathscr{G} = G_{\mathcal{S}}/\mathcal{Z}$ (cf. définition 3.17). Pour simplifier on notera simplement $\mathscr{G}/\Gamma$ pour $\mathscr{G}/(\Gamma/\mathcal{Z})$. On a alors :

$$\mu_{\mathcal{S}}(G_{\mathcal{S}}/\Gamma) \quad = \quad \mu_{\mathcal{S}}(\mathscr{G}/\Gamma). \tag{9.8}$$

Lorsque l'on travaille avec des groupes algébriques $G$ admissibles pour un même groupe fixé $\mathscr{G}$, alors le groupe $G_{\mathcal{S}}$ ne varie pas avec $G$, de même que la mesure $\mu_{\mathcal{S}}$ sur $G_{\mathcal{S}}$ (et sur $\mathscr{G}$). Dans cette situation l'indice $\mathcal{S}$ devient inutile, et l'on notera :

$$\mu \quad := \quad \mu_{\mathcal{S}}. \tag{9.9}$$

## §9.4 Calcul dans le cas quasi-déployé

La formule du volume de Prasad s'obtient en ramenant le calcul au cas d'un groupe quasi-déployé. Plus précisément, nous devons commencer par certains calculs dans $G'$, la forme interne quasi-déployée de $G$. Ce paragraphe sera l'occasion d'introduire plusieurs notations intervenant dans la formule de Prasad. Fixons sur $G'$ une forme de Tamagawa $\omega$. On rappelle (cf. §6.3) que pour chaque place $v \in V$ cette forme détermine une mesure de Haar $\omega_v$ sur $G'(k_v)$.

**9.6 La collection $\mathscr{P}'$.** Dans $G'$ on fixe une collection cohérente $\mathscr{P}' = (P'_v)$ de sous-groupes parahoriques de la façon suivante : si $G'$ est déployé sur $\hat{k}_v$ alors $P'_v$ est choisi hyperspécial, et pour le nombre fini de places où $G'$ n'est pas déployé sur $\hat{k}_v$, on choisit $P'_v$ comme étant spécial. De plus dans ce dernier cas, si $G$ est de type $\mathrm{A}_r$ avec rang $r$ pair, on impose que le groupe fini semi-simple $\overline{\mathcal{G}}^{\mathrm{ss}}_{P'_v}$ attaché à $P'_v$ soit de type B. La remarque 9.3 garantit qu'un tel choix pour la collection cohérente $\mathscr{P}'$ est possible. Notons que notre choix pour $\mathscr{P}'$ revient à dire que chaque $P'_v$ est de volume maximal dans $G'(k_v)$.

**9.7 Constantes $\gamma_v$ : cas archimédien.** Pour chaque $v \in V_\infty$ on choisit $c_v \in \mathbb{R}^\times$ de façon à ce que la forme différentielle $c_v\omega$ donne la mesure définie comme dans §9.4 : l'intégration de $c_v\omega$ sur la forme compacte réelle de $\mathbf{R}_{k_v|\mathbb{R}}(G')(\mathbb{R})$ donne une mesure 1. Clairement $\gamma_v := |c_v|_v$ est déterminé de façon unique.

**9.8 Constantes $\gamma_v$ : cas non archimédien.** Soit $\mathcal{G}_{P'_v}$ le schéma sur $\mathscr{O}_v$ déterminé par le sous-groupe parahorique $P'_v$ (cf. §8.7). Pour chaque $v \in V_{\mathrm{f}}$, il existe un $c_v \in k_v^\times$ (pas unique) tel que

- la forme $c_v\omega$ induit sur $\mathcal{G}_{P'_v}$ une forme extérieure définie sur $\mathscr{O}_v$ (de degré maximal et invariante) ;
- de plus la réduction de $c_v\omega$ modulo $v$ donne une forme extérieure (de degré maximal et invariante) sur $\overline{\mathcal{G}}_{P'_v}$ qui n'est pas nulle.

Pour chaque $v \in V_{\mathrm{f}}$, la valeur

$$\gamma_v \quad := \quad |c_v|_v \tag{9.10}$$

ne dépend pas d'un choix particulier de $c_v$. On peut voir que les facteurs $\gamma_v$ sont presque tous triviaux ($= 1$) [Pra89, §1].

**9.9 Le corps $\ell$.** Soit $L$ le corps de déployement de $G'$. On notera par $\ell$ une extension finie de $k$ fixée comme suit (en fonction de $G$) :

1. Si $G$ n'est pas de type ${}^6\mathrm{D}_4$, alors $\ell := L$.
2. Si $G$ est de type ${}^6\mathrm{D}_4$, alors $\ell$ est choisi comme un sous-corps $\ell \subset L$ contenant $k$ et de degré $[\ell : k] = 3$, fixé une fois pour toute. Un tel choix détermine uniquement $\ell$ à $k$-isomorphisme près.

**9.10 La constante $C(G')$.** On définit une constante $C(G')$ qui ne dépend que du type absolu de $G'$ par :

$$C(G') \quad := \quad \prod_{i=1}^{r} \frac{m_i!}{(2\pi)^{m_i+1}}, \tag{9.11}$$

où $r$ est le rang de $G'$ et $m_i$ sont des entiers appelés *exposants*, qui ne dépendent que du type de $G'$. Une explication plus détaillée sur la nature des exposants est donnée dans [Pra89, 1.5], où une liste complète pour chaque type apparaît. On donne dans le tableau 9.1 les exposants pour les types classiques. On remarque que pour le type $\mathrm{D}_r$ avec $r$ impair, l'exposant $r-1$ possède une multiplicité double. On notera plus tard $C(G) := C(G')$ lorsque l'on travaillera dans le cas non quasi-déployé.

| type de $G'$ | $m_1, \ldots, m_r$ |
|---|---|
| $\mathrm{A}_r$ | $1, 2, \ldots, r$ |
| $\mathrm{B}_r, \mathrm{C}_r$ | $1, 3, 5, \ldots, 2r-1$ |
| $\mathrm{D}_r$ | $1, 3, 5, \ldots, 2r-5, 2r-3, r-1$ |

TAB. 9.1 – Exposants des types classiques

**9.11 L'entier $\mathfrak{s}$.** Si $G'$ n'est pas déployé nous avons besoin d'une dernière constante, notée $\mathfrak{s} = \mathfrak{s}(G')$ et définie dans [Pra89, 0.4]. Pour les formes externes des types classiques on donne dans le tableau suivant la valeur de $\mathfrak{s}$ :

| type de $G'$ | $\mathfrak{s}$ |
|---|---|
| ${}^2\mathrm{A}_r$ ($r$ pair) | $r(r+3)/2$ |
| ${}^2\mathrm{A}_r$ ($r$ impair) | $(r-1)/2$ |
| ${}^2\mathrm{D}_r$ | $2r-1$ |
| ${}^3\mathrm{D}_4, {}^6\mathrm{D}_4$ | $7$ |

TAB. 9.2 – Valeur de $\mathfrak{s}$

Nous possédons à présent tous les éléments pour énoncer le théorème suivant [Pra89, theorem 1.6] :

**Théorème 9.12.** *On a l'égalité :*

$$\prod_{v \in V} \gamma_v \quad = \quad {\mathscr{D}_{\ell|k}}^{\mathfrak{s}/2} \cdot C(G')^{[k:\mathbb{Q}]}.$$

Ce produit ne dépend pas d'un choix particulier de la forme de Tamagawa $\omega$. Le facteur ${\mathscr{D}_{\ell|k}}^{\mathfrak{s}/2}$ apparaît essentiellement en lien avec les facteurs $\gamma_v$ des places finies, alors que le facteur $C(G')$ est lié au $\gamma_v$ des places archimédiennes. Dans le cas où $G'$ est déployé la partie concernant les places finies devient triviale : $\mathscr{D}_{\ell|k} = 1$. Ceci justifie le fait que nous avons renoncé à définir $\mathfrak{s}$ dans ce cas.

Pour $v \in V_{\mathrm{f}}$ les facteurs $\gamma_v$ sont essentiels pour l'obtention d'une formule de volume : la forme extérieure $c_v\omega$ qui apparaît en 9.8 est telle que le calcul du volume (par rapport à cette forme) est possible par réduction modulo $v$. On a en effet [Pra89, 2.9] :

$$\gamma_v \omega_v(P'_v) \quad = \quad \frac{\#\overline{\mathscr{M}}_v(\mathbb{F}_v)}{q_v^{\dim(\overline{\mathscr{M}}_v)}}, \tag{9.12}$$

où l'on utilise à présent la notation $\overline{\mathscr{M}}_v$ pour désigner le $\mathbb{F}_v$-groupe réductif $\overline{\mathcal{G}}^{\mathrm{red}}_{P'_v}$ défini pour chaque $P'_v$ (cf. §8.7), et où l'on désigne désormais par $q_v$ la cardinalité de $\mathbb{F}_v$ :

$$q_v \quad := \quad \#\mathbb{F}_v.$$

**Remarque 9.13.** La notation $\overline{\mathscr{M}}_v$ est reprise de [Pra89], où la forme interne quasi-déployée de $G$ est notée par $\mathscr{G}$ et le sous-groupe parahorique $P'_v$ par $\mathscr{P}_v$. Malgré notre choix de notation $G'$ pour la forme interne, nous suivons donc Prasad pour le $\mathbb{F}_v$-groupe $\overline{\mathscr{M}}_v$ associé à $P'_v$.

## §9.5 La formule du volume

Le calcul du covolume $\mu(G/\Lambda)$ d'un sous-groupe arithmétique principal $\Lambda$ va se ramener à la situation de la forme interne quasi-déployée $G'$. Pour cela on fixe un $\overline{k}$-isomorphisme

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

pour lequel $\varphi^{-1} \circ {}^{\sigma}\varphi \in \overline{G}$ pour chaque $\sigma \in \mathrm{Gal}(\overline{k}|k)$. Cet isomorphisme détermine, en prenant le pullback, une forme de Tamagawa sur $G$ :

$$\omega^* \quad := \quad \varphi^*\omega,$$

où $\omega$ est la forme de Tamagawa fixée sur $G'$. Pour chaque $v \in V$ on a ainsi une mesure $\omega_v^*$ sur $G(k_v)$ qui est étroitement liée à la mesure $\omega_v$ sur $G'(k_v)$.

Pour les places $v \in V_\infty$ on a que $\gamma_v\omega_v^*$ est (tout comme $\gamma_v\omega_v$) la mesure qui donne mesure 1 à la forme compacte réelle de $\mathbf{R}_{k_v|\mathbb{R}}(G)(\mathbb{R})$. En d'autres termes on a l'égalité (pour $v \in V_\infty$) :

$$\gamma_v\omega_v^* \quad = \quad \mu_v. \tag{9.13}$$

Soit $\mathscr{P} = (P_v)$ la collection cohérente associée au sous-groupe principal $\Lambda$. Des calculs de volume locaux dans [Pra89, §2] montrent que pour les places finies $v \in V_{\mathrm{f}}$, la mesure $\gamma_v\omega_v^*$ appliquée sur $P_v$ donne :

$$\gamma_v\omega_v^*(P_v) \quad = \quad \frac{\#\overline{\mathrm{M}}_v(\mathbb{F}_v)}{q_v^{(\dim \overline{\mathrm{M}}_v + \dim \overline{\mathscr{M}}_v)/2}}, \tag{9.14}$$

où $\overline{\mathrm{M}}_v$ est la notation qu'on utilisera dans ce contexte pour le $\mathbb{F}_v$-groupe $\overline{\mathcal{G}}^{\mathrm{red}}_{P_v}$. Comme pour $\overline{\mathscr{M}}_v$, la description de la structure $\overline{\mathrm{M}}_v$ suit de la proposition 8.22. Pour tous les cas que nous aurons à traiter dans cette thèse, le contenu de §7.9 sera alors suffisant pour obtenir l'ordre de $\overline{\mathrm{M}}_v(\mathbb{F}_v)$. Pour connaître la dimension de $\overline{\mathrm{M}}_v$ (resp. de $\overline{\mathscr{M}}_v$) on s'appuiera sur les dimensions des groupes semi-simples, qu'il vaut la peine de rappeler dans le tableau 9.3 (pour les types classiques). La notation $\overline{\mathrm{M}}_v$ est comme pour $\overline{\mathscr{M}}_v$ (cf. remarque 9.13) reprise de [Pra89].

| type de $H$ | $\dim(H)$ |
|---|---|
| $\mathrm{A}_r$ | $r(r+2)$ |
| $\mathrm{B}_r, \mathrm{C}_r$ | $r(2r+1)$ |
| $\mathrm{D}_r$ | $r(2r-1)$ |

TAB. 9.3 – Dimension de $H$ semi-simple

**Remarque 9.14.** Si $G$ est $k_v$-isomorphe à $G'$ et que $P_v$ est du même type que $P'_v$, alors on peut identifier $P_v \subset G(k_v)$ avec $P'_v \subset G'(k_v)$ et la mesure (9.14) correspond exactement au calcul donné en (9.12). Selon le théorème 9.4 et le lemme 9.2 c'est le cas pour toutes les places $v \in V_\mathrm{f}$ à l'exception d'un nombre fini d'entre elles, et on notera par $\mathrm{T} \subset V_\mathrm{f}$ l'ensemble de ces places où l'identification entre $P_v$ et $P'_v$ n'est pas permise. T contient au minimum l'ensemble des places finies $v$ pour lesquelles $G$ n'est pas $k_v$-isomorphe à $G'$.

**Remarque 9.15.** Selon [Pra89, 2.10], le quotient (9.14) est strictement inférieur à 1.

A l'aide des notations qui ont été introduites tout au long du chapitre, on peut donner la formule qui permet le calcul du covolume des sous-groupes principaux :

**Théorème 9.16** (Formule du volume de Prasad)**.** *Le covolume dans $G_\mathcal{S}$ du sous-groupe arithmétique principal $\Lambda = \Lambda_\mathscr{P}$ est donné par :*

$$\mu(G_\mathcal{S}/\Lambda) \quad = \quad \mathscr{D}_k^{\dim G/2} \left(\mathscr{D}_{\ell|k}\right)^{\mathfrak{s}/2} \cdot C(G)^{[k:\mathbb{Q}]} \cdot \mathscr{E}(\mathscr{P}),$$

*où le dernier facteur est un produit d'Euler donné par :*

$$\mathscr{E}(\mathscr{P}) \quad := \quad \prod_{v \in V_\mathrm{f}} \frac{q_v^{(\dim \overline{\mathrm{M}}_v + \dim \overline{\mathscr{M}}_v)/2}}{\#\overline{\mathrm{M}}_v(\mathbb{F}_v)} \, .$$

PREUVE. On veut calculer $\mu(G_\mathcal{S}/\Lambda)$, ce qui par le contenu de §9.3 revient à calculer $\mu_\infty(G_\infty/\Lambda)$. On remarque par (9.13) qu'on peut exprimer $\mu_\infty$ comme

$$\mu_\infty \quad = \quad \prod_{v \in V_\infty} \gamma_v \cdot \omega_\infty^* .$$

Par le lemme 6.10 appliqué sur la forme de Tamagawa $\omega^*$, on obtient ainsi :

$$\begin{aligned} \mu_\infty(G_\infty/\Lambda) \quad &= \quad \prod_{v \in V_\infty} \gamma_v \cdot \mathscr{D}_k^{\dim G/2} \cdot \prod_{v \in V_\mathrm{f}} \omega_v^*(P_v)^{-1} \\ &= \quad \mathscr{D}_k^{\dim G/2} \cdot \prod_{v \in V} \gamma_v \cdot \prod_{v \in V_\mathrm{f}} \gamma_v^{-1} \omega_v^*(P_v)^{-1}. \end{aligned}$$

La formule du théorème suit alors du théorème 9.12 et du calcul de mesure donné par (9.14). □

**Remarque 9.17.** On voit qu'avec l'utilisation dans la preuve du lemme 6.10, lequel repose sur l'approximation forte, l'hypothèse que $G$ est simplement connexe est essentielle. Il y a bien une généralisation de Gross [Gro97] de la formule pour les groupes semi-simples qui ne sont pas simplement connexes, mais la preuve y est ramenée au travail de Prasad. De plus le travail de Gross semble plus difficile à appliquer, notamment à cause de la théorie de Bruhat-Tits, où le cas non simplement connexe est moins évident.

Comme il est remarqué dans [Pra89, 3.11], la formule du théorème 9.16 prend une forme encore plus concise en exprimant le produit $\mathscr{E}(\mathscr{P})$ comme un certain produit de valeurs spéciales de fonctions $L$ et fonctions zêta. Nous allons expliquer cela dans les exemples 9.18 et 9.19 ci-dessous. Reprenons l'ensemble fini de places T de la remarque 9.14, et définissons pour chaque $v \in \mathrm{T}$ un facteur, appelé *facteur lambda*, comme suit :

$$\lambda_v \quad := \quad \frac{q_v^{(\dim \overline{\mathrm{M}}_v + \dim \overline{\mathscr{M}}_v)/2}}{\#\overline{\mathrm{M}}_v(\mathbb{F}_v)} \cdot \frac{\#\overline{\mathscr{M}}_v(\mathbb{F}_v)}{q_v^{\dim(\overline{\mathscr{M}}_v)}} \tag{9.15}$$

Ceci permet d'écrire le produit d'Euler $\mathscr{E}(\mathscr{P})$ sous la forme :

$$\mathscr{E}(\mathscr{P}) \quad = \quad \prod_{v \in \mathrm{T}} \lambda_v \cdot \prod_{v \in V_{\mathrm{f}}} \frac{q_v^{\dim(\overline{\mathscr{M}}_v)}}{\#\overline{\mathscr{M}}_v(\mathbb{F}_v)}, \tag{9.16}$$

C'est ce dernier produit infini qui pourra se ramener à des fonctions $L$ et fonctions zêta.

**Exemple 9.18.** Soit $G$ de type ${}^1\mathrm{D}_r$ pour $r \geq 3$ (avec $\mathrm{D}_3 = \mathrm{A}_3$). Pour chaque place $v \in V_{\mathrm{f}} \smallsetminus \mathrm{T}$, le groupe $G|k_v$ est quasi-déployé (car isomorphe sur $k_v$ à $G'$) et donc déployé. Il suit alors de l'exemple 8.23 que pour $v \notin \mathrm{T}$ le groupe $\overline{\mathscr{M}}_v = \overline{\mathrm{M}}_v$ est semi-simple de type ${}^1\mathrm{D}_r$. Le tableau 7.1 nous donne alors la valeur de $\#\overline{\mathscr{M}}_v(\mathbb{F}_v)$. En utilisant le fait que pour le type ${}^1\mathrm{D}_r$ on a $\dim(\overline{\mathscr{M}}_v) = 2r^2 - r$, on obtient

$$\mathscr{E}(\mathscr{P}) \quad = \quad \prod_{v \in \mathrm{T}} \lambda_v \cdot \prod_{v \in V_{\mathrm{f}}} \frac{q_v^{r^2}}{(q_v^r - 1)\prod_{j=1}^{r-1}(q_v^{2j} - 1)},$$

Or, comme pour $v = \mathfrak{p}$ le nombre $q_v$ n'est rien d'autre que $\mathcal{N}_{k|\mathbb{Q}}(\mathfrak{p})$, selon §4.7 ce dernier produit peut s'écrire sous la forme :

$$\zeta_k(r)\prod_{j=1}^{r-1}\zeta_k(2j) \quad = \quad \prod_{v \in V_{\mathrm{f}}} \frac{1}{1-(1/q_v)^r} \cdot \prod_{j=1}^{r-1}\left(\prod_{v \in V_{\mathrm{f}}} \frac{1}{1-(1/q_v)^{2j}}\right)$$

**Exemple 9.19.** Supposons à présent que $G$ soit de type ${}^2\mathrm{D}_r$, avec $r \geq 4$. Pour les places $v \in V_{\mathrm{f}} \smallsetminus \mathrm{T}$ il y a trois possibilités :

- Si $G|k_v$ est déployé sur $\hat{k}_v$ et est de type ${}^1\mathrm{D}_r$, alors $\overline{\mathscr{M}}_v$ est de type ${}^1\mathrm{D}_r$ (cf. exemple 8.23). C'est le cas lorsque $\ell$ est un sous-corps de $k_v$, ce qui correspond au cas où $v$ est décomposé dans $\ell|k$.
- Si $G|k_v$ est déployé sur $\hat{k}_v$ et est de type ${}^2\mathrm{D}_r$, alors $\overline{\mathscr{M}}_v$ est de type ${}^2\mathrm{D}_r$, comme le montre l'exemple 8.25. C'est le cas lorsque $\ell \not\subset k_v$ et $\ell \subset \hat{k}_v$, i.e. lorsque $v$ est inerte dans $\ell|k$.

– Si $G|k_v$ n'est pas déployé sur $\hat{k}_v$ : alors l'exemple 8.24 montre que $\overline{\mathscr{M}}_v$ est de type $\mathrm{B}_{r-1}$. C'est le cas pour $\ell \not\subset \hat{k}_v$, i.e. pour $v$ ramifié dans $\ell|k$.

En analysant l'ordre de $\overline{\mathscr{M}}_v(\mathbb{F}_v)$ et $\dim(\overline{\mathscr{M}}_v)$ (cf. tableaux 7.1 et 9.3) pour ces trois cas, on peut observer que le produit d'Euler $\mathscr{E}(\mathscr{P})$ prend la forme suivante :

$$\mathscr{E}(\mathscr{P}) \quad = \quad \prod_{v\in \mathrm{T}} \lambda_v \quad L_{\ell|k}(r) \prod_{j=1}^{r-1} \zeta_k(2j).$$

On montre que pour le cas ${}^2\mathrm{A}_3 = {}^2\mathrm{D}_3$ la même formule pour $\mathscr{E}(\mathscr{P})$ reste correcte.

**Remarque 9.20.** Le fait que le covolume d'un sous-groupe arithmétique $\Gamma < G_{\mathcal{S}}$ fasse intervenir un produit de valeurs spéciales de fonctions $L$ et zêta était déjà connu avant le formule de Prasad. En effet la théorie de Tamagawa suffit en quelque sorte pour calculer le covolume de $\Gamma$ à un facteur rationnel près. De tels calculs apparaissent déjà dans [Ono66]. Si l'on se place au point de vue de la théorie des nombres, connaître un volume à un facteur rationnel près est un résultat très satisfaisant. Mais sans avoir à disposition de bornes pour le facteur rationnel, le géomètre ne peut pleinement se contenter d'un pareil résultat.

**Remarque 9.21.** Il a déjà été question dans notre introduction du fait que la formule de Prasad généralise les calculs de volume de Borel [Bor81] pour $G_{\mathcal{S}}$ formé de produit des groupes d'isométries de $\mathbb{H}^2$ et $\mathbb{H}^3$. Ces calculs arithmétiques de volumes pour $\mathbb{H}^2$ et $\mathbb{H}^3$ sont présentés dans [MR03, Ch. 11].

# Chapitre 10. Sous-groupes arithmétiques maximaux

Tout au long du chapitre, $G$ désigne un $k$-groupe algébrique qui est comme dans §9.1. Un sous-groupe arithmétique $\Gamma < G_{\mathcal{S}}$ est *maximal dans* $G_{\mathcal{S}}$ s'il n'est strictement inclus dans aucun sous-groupe discret (qui serait nécessairement arithmétique) de $G_{\mathcal{S}}$. Ce court chapitre examine le problème de la maximalité, ingrédient important pour la preuve des théorèmes 1.3 et 1.4 (cf. discussion en §1.4). Une réponse complète au problème est donnée dans les travaux de Rohlfs [Roh79] [MR86]. Nous n'aurons besoin que d'une partie de la solution.

## §10.1 Maximalité dans $G(k)$

Un sous-groupe arithmétique $\Gamma < G(k)$ est dit *maximal dans* $G(k)$ s'il n'est strictement inclus dans aucun sous-groupe discret de $G(k)$. C'est une propriété plus faible que la maximalité dans $G_{\mathcal{S}}$ : un sous-groupe arithmétique de $G_{\mathcal{S}}$ n'est pas nécessairement inclus dans $G(k)$, comme le montre l'exemple suivant :

**Exemple 10.1.** Soit $G := \mathrm{SL}_2$ défini sur $k := \mathbb{Q}(\sqrt{-3})$. Dans cette situation on a $G_{\mathcal{S}} = \mathrm{SL}_2(\mathbb{C})$. L'élément

$$g \;:=\; \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

appartient à $G_{\mathcal{S}}$, mais n'est pas dans $\mathrm{SL}_2(k)$. Or si l'on ajoute le générateur $g$ au sous-groupe arithmétique $\mathrm{SL}_2(\mathscr{O}_k)$ on obtient un sous-groupe discret de $G_{\mathcal{S}}$, qu'on va noter $\Gamma$. Ceci peut se voir en utilisant le groupe adjoint $\overline{G}$. Pour un plongement matriciel bien choisi, on a $\pi(\Gamma) = \overline{G}(\mathscr{O}_k)$ (cf. 2.40), qui est donc arithmétique. $\Gamma$ est alors lui-même arithmétique dans $G_{\mathcal{S}}$, sans être inclus dans $G(k)$.

La question de la maximalité dans $G(k)$ est assez facilement réglée par le résultat suivant :

**Proposition 10.2.** *Un sous-groupe arithmétique de $G(k)$ est maximal dans $G(k)$ si et seulement s'il s'agit d'un sous-groupe arithmétique principal $\Lambda_{\mathscr{P}}$, où la collection cohérente $\mathscr{P} = (P_v)_{v \in V_f}$ est telle que chaque sous-groupe $P_v \subset G(k_v)$ est un sous-groupe parahorique maximal.*

Idée de la preuve. Soit $\Gamma$ un sous-groupe arithmétique maximal de $G(k)$. Pour chaque $v \in V_{\mathrm{f}}$ on note par $\Gamma_v$ l'adhérence de $\Gamma$ dans $G(k_v)$. On montre alors que la collection $(\Gamma_v)_v$ est cohérente (voir par exemple [RC97, Prop. 1.4 et 1.6]). Supposons qu'il existe une place $v$ telle que $\Gamma_v$ n'est pas parahorique maximal.

Soit alors $P_v \subset G(k_v)$ un sous-groupe parahorique maximal qui contient $\Gamma_v$. En remplaçant $\Gamma_v$ par $P_v$ pour cette place dans la collection cohérente, on obtient un sous-groupe arithmétique de $G(k)$ qui contient $\Gamma$, et même strictement selon la proposition 6.9. Ceci contredit la maximalité de $\Gamma$. □

Les sous-groupes parahoriques maximaux de $G(k_v)$ sont décrits à l'aide du système de Tits affine présenté en §8.1 : ce sont les sous-groupes parahoriques correspondants aux types obtenu en retirant un seul noeud au diagramme de Dynkin local $\Delta_v$. La formule de Prasad permet le calcul du covolume des sous-groupes arithmétiques maximaux de $G(k)$.

## §10.2 Maximalité dans $G_{\mathcal{S}}$

L'étude de la maximalité dans $G_{\mathcal{S}}$ est plus subtile que celle dans $G(k)$. Elle nécessite l'utilisation d'une propriété particulière du groupe adjoint $\overline{G}$ de $G$ [BP89, 1.2] :

**Lemme 10.3.** *Chaque sous-groupe arithmétique de $\overline{G}_{\mathcal{S}} = \prod_{v\in\mathcal{S}} \overline{G}(k_v)$ est contenu dans $\overline{G}(k)$.*

Une illustration de ce lemme apparaît d'ailleurs déjà dans l'exemple 10.1.

Relevons que dans le cas où le groupe simplement connexe $G$ est adjoint (i.e. pour les types $\mathrm{E}_8$, $\mathrm{F}_4$ et $\mathrm{G}_2$) ce lemme montre que la proposition 10.2 résout la question de la maximalité dans $G_{\mathcal{S}}$. Dans le cas général on a la condition nécessaire suivante pour qu'un sous-groupe arithmétique soit maximal dans $G_{\mathcal{S}}$ :

**Théorème 10.4.** *Soit $\Gamma$ un sous-groupe arithmétique maximal de $G_{\mathcal{S}}$. Alors il s'écrit sous la forme d'un normalisateur :*

$$\Gamma \quad = \quad N_{G_{\mathcal{S}}}(\Lambda),$$

*où $\Lambda$ est un sous-groupe arithmétique principal de $G(k)$.*

Idée de la preuve. On renvoie à [Roh79, 3.4] ou [BP89, 1.4] pour les détails. Soit $\pi$ l'isogénie entre $G$ et $\overline{G}$, et soit $\Gamma$ maximal dans $G_{\mathcal{S}}$. Notons par $\overline{\Gamma}_v$ l'adhérence de $\pi(\Gamma)$ dans $G(k_v)$ (comme $\pi(\Gamma) \subset G(k)$). Pour chaque $v \in V_{\mathrm{f}}$ il existe un sous-groupe compact et ouvert maximal $\overline{P}_v \subset \overline{G}(k_v)$ qui contient $\overline{\Gamma}_v$. La théorie de Bruhat-Tits montre que $\overline{P}_v$ est le stabilisateur d'un sous-groupe parahorique de $G(k_v)$ ($\overline{G}$ opère sur $G$ comme automorphismes internes). On note par $P_v$ ce sous-groupe parahorique de $G(k_v)$ que $\overline{P}_v$ stabilise. La collection $\mathscr{P} = (P_v)$ est alors cohérente. Pour $\gamma \in \Gamma$, on a par construction $\pi(\gamma) \in \overline{P}_v$ pour chaque $v \in V_{\mathrm{f}}$, i.e. $\gamma^{-1} P_v \gamma = P_v$. Ainsi $\Gamma \subset N_{G_{\mathcal{S}}}(\Lambda_{\mathscr{P}})$ ; c'est un résultat général sur les réseaux des groupes semi-simples (sans facteurs compacts) qu'un tel normalisateur reste discret [Rag72, 5.17]. Par maximalité de $\Gamma$ on a donc $\Gamma = N_{G_{\mathcal{S}}}(\Lambda_{\mathscr{P}})$. □

**Remarque 10.5.** Par définition (définitions 3.3 et 3.16) les sous-groupes $\Lambda$ et $\Gamma$ de ce théorème sont commensurables. Plus généralement, si $\Gamma$ (pas supposé maximal) est le normalisateur d'un sous-groupe arithmétique $\Lambda$ de $G_{\mathcal{S}}$, on voit grâce à (3.1) (avec le fait que $\Gamma$ reste discret selon [Rag72, 5.17], et possède donc un covolume positif) que l'indice $[\Gamma : \Lambda]$ est fini.

La question de savoir quels sont les sous-groupes principaux $\Lambda$ dont les normalisateurs sont maximaux a été résolue par J. Rohlfs, d'abord dans le cas déployé [Roh79]. Sa solution s'étend cependant sans difficulté au cas général [MR86, §2]. Signalons encore que l'article [RC97] donne une reformulation du travail de Rohlfs. Pour notre part nous nous contenterons d'une condition particulière suffisante pour la maximalité ; elle découle des travaux de Rohlfs :

**Théorème 10.6.** *Si le sous-groupe principal $\Lambda$ est maximal dans $G(k)$, alors son normalisateur $\Gamma = N_{G_{\mathcal{S}}}(\Lambda)$ est maximal dans $G_{\mathcal{S}}$.*

# Chapitre 11. Cohomologie galoisienne

Nous donnons ici quelques éléments concernant un outil classique qui apparaît lors de l'étude des groupes algébriques définis sur un corps non algébriquement clos : la *cohomologie galoisienne* [Ser02]. Dans ce chapitre nous nous plaçons d'abord dans la situation général d'un corps $K$ respectant les conventions définies en §2.1. Nous avons en vue des applications où le corps $K$ sera un corps de nombres ou un corps $\mathfrak{p}$-adique. Notre discussion a pour but de préparer le chapitre 12, et nous laisserons de côté une application essentielle de la cohomologie galoisienne, à savoir la classification des $k$-formes des groupes algébriques.

## §11.1 Ensembles de cohomologie

Soit $G$ un groupe algébrique défini sur $K$. L'opération de $\mathrm{Gal}(\overline{K}|K)$ sur $G = G(\overline{K})$ nous permet de définir une « cohomologie » de $\mathrm{Gal}(\overline{K}|K)$, pour laquelle $G$ jouera le rôle des coefficients. Pour ces donnés, l'*ensemble de cohomologie de* $\mathrm{Gal}(\overline{K}|K)$ *dans* $G$ *de dimension* 0 est simplement défini comme étant l'ensemble $G(K)$ des points $K$-rationnels de $G$, qu'on peut également caractériser comme l'ensemble des points fixes par l'action de $\mathrm{Gal}(\overline{K}|K)$ :

$$G(K) \quad = \quad G^{\mathrm{Gal}(\overline{K}|K)} \tag{11.1}$$

La notation $H^0(K, G)$, simplification de l'écriture $H^0(\mathrm{Gal}(\overline{K}|K), G)$, peut s'utiliser pour $G(K)$ (mais on préférera cette dernière notation à la fois plus succinte et plus explicite).

La définition de l'ensemble de cohomologie de dimension 1 demande plus de travail. On commence par définir un ensemble de cocycles. Une fonction de la forme

$$\begin{array}{rccc} a \quad : & \mathrm{Gal}(\overline{K}|K) & \to & G \\ & \sigma & \mapsto & a_\sigma, \end{array} \tag{11.2}$$

pour laquelle il existe une extension finie $L|K$ telle que $a_\sigma = 1$ pour tous les $\sigma \in \mathrm{Gal}(\overline{K}|L)$ est appelée *cocycle* de $\mathrm{Gal}(\overline{K}|K)$ dans $G$ si pour tous $\sigma, \tau \in \mathrm{Gal}(\overline{K}|K)$ on a :

$$a_{\sigma\tau} \quad = \quad a_\sigma \cdot {}^\sigma a_\tau, \tag{11.3}$$

où ${}^\sigma a_\tau$ désigne l'image de $a_\tau$ obtenue en laissant agir $\sigma$ sur chaque composante de $a_\tau$ (cf. 2.7). On note par $Z^1(K, G)$ l'ensemble des cocycles ainsi définis. On introduit sur $Z^1(K, G)$ la relation d'équivalence suivante : deux éléments $a$ et $a'$

de $Z^1(K,G)$ sont *cohomologues* s'il existe $b \in G$ tel que pour tout $\sigma \in \mathrm{Gal}(\overline{K}|K)$ on ait :

$$a'_\sigma = b^{-1} a_\sigma \, {}^\sigma b. \tag{11.4}$$

**Définition 11.1.** La relation de cohomologie ainsi définie sur $Z^1(K,G)$ détermine un ensemble de classe d'équivalence, appelé *ensemble de cohomologie de* $\mathrm{Gal}(\overline{K}|K)$ *dans* $G$ *de dimension* 1. On note cet ensemble par $H^1(\mathrm{Gal}(\overline{K}|K), G)$, ou plus simplement par $H^1(K,G)$. Le cocycle trivial $\sigma \mapsto 1$ ($\forall\, \sigma \in \mathrm{Gal}(\overline{K}|K)$) représente l'élément dit *trivial* de $H^1(K,G)$ et est noté par le symbole 1.

**Remarque 11.2.** Il est possible de représenter l'ensemble $H^1(K,G)$ comme une certaine limite inductive, grâce à une topologie naturelle sur $\mathrm{Gal}(\overline{K}|K)$ qui en fait en groupe profini.

Si $G = A$ est un groupe abélien, $A$ est un module sur $\mathrm{Gal}(\overline{K}|K)$ et les ensembles $H^0(K,G)$ et $H^1(K,G)$ correspondent aux groupes de cohomologies $H^q(\mathrm{Gal}(\overline{K}|K), A)$ pour $q = 0, 1$ pour le groupe profini $\mathrm{Gal}(\overline{K}|K)$ [Ser02, Ch. I §1]. En particulier dans ce cas les ensembles de cohomologie sont naturellement équipés d'une structure de groupe commutatif. On note alors souvent dans cette situation par 0 l'élément trivial de $H^1(K,G)$. Mais dans le cas général où $G$ n'est pas supposé abélien, l'ensemble $H^1(K,G)$ n'a pas de structure de groupe. De plus dans ce cas les ensembles de cohomologies de dimensions $q > 1$ ne sont habituellement pas définis.

Le calcul de la cohomologie de $\mathbf{G}_\mathrm{m}$ est donné par le fameux théorème :

**Théorème 11.3** (Théorème 90 de Hilbert)**.**

$$H^1(K, \mathbf{G}_\mathrm{m}) \quad = \quad 0.$$

## §11.2 Propriétés fonctorielles de $H^1$

Soient $A$ et $B$ deux $K$-groupes avec un $K$-homomorphisme $A \to B$ entre eux. Cet homomorphisme donne de manière évidente une application $Z^1(K,A) \to Z^1(K,B)$ qui préserve la relation de cohomologie (11.4) et induit donc une application

$$H^1(K,A) \quad \to \quad H^1(K,B), \tag{11.5}$$

qui préserve l'élément trivial.

**Exemple 11.4.** Si $A$ est un $K$-sous-groupe de $B$, l'inclusion $A \subset B$ induit une application $H^1(K,A) \to H^1(K,B)$. Cette application ne doit pas forcément être injective.

Plutôt que faire varier le groupe $G$ dans l'expression $H^1(K,G)$, on peut faire varier le corps $K$. Si $L|K$ est une extension de corps (pour laquelle on fixe une inclusion $\overline{K} \subset \overline{L}$), chaque élément $\sigma \in \mathrm{Gal}(\overline{L}|L)$ détermine par restriction sur $\overline{K}$ un élément de $\mathrm{Gal}(\overline{K}|K)$ que l'on note par le même symbole $\sigma$. A un cocycle $a \in Z^1(K,G)$ correspond donc naturellement un cocycle dans $Z^1(L,G)$, où $G$ est considéré ici par extension des scalaires comme un $L$-groupe. Là aussi l'image

de $a$ dans $Z^1(L,G)$ est notée par le même symbole. La relation de cohomologie est conservée, ce qui nous donne une application

$$H^1(K,G) \quad \to \quad H^1(L,G), \tag{11.6}$$

et celle-ci préserve l'élément trivial.

En présence d'une extension finie $L|K$ et d'un $L$-groupe $G$, on peut considérer le $K$-groupe $\mathbf{R}_{L|K}(G)$ obtenu par restriction des scalaires. La proprosition 2.29 montre alors l'existence d'une bijection canonique entre $H^0(L,G)$ et $H^0(K,\mathbf{R}_{L|K}(G))$. Ceci reste vrai pour l'ensemble de cohomologie de dimension 1 : on a une identification canonique

$$H^1(K,\mathbf{R}_{L|K}(G)) \quad = \quad H^1(L,G) \tag{11.7}$$

## §11.3 Suites exactes en cohomologie galoisienne

Comme toute théorie cohomologique, la cohomologie galoisienne associe à une suite exacte courte une suite exacte « longue ». Considérons une suite de $K$-homomorphismes

$$1 \to A \to B \to C \to 1, \tag{11.8}$$

pour des $K$-groupes $A, B$ et $C$ donnés. On définit une application

$$\delta \quad : \quad C(K) \to H^1(K,A)$$

de la façon suivante : pour $y \in C(K)$, on choisit un $x \in B$ dont l'image vaut $y$. L'exactitude de la suite (11.8) garantit l'existence d'un tel $x$, mais on rappelle (cf. exemple 2.40) que $x$ ne doit pas être dans $B(K)$. On définit alors $\delta(y)$ comme la classe du cocycle

$$\sigma \quad \mapsto \quad x^{-1} \cdot {}^{\sigma}x,$$

laquelle ne dépend pas du choix de $x$. La suite

$$1 \to A(K) \to B(K) \to C(K) \xrightarrow{\delta} H^1(K,A) \to H^1(K,B) \to H^1(K,C) \tag{11.9}$$

est alors une suite *exacte*, c'est-à-dire que l'image d'une application est égale à la fibre de l'élément trivial de l'application qui suit. Les précautions que nous prenons pour définir la notion d'exactitude dans cette situation sont nécessaires : les ensembles $H^1(K,\bullet)$ ne sont en général pas des groupes. Cependant, si $A$ est abélien, $\delta$ est bien un homomorphisme de groupes.

**Remarque 11.5.** La suite exacte (11.9) montre que l'ensemble de cohomologie de dimension 1 sert à mesurer l'ampleur du phénomène expliqué dans l'exemple 2.40. En effet, dans (11.9) l'ensemble $H^1(K,A)$ est trivial si et seulement si l'homomorphisme $B(K) \to C(K)$ est surjectif.

**Exemple 11.6.** Soit $\mathfrak{n}$ un entier et supposons le corps $K$ de caractéristique nulle. L'homomophisme $\mathbf{G}_{\mathrm{m}} \to \mathbf{G}_{\mathrm{m}}$ défini sur $K$ donné par $\pi : x \mapsto x^{\mathfrak{n}}$ donne la suite exacte :

$$1 \to \mu_{\mathfrak{n}} \to \mathbf{G}_{\mathrm{m}} \xrightarrow{\pi} \mathbf{G}_{\mathrm{m}} \to 1,$$

où $\mu_{\mathfrak{n}} < \mathbf{G}_{\mathrm{m}}$ désigne le $K$-sous-groupe fini qui annule le polynôme $x^{\mathfrak{n}} - 1$. On a donc exactitude de la suite

$$K^{\times} \xrightarrow{\pi} K^{\times} \to H^1(K, \mu_{\mathfrak{n}}) \to H^1(K, \mathbf{G}_{\mathrm{m}}),$$

ce qui par le théorème 11.3 montre qu'il y a identification naturelle entre groupes ($\mu_{\mathfrak{n}}$ est abélien) :

$$H^1(K, \mu_{\mathfrak{n}}) \quad = \quad K^{\times}/(K^{\times})^{\mathfrak{n}}.$$

**Exemple 11.7.** Par (11.7) et l'exemple précédent, on a :

$$H^1(K, \mathbf{R}_{L|K}(\mu_{\mathfrak{n}})) \quad = \quad L^{\times}/(L^{\times})^{\mathfrak{n}}.$$

On aura encore besoin d'un calcul de cohomologie pour un exemple un peu plus sophistiqué :

**Exemple 11.8.** On considère le groupe

$$\mathbf{R}^{(\mathbf{1})}_{L|K}(\mu_{\mathfrak{n}}) \quad := \quad \mathbf{R}_{L|K}(\mu_{\mathfrak{n}}) \cap \mathbf{R}^{(\mathbf{1})}_{L|K}(\mathbf{G}_{\mathrm{m}}),$$

où $\mathbf{R}^{(\mathbf{1})}_{L|K}(\mathbf{G}_{\mathrm{m}})$ à été défini dans l'exemple 7.36 comme noyau de l'application norme $N_{L|K}$. On a ainsi la suite exacte :

$$1 \to \mathbf{R}^{(\mathbf{1})}_{L|K}(\mu_{\mathfrak{n}}) \to \mathbf{R}_{L|K}(\mu_{\mathfrak{n}}) \overset{N_{L|K}}{\to} \mu_{\mathfrak{n}} \to 1.$$

Ce qui selon (11.9) et les exemples ci-dessus donne la suite exacte :

$$\begin{aligned} 1 \to \mu_{\mathfrak{n}}(K)/N_{L|K}(\mu_{\mathfrak{n}}(L)) \to H^1(K, \mathbf{R}^{(\mathbf{1})}_{L|K}(\mu_{\mathfrak{n}})) \\ \to \ker\left(L^{\times}/(L^{\times})^{\mathfrak{n}} \overset{N_{L|K}}{\to} K^{\times}/(K^{\times})^{\mathfrak{n}}\right) \to 1. \end{aligned} \tag{11.10}$$

## §11.4 Principe de Hasse

Pour comprendre les énoncés du chapitre 12, il nous faut encore exposer deux résultats importants de la cohomologie galoisienne. Le premier concerne la cohomologie des corps $\mathfrak{p}$-adiques [PR94, theorem 6.4] :

**Théorème 11.9** (Kneser)**.** *Soit $k_v$ un corps $\mathfrak{p}$-adique et soit $G$ un $k_v$-groupe semi-simple simplement connexe. Alors*

$$H^1(k_v, G) \quad = \quad 1.$$

Ainsi pour un corps de nombres $k$, la cohomologie d'un $k$-groupe $G$ simplement connexe devient triviale lorsque considérée sur les places finies. Les places infinies suffisent alors à comprendre l'ensemble $H^1(k, G)$, comme le montre le théorème suivant [PR94, theorem 6.6] :

**Théorème 11.10** (Principe de Hasse, cas simplement connexe)**.** *Soit $G$ un $k$-groupe semi-simple simplement connexe, avec $k$ un corps de nombres. L'application diagonale*

$$H^1(k,G) \quad \to \quad \prod_{v\in V_\infty} H^1(k_v,G)$$

*est alors bijective.*

L'injectivité reste vérifiée pour $G=\mathrm{SO}_f$ (qui n'est pas simplement connexe) si l'on considère toutes les places $V$ au lieu de $V_\infty$. C'est là une forme équivalente du *théorème de Hasse-Minkowski* [O'M63, 66 :4] pour les formes quadratiques ; on dit aussi que le *principe de Hasse* est valide pour les formes quadratiques. Ceci explique le nom donné au théorème 11.10. Il existe des contre-exemples pour des groupes $G$ qui ne sont pas simplement connexes [Ser02, Ch. III : 4.7]. Le lecteur intéressé peut consulter [PR94, §6.1 : page 286] pour un survol historique de la preuve du théorème 11.10, qui implique plusieurs auteurs.

## §11.5 Complétions de corps et restriction des scalaires

Le théorème 11.10 motive la question de décrire la cohomologie de $k_v$ à coefficients dans un $k$-groupe, avec $v$ une place du corps de nombres $k$. On explique ici comment comprendre cette cohomologie lorsque le $k$-groupe est défini à l'aide de la restriction des scalaires.

Nous avons vu en §6.1 que les points réels $\mathbf{R}_{k|\mathbb{Q}}(G)(\mathbb{R})$ pour un $k$-groupe $G$ se décrivent comme le produit $\prod_{v\in V_\infty} G(k_v)$. Plus généralement, si $\ell$ est une extension finie de $k$ et $v\in V(k)$, alors on a

$$\mathbf{R}_{\ell|k}(G)(k_v) \quad \cong \quad \prod_{w|v} G(\ell_w). \tag{11.11}$$

Ce dernier produit peut s'écrire comme les $\ell_v$-points de $G$ :

$$G(\ell_v) \quad = \quad \prod_{w|v} G(\ell_w),$$

où $\ell_v$ est défini par (5.2). Nous n'avons en fait uniquement défini pour des corps la notion de point rationnel d'un groupe algébrique. Or l'anneau $\ell_v$ n'en est pas nécessairement un. Cette dernière égalité peut cependant être vue comme une définition. L'isomorphisme canonique (11.11) suit de l'isomorphisme $\ell_v \cong \ell\otimes_k k_v$.

Ce qui précède (et qui décrit la situation pour la cohomologie de dimension 0) peut s'utiliser pour comprendre le cas de la cohomologie de dimension 1. Ainsi si l'on reprend l'exemple 11.7, on observe que le groupe de cohomologie $H^1(k_v,\mathbf{R}_{\ell|k}(\mu_\mathfrak{n}))$ s'identifie naturellement avec $\ell_v^\times/(\ell_v^\times)^\mathfrak{n}$. L'application $H^1(k,\mathbf{R}_{\ell|k}(\mu_\mathfrak{n}))\to H^1(k_v,\mathbf{R}_{\ell|k}(\mu_\mathfrak{n}))$ correspond à l'application

$$\ell^\times/(\ell^\times)^\mathfrak{n}\to \ell_v^\times/(\ell_v^\times)^\mathfrak{n}$$

qui est induite par le plongement diagonal $\ell\to\prod_{w|v}\ell_w$. Traitons finalement

le cas de l'exemple 11.8, i.e. avec $G = \mathbf{R}^{(\mathbf{1})}_{\ell|k}(\mu_{\mathfrak{n}})$. Le groupe de cohomologie $H^1(k_v, G)$ s'obtient en remplaçant $K$ par $k_v$ et $L$ par $\ell_v$ dans la suite exacte (11.10), la norme $N_{\ell_v|k_v} : \ell_v \to k_v$ étant donnée par le produit (dans $k_v$) :

$$N_{\ell_v|k_v} \quad = \quad \prod_{w|v} N_{\ell_w|k_v}.$$

L'homomorphisme $H^1(k, G) \to H^1(k_v, G)$ est alors décrit par le diagramme commutatif suivant (chaque ligne étant exacte, avec l'homomorphisme de gauche injectif, celui de droite surjectif) :

$$\begin{array}{ccccc}
\mu_{\mathfrak{n}}(k)/N_{\ell|k}(\mu_{\mathfrak{n}}(\ell)) & \longrightarrow & H^1(k,G) & \longrightarrow & \ker\left(\ell^\times/(\ell^\times)^{\mathfrak{n}} \overset{N_{\ell|k}}{\to} k^\times/(k^\times)^{\mathfrak{n}}\right) \\
\downarrow & & \downarrow & & \downarrow \\
\mu_{\mathfrak{n}}(k_v)/N_{\ell_v|k_v}(\mu_{\mathfrak{n}}(\ell_v)) & \longrightarrow & H^1(k_v,G) & \longrightarrow & \ker\left(\ell_v^\times/(\ell_v^\times)^{\mathfrak{n}} \overset{N_{\ell_v|k_v}}{\to} k_v^\times/(k_v^\times)^{\mathfrak{n}}\right)
\end{array}$$

FIG. 11.1 – Diagramme commutatif décrivant $H^1\left(k, \mathbf{R}^{(\mathbf{1})}_{\ell|k}(\mu_{\mathfrak{n}})\right)$

# Chapitre 12. Calcul d'indice dans le normalisateur

A la lumière du chapitre 10 nous savons que le calcul du volume d'un sous-groupe arithmétique maximal ne peut passer uniquement pas la formule de Prasad, limitée aux sous-groupes principaux. Il nous faut encore pouvoir calculer l'indice d'un sous-groupe arithmétique principal dans son normalisateur (indice qui est fini, selon la remarque 10.5). Ce problème est assez difficile en général, et il faut se contenter dans bien des cas d'une borne supérieure pour cet indice (et donc d'une borne inférieure pour le covolume). La méthode générale qui permet ces estimations a été établie dans l'article [BP89]. Elle s'appuie sur une formulation cohomologique. Notre exposition reprend les aspects importants de cette méthode, souvent dans une forme adaptée à notre situation plus particulière. Pour les preuves de plusieurs résultats nous renvoyons à [BP89, §2, §3 et §5].

## §12.1 Opération de $H^1(k_v, \mathrm{C})$ sur $\Delta_v$

On travaille dans ce chapitre avec un $k$-groupe $G$ qui suit les conventions et notations de §9.1. Suivant la matière exposée en §2.9 on identifie le groupe des automorphismes internes de $G$ avec le quotient $\overline{G} = G/\mathrm{C}$. On a donc la suite exacte :

$$1 \quad \to \quad \mathrm{C} \quad \to \quad G \quad \stackrel{\pi}{\to} \quad \overline{G} \quad \to \quad 1. \tag{12.1}$$

Pour une extension $K|k$ quelconque on obtient par (11.9) la suite exacte :

$$G(K) \quad \stackrel{\pi}{\to} \quad \overline{G}(K) \quad \stackrel{\delta}{\to} \quad H^1(K, \mathrm{C}) \quad \to \quad H^1(K, G). \tag{12.2}$$

Si $K = k_v$ est un complété $\mathfrak{p}$-adique de $k$, le théorème 11.9 réduit la suite (12.2) à l'isomorphisme :

$$\overline{G}(k_v)/\pi\left(G(k_v)\right) \quad \cong \quad H^1(k_v, \mathrm{C}). \tag{12.3}$$

Ceci montre, en reprenant les idées exposées dans §8.8, que pour chaque $v \in V_{\mathrm{f}}$ le groupe $H^1(k_v, \mathrm{C})$ opère sur le diagramme de Dynkin local $\Delta_v$ en permutant les types des sous-groupes parahoriques. On note cette opération comme un homomorphisme :

$$\xi_v \quad : \quad H^1(k_v, \mathrm{C}) \to \mathrm{Aut}(\Delta_v), \tag{12.4}$$

dont l'image est notée à l'aide du symbole $\Xi_v$.

## §12.2 Suite exacte de Rohlfs

On désigne par $\Gamma$ un sous-groupe arithmétique maximal de $G_{\mathcal{S}}$. Par le théorème 10.4, $\Gamma$ s'écrit comme normalisateur $N_{G_{\mathcal{S}}}(\Lambda)$ d'un sous-groupe arithmétique principal $\Lambda \subset G(k)$. Le calcul de l'indice $[\Gamma : \Lambda]$ repose en premier lieu sur le lemme 12.1 ci-dessous, dont l'énoncé requiert un peu de préparation.

On sait par le lemme 10.3 que la projection par $\pi$ de $\Gamma$ est contenue dans $\overline{G}(k)$. Comme $\Lambda \subset G(k)$ on obtient donc une séquence d'homomorphismes (le second venant de (12.2) avec $K = k$) :

$$\Gamma/\Lambda \quad \to \quad \overline{G}(k)/\pi(G(k)) \quad \stackrel{\delta}{\to} \quad H^1(k, \mathrm{C}),$$

dont la composition est denotée par le symbole $\partial$.

Pour $x \in H^1(k, \mathrm{C})$, on note pour chaque $v \in V_{\mathrm{f}}$ par $x_v$ l'image de $x$ dans $H^1(k_v, \mathrm{C})$ (c'est l'application donnée dans (11.6), qui est un homorphisme comme C est abélien). On considère alors l'homomorphisme $\xi$ donné par

$$\xi(x) \quad := \quad (\xi_v(x_v))_{v \in V_{\mathrm{f}}}\,, \tag{12.5}$$

pour $x \in H^1(k, \mathrm{C})$. On peut en fait facilement voir [MR86, §2] que l'image $\xi_v(x_v)$ est triviale pour presque tous les $v \in V_{\mathrm{f}}$, ce qui montre que l'image de $\xi$ est contenue dans la somme directe des $\Xi_v$ :

$$\xi \quad : \quad H^1(k, \mathrm{C}) \to \bigoplus_{v \in V_{\mathrm{f}}} \Xi_v. \tag{12.6}$$

Soit $\theta = (\theta_v)$ le type global du sous-groupe arithmétique principal $\Lambda$ (cf. paragraphe §9.2). On note par $H^1(k, \mathrm{C})_\theta$ le sous-groupe composé des éléments $x \in H^1(k, \mathrm{C})$ dont l'image par $\xi$ laissent $\theta$ invariant (i.e. $\xi_v(x_v) \cdot \theta_v = \theta_v \quad \forall\, v \in V_{\mathrm{f}}$). Contrairement à $H^1(k, \mathrm{C})$, le sous-groupe $H^1(k, \mathrm{C})_\theta$ est fini. On impose également des restrictions sur les places archimédiennes, en définissant le groupe :

$$A \quad := \quad \ker\left( H^1(k, \mathrm{C}) \to \prod_{v \in V_\infty} H^1(k_v, \mathrm{C}) \right), \tag{12.7}$$

l'homomorphisme dont on prend le noyau étant donné de façon diagonale. En intersectant avec $H^1(k, \mathrm{C})_\theta$ on obtient un sous-groupe fini $A_\theta$.

On remarque finalement que comme $\Gamma$ est maximal, il contient le centre $\mathcal{Z}$ de $G_{\mathcal{S}}$ ; et comme $\Lambda$ est principal, il contient $\mathrm{C}(k)$ (c'est le cas de chaque sous-groupe parahorique).

**Lemme 12.1.** *On a la suite exacte suivante :*

$$1 \quad \to \quad \mathcal{Z}/\mathrm{C}(k) \quad \to \quad \Gamma/\Lambda \quad \stackrel{\partial}{\to} \quad A_\theta \quad \to \quad 1.$$

Preuve. Pour le normalisateur dans $G(\overline{k})$ (plutôt que dans $G_{\mathcal{S}}$) cette suite exacte apparaît d'abord dans [Roh79] (cas déployé) et [MR86]. Ceci explique le titre de ce paragraphe. Notre énoncé est un cas particulier de la proposition donnée dans [BP89, 2.9], à la différence près que $A$ doit être remplacé par le groupe $\delta(\overline{G}(k))'$ donné par

$$\delta(\overline{G}(k))' \quad := \quad \left\{ x \in \delta(\overline{G}(k)) \;\middle|\; x_v \in (\delta_v \circ \pi)(G(k_v)),\ \forall\, v \in \mathcal{S} \right\}.$$

(Ici $\delta_v$ désigne l'application $\delta$ de la suite (12.2) qu'on obtient pour $K = k_v$.) Il s'agit donc de montrer que dans notre situation (où l'on dispose notamment de l'hypothèse selon laquelle $G$ est simplement connexe), on a bien $A = \delta(\overline{G}(k))'$.

Un élément $x \in H^1(k, \mathrm{C})$ est dans $\delta(\overline{G}(k))'$ si et seulement si les deux conditions suivantes sont respectées :

1. $x \in \delta(\overline{G}(k))$
2. $x_v \in (\delta_v \circ \pi)(G(k_v))\ \forall v \in \mathcal{S}$.

Par exactitude de la suite (12.2), la deuxième condition est clairement équivalente à dire que $x_v$ est trivial dans $H^1(k_v, \mathrm{C})$ pour chaque $v \in \mathcal{S}$. On utilise le théorème 11.10 pour réécrire la première condition. Avec ce théorème on voit que cette condition revient à dire que $x_v$ est trivial dans $H^1(k_v, G)$ pour tous les $v \in V_\infty$. Or de la condition 2 il suit déjà que $x_v = 1 \in H^1(k_v, G)$ pour les places $v \in \mathcal{S}$. Pour les places $v \in V_\infty \smallsetminus \mathcal{S}$ on sait que $G(k_v)$ est compact, ce qui implique que l'application $\pi : G(k_v) \to \overline{G}(k_v)$ est en fait surjective [PR94, §3.2 : corol. 1 et 3], et que donc l'application $H^1(k_v, \mathrm{C}) \to H^1(k_v, G)$ possède un noyau trivial. Pour ces places $v \in V_\infty \smallsetminus \mathcal{S}$ être trivial dans $H^1(k_v, G)$ équivaut donc à être trivial dans $H^1(k_v, \mathrm{C})$. Ce qui prouve que $A$ est bien égal à $\delta(\overline{G}(k))'$. □

Le calcul de $\mathcal{Z}/\mathrm{C}(k)$ suit immédiatement de la description du centre C de $G$ (qu'on donnera en §12.4). Plus compliqué sera le calcul de l'ordre de $A_\theta$ : il nécessite de savoir comment le groupe $H^1(k, \mathrm{C})$ opère sur les diagrammes de Dynkin locaux $\Delta_v$.

## §12.3 Covolume minimal et indice

Le groupe $A$ ne dépend que du groupe algébrique $G$, contrairement à son sous-groupe $A_\theta$ qui lui dépend du sous-groupe arithmétique $\Lambda$. Nous expliquons ici que lorsque le normalisateur $\Gamma$ est de covolume minimal dans la classe de commensurabilité des sous-groupes arithmétiques de $G_{\mathcal{S}}$, alors $A_\theta$ possède une forme simplifiée qui elle ne dépend que de $G$.

Notons par $A_\xi$ (resp. $H^1(k, \mathrm{C})_\xi$) le sous-groupe de $A$ (resp. de $H^1(k, \mathrm{C})$) qui opère trivialement sur chacun des $\Delta_v$, et par $\Xi_{\theta_v}$ le sous-groupe de $\Xi_v$ qui stabilise $\theta_v$. Le groupe $A_\xi$ est le noyau de l'opération de $A_\theta$ sur le produit $\prod_v \Delta_v$, et on a alors l'inégalité :

$$\#A_\theta \quad \leq \quad \#A_\xi \prod_{v \in V_{\mathrm{f}}} \#\Xi_{\theta_v}. \tag{12.8}$$

Or cette inégalité n'est pas triviale, dans le sens où le produit sur la droite est fini. Cela suit (avec le lemme 9.2) du constat suivant :

**Proposition 12.2.** *Si le type local $\theta_v \subset \Delta_v$ est spécial, alors $\Xi_{\theta_v} = 1$.*

Idée de la preuve. [1] Dans le cas où $G|k_v$ est déployé, cela suit du fait déjà observé par Iwahori et Matsumoto [IM65, 16.8] que le groupe $\Xi_v$ opère alors simplement transitivement sur l'ensemble des sommets (hyper)spéciaux. Si $G$ n'est pas déployé mais le devient sur l'extension maximale non ramifiée $\hat{k}_v$, on

[1] Cette démonstration, qui n'apparaît pas dans [BP89], nous a été communiquée par Gopal Prasad.

peut utiliser [BP89, 2.3] pour ramener le problème sur $k_v$ à la situation sur $\hat{k}_v$. Si $G$ n'est pas déployé sur $\hat{k}_v$ on conclut par une analyse au cas par cas des indices de Tits possibles [Tit79, §4]. □

Considérons la collection cohérente $(P_v)$ attachée au sous-groupe principal $\Lambda$. Les sous-groupes parahoriques $P_v$ qui sont hyperspéciaux (c'est-à-dire tous sauf un nombre fini) sont de volume maximal. On peut remplacer chaque sous-groupe parahorique $P_v \subset G(k_v)$ qui n'est pas hyperspécial par un sous-groupe parahorique $P_v^{\mathfrak{m}}$ de volume maximal, qui contient un même sous-groupe d'Iwahori que $P_v$. Cela nous donne (cf. remarque 9.3) une collection cohérente qui détermine un sous-groupe arithmétique principal $\Lambda^{\mathfrak{m}}$, dont le type global sera noté par $\theta^{\mathfrak{m}} = (\theta_v^{\mathfrak{m}})$. La proposition 8.17 montre que chaque type $\theta_v^{\mathfrak{m}}$ est spécial, et ainsi (par la proposition 12.2) :

$$A_{\theta^{\mathfrak{m}}} \quad = \quad A_\xi. \tag{12.9}$$

La formule de volume de Prasad montre que $\Lambda^{\mathfrak{m}}$ atteint le covolume minimal des sous-groupes arithmétiques principaux de $G(k)$. Son normalisateur $\Gamma^{\mathfrak{m}} := N_{G_{\mathcal{S}}}(\Lambda^{\mathfrak{m}})$ est d'après le théorème 10.6 un sous-groupe arithmétique maximal de $G_{\mathcal{S}}$.

**Proposition 12.3.** *Le sous-groupe arithmétique $\Gamma^{\mathfrak{m}}$ défini ci-haut possède un covolume inférieur ou égal à $\Gamma$.*

Preuve. Par [BP89, 3.1-3.3] on a l'inégalité :

$$\frac{[\Lambda^{\mathfrak{m}} : \Lambda^{\mathfrak{m}} \cap \Lambda]}{[\Lambda : \Lambda^{\mathfrak{m}} \cap \Lambda]} \quad \geq \quad \prod_{v \in V_{\mathrm{f}}} \#\Xi_{\theta_v}.$$

Pour une mesure de Haar $\mu$, en combinant cette inégalité avec (12.8) on obtient :

$$\begin{aligned}
\mu(G_{\mathcal{S}}/\Gamma) \quad &= \quad \frac{1}{\#(\mathcal{Z}/\mathrm{C}(k)) \cdot \#A_\theta}\, \mu(G_{\mathcal{S}}/\Lambda) \qquad \text{(lemme 12.1)} \\
&\geq \quad \frac{1}{\#(\mathcal{Z}/\mathrm{C}(k)) \cdot \#A_\theta} \left( \prod_{v \in V_{\mathrm{f}}} \#\Xi_{\theta_v} \right) \mu(G_{\mathcal{S}}/\Lambda^{\mathfrak{m}}) \\
&\geq \quad \frac{1}{\#(\mathcal{Z}/\mathrm{C}(k)) \cdot \#A_\xi}\, \mu(G_{\mathcal{S}}/\Lambda^{\mathfrak{m}})
\end{aligned}$$

Or par (12.9) cette dernière expression correspond exactement à $\mu(G_{\mathcal{S}}/\Gamma^{\mathfrak{m}})$. □

Cette proposition montre que pour l'étude du volume minimal on pourra se retreindre à l'étude des sous-groupes de la forme $\Gamma^{\mathfrak{m}}$. Le choix du groupe $\Gamma^{\mathfrak{m}}$ à partir de $\Gamma$ n'est pas unique : de différents sous-groupes parahoriques $P_v^{\mathfrak{m}}$ de volume maximal peuvent être choisis. Par contre le covolume de $\Lambda^{\mathfrak{m}}$ est bien uniquement déterminé par $\Gamma$, et même uniquement déterminé par le groupe algébrique $G$. De plus, comme $A_\xi$ ne dépend que de $G$, le covolume de $\Gamma^{\mathfrak{m}}$ ne dépend également que de $G$. N'importe quel normalisateur d'un sous-groupe principal $\Lambda$ qui possède une structure locale similaire à celle de $\Lambda^{\mathfrak{m}}$ atteint donc le covolume minimal des sous-groupes arithmétiques[2] de $G_{\mathcal{S}}$. On résume ceci dans la proposition suivante :

[2]On rappelle que par « sous-groupe arithmétique de $G_{\mathcal{S}}$ » on entend uniquement la classe de commensurabilité de $G(\mathcal{O}_k)$, et non pas tous les réseaux arithmétiques dans le groupe de Lie $G_{\mathcal{S}}$.

**Proposition 12.4.** *Soit $\Gamma < G_{\mathcal{S}}$ qui atteint le covolume minimal parmi les sous-groupes arithmétiques de $G_{\mathcal{S}}$. Alors $\Gamma = N_{G_{\mathcal{S}}}(\Lambda)$, où $\Lambda < G(k)$ est un sous-groupe arithmétique principal, associé à une collection cohérente $(P_v)$ telle que chaque sous-groupe parahorique $P_v \subset G(k_v)$ est de volume maximal. L'indice de $\Lambda$ dans $\Gamma$ se calcule par*

$$[\Gamma : \Lambda] \quad = \quad \#(\mathcal{Z}/\mathrm{C}(k)) \cdot \#A_{\xi}.$$

## §12.4 Description du centre

Nous avons besoin de décrire le centre C du groupe $G$, non seulement pour calculer $\mathcal{Z}/\mathrm{C}(k)$, mais surtout pour comprendre l'opération de $H^1(k, \mathrm{C})$ (et donc l'opération de $A$) sur chaque $\Delta_v$. Par la proposition 7.54 nous savons que le centre ne dépend que de la forme interne quasi-déployée. La description par type que nous donnons ci-dessous couvre ainsi tous les cas.

Si $G$ est de type $\mathrm{E}_8$, $\mathrm{F}_4$ ou $\mathrm{G}_2$ alors le centre de $G$ est trivial ; en d'autres termes $G$ est adjoint. On sait alors que dans cette situation les sous-groupes arithmétiques maximaux sont précisément les sous-groupes principaux maximaux, et la question de l'indice ne se pose pas.

Pour les cas non triviaux nous allons commencer par les types internes : pour ceux-ci le centre est particulièrment simple. En effet, si $G$ est une forme interne de la forme déployée, alors dans tous les cas le centre est donné par

$$\mathrm{C} \quad \cong \quad (\mu_{\mathfrak{n}})^{\varepsilon}, \tag{12.10}$$

où les entiers $\mathfrak{n}$ et $\varepsilon$ sont donnés pour chaque type dans le tableau suivant :

| type de $G$ | $\mathfrak{n}$ | $\varepsilon$ |
|---|---|---|
| $\mathrm{A}_r$ | $r+1$ | 1 |
| $\mathrm{B}_r, \mathrm{C}_r, \mathrm{E}_7$ | 2 | 1 |
| $\mathrm{D}_r$ ($r$ pair) | 2 | 2 |
| $\mathrm{D}_r$ ($r$ impair) | 4 | 1 |
| $\mathrm{E}_6$ | 3 | 1 |

TAB. 12.1 – Entiers $\mathfrak{n}$ et $\varepsilon$

Il nous reste à décrire le centre des formes externes, i.e. pour les types ${}^2\mathrm{A}_r$, ${}^2\mathrm{D}_r$, ${}^3\mathrm{D}_4$, ${}^6\mathrm{D}_4$ et ${}^2\mathrm{E}_6$. On reprend pour cela les entiers $\mathfrak{n}$ et $\varepsilon$ du tableau 12.1. Nous avons également besoin de l'extension de corps $\ell|k$ définie en 9.9 (on observe notamment qu'à part pour le type ${}^6\mathrm{D}_4$, le groupe $G|\ell$ devient une forme interne, et C doit être $\ell$-isomorphe à $(\mu_{\mathfrak{n}})^{\varepsilon}$). Alors, à l'exception du type ${}^2\mathrm{D}_r$ avec $r$ pair, le centre d'une forme externe (simplement connexe) est donné par (y compris pour les types ${}^{3,6}\mathrm{D}_4$) :

$$\mathrm{C} \quad = \quad \mathbf{R}^{(\mathbf{1})}_{\ell|k}(\mu_{\mathfrak{n}}). \tag{12.11}$$

Le centre d'un groupe $G$ de type ${}^2\mathrm{D}_r$ dont le rang $r$ est pair est lui donné par :

$$\mathrm{C} \quad = \quad \mathbf{R}_{\ell|k}(\mu_2). \tag{12.12}$$

## §12.5 Calcul du noyau de $\xi$

On présente ici les idées qui permettent de s'attaquer au délicat problème du calcul de l'ordre de $A_\xi$ (ou plus généralement de $H^1(k,\mathrm{C})_\xi$). Rappelons d'abord pour cela les calculs de cohomologie pour C que donnent les exemples vu en §11.3. On va souvent noter $r = 2m+1$ ou $r = 2m$ pour différencier un rang pair ou impair. On a les descriptions suivantes pour $H^1(k,\mathrm{C})$ :

- pour $G$ de type interne, sauf ${}^1\mathrm{D}_{2m}$ : $k^\times/(k^\times)^{\mathfrak{n}}$ ;
- pour $G$ de type ${}^1\mathrm{D}_{2m}$ : $\left(k^\times/(k^\times)^2\right)^2$ ;
- pour $G$ de type ${}^2\mathrm{D}_{2m}$ : $\ell^\times/(\ell^\times)^2$ ;
- dans le reste des cas, on a la suite exacte :

$$1 \quad \to \quad \mu_{\mathfrak{n}}(k)/N_{\ell|k}(\mu_{\mathfrak{n}}(\ell)) \quad \to \quad H^1(k,\mathrm{C}) \quad \to \quad \mathbf{L}/(\ell^\times)^{\mathfrak{n}} \quad \to \quad 1,$$

où $\mathbf{L} = \left\{x \in \ell^\times | N_{\ell|k}(x) \in (k^\times)^{\mathfrak{n}}\right\}$.

Afin d'unifier la discussion nous allons exclure le deuxième cas de cette liste (nous n'en aurons du reste pas besoin aux chapitres 13 à 15). Nous pouvons en effet pour les cas restants toujours parler de l'image de $H^1(k,\mathrm{C})$ dans $\ell^\times/(\ell^\times)^{\mathfrak{n}}$ (où pour les formes internes on a $\ell = k$). En posant $\mathbf{L} := \ell^\times$ dans les cas des formes internes et pour le type ${}^2\mathrm{D}_{2m}$, on a la notation unifiée $\mathbf{L}/(\ell^\times)^{\mathfrak{n}}$ pour cette image de $H^1(k,\mathrm{C})$ dans $\ell^\times/(\ell^\times)^{\mathfrak{n}}$. Comme nous porterons notre attention sur le sous-groupe $A$ de $H^1(k,\mathrm{C})$, nous définissons encore $\mathbf{A} < \mathbf{L}$ comme le sous-groupe maximal de $\ell^\times$ pour lequel l'image de $A$ dans $\ell^\times/(\ell^\times)^{\mathfrak{n}}$ vaut $\mathbf{A}/(\ell^\times)^{\mathfrak{n}}$.

**12.5 « Mauvaises places ».** On considère $\mathscr{R}$ l'ensemble des places finies $v$ où $G|\hat{k}_v$ n'est pas déployé et on définit $\hat{\mathrm{T}}$ comme l'ensemble des places finies $v \notin \mathscr{R}$ où $G|k_v$ n'est pas quasi-déployé. On notera par M la réunion disjointe $\hat{\mathrm{T}} \cup \mathscr{R}$. Nous avons déjà vu que M est un ensemble fini (théorème 9.4 et proposition 9.5).

**Remarque 12.6.** Pour $G$ qui n'est pas de type ${}^6\mathrm{D}_4$, la proposition 9.5 affirme que $\mathscr{R}$ correspond à l'ensemble des places $v \in V_\mathrm{f}$ qui ne sont pas ramifiées dans $\ell|k$ (comme $\ell = L$ dans ce cas, cf. 9.9). En fait cela reste vrai pour le type ${}^6\mathrm{D}_4$ : on peut voir que dans ce cas $v$ est ramifiée dans $L|k$ si est seulement si $v$ est ramifiée dans $\ell|k$ (cf. [Pra89, page 98]).

En dehors de cet ensemble fini de places M, le lemme suivant (qui découle de [BP89, 2.3, 2.7 et 5.3]) permet d'expliciter le noyau de l'opération de $H^1(k,\mathrm{C})$ sur $\Delta_v$. On rappelle que pour une place finie $w$ d'un corps de nombres, $\tilde{w}$ désigne sa valuation normalisée associée (cf. §5.3).

**Lemme 12.7.** *Soit une place finie $v \notin \mathrm{M}$. Un élément de $H^1(k,\mathrm{C})$ opère trivialement sur $\Delta_v$ exactement lorsque son image dans $\mathbf{L}/(\ell^\times)^{\mathfrak{n}}$ est représentée par un élément $x \in \mathbf{L}$ tel que $\tilde{w}(x) \in \mathfrak{n}\mathbb{Z}$ $\forall\, w|v$.*

Dans la situation idéale où $\mathrm{M} = \emptyset$, on peut ainsi décrire $H^1(k,\mathrm{C})_\xi$ comme une éventuelle extension (par un sous-groupe de $\mu_{\mathfrak{n}}(k)/N_{\ell|k}(\mu_{\mathfrak{n}}(\ell))$ ) du groupe $\mathbf{L}_{\mathfrak{n}}/(\ell^\times)^{\mathfrak{n}}$, avec $\mathbf{L}_{\mathfrak{n}} := \mathbf{L} \cap \ell_{\mathfrak{n}}$ et ce dernier groupe est défini par

$$\ell_{\mathfrak{n}} \quad := \quad \left\{ x \in \ell^\times \;\middle|\; \tilde{w}(x) \in \mathfrak{n}\mathbb{Z} \quad \forall\, w \in V_\mathrm{f}(\ell) \right\}$$

De même la description de $A_\xi$ dans cette situation idéale passe par la considération du groupe $\mathbf{A}_{\mathfrak{n}} := \mathbf{A} \cap \ell_{\mathfrak{n}}$.

Si M n'est pas vide on va également ramener le calcul de l'ordre de $A_\xi$ au problème du calcul de $\mathbf{A}_\mathfrak{n}/(\ell^\times)^\mathfrak{n}$. Pour cela définissons le groupe $A_{\xi,\mathrm{M}}$ comme le noyau de l'application

$$\xi_\mathrm{M} \quad : \quad A \to \bigoplus_{v\in V_\mathrm{f}\setminus \mathrm{M}} \Xi_v,$$

définie de façon similaire à $\xi$, mais sans considérer les places dans M. On définit le sous-groupe de $\ell^\times$ suivant :

$$\mathbf{A}_\mathfrak{n}^\mathrm{M} \quad := \quad \{x\in\mathbf{A} \mid \tilde{w}(x)\in\mathfrak{n}\mathbb{Z} \quad \forall\, w|v \text{ et } v\in V_\mathrm{f}\smallsetminus \mathrm{M}\} \tag{12.13}$$

Selon le lemme 12.7 l'image de $A_{\xi,\mathrm{M}}$ dans $\mathbf{A}/(\ell^\times)^\mathfrak{n}$ est égale à $\mathbf{A}_\mathfrak{n}^\mathrm{M}/(\ell^\times)^\mathfrak{n}$. Nous pouvons alors décrire la situation par le schéma suivant :

$$\begin{array}{ccc} A_{\xi,\mathrm{M}} & \xrightarrow{\bar{q}} & \mathbf{A}_\mathfrak{n}^\mathrm{M}/(\ell^\times)^\mathfrak{n} \\ {\scriptstyle q'}\uparrow & & \uparrow{\scriptstyle q} \\ A_\xi & & \mathbf{A}_\mathfrak{n}/(\ell^\times)^\mathfrak{n} \end{array}$$

où $q$ et $q'$ représentent les indices des inclusions verticales, et $\bar{q}$ est l'ordre du noyau de la surjection horizontale.

**12.8 Calcul de $\bar{q}$.** Si $\ell = k$ (i.e. $G$ est une forme interne) ou si $G$ est de type ${}^2\mathrm{D}_{2m}$ alors $A\cong\mathbf{A}/(\ell^\times)^\mathfrak{n}$ et dans ce cas on a trivialement $\bar{q}=1$. Pour les autres cas, $H^1(k,\mathrm{C})$ est une extension de $\mathbf{L}/(\ell^\times)^\mathfrak{n}$ par $\mu_\mathfrak{n}(k)/N_{\ell|k}(\mu_\mathfrak{n}(\ell))$. Si $G$ est une forme trialitaire, $\mathfrak{n}=2$ et $[\ell:k]=3$ et on calcule facilement avec ça que ce dernier groupe quotient est trivial. Donc $\bar{q}=1$ dans ce cas également. Pour le reste des cas, l'orde de $\mu_\mathfrak{n}(k)/N_{\ell|k}(\mu_\mathfrak{n}(\ell))$ (qui vaut en fait toujours 2) peut servir de borne pour $\bar{q}$, mais n'est en général pas la valeur exacte de $\bar{q}$. On doit en effet se restreindre à $A$ (et non tout $H^1(k,\mathrm{C})$), ce qui implique d'utiliser la relation (12.7) à l'aide du diagramme de la figure 11.1 pour calculer $\bar{q}$ avec précision.

**12.9 Borne pour $q'$.** Le groupe $A_{\xi,\mathrm{M}}$ opère sur $\prod_{v\in\mathrm{M}}\Delta_v$ avec noyau $A_\xi$. On a donc la borne :

$$q' \quad \le \quad \prod_{v\in\mathrm{M}} \#\Xi_v$$

**12.10 Borne pour $q$.** Notons par $\mathrm{M}_\ell$ (resp. $\hat{\mathrm{T}}_\ell$, resp. $\mathscr{R}_\ell$) l'ensemble des places de $\ell$ qui sont au-dessus de M (resp. de $\hat{\mathrm{T}}$, resp. de $\mathscr{R}$). On a $\mathrm{M}_\ell = \hat{\mathrm{T}}_\ell\cup\mathscr{R}_\ell$ et clairement $\#\mathrm{M}_\ell \le [\ell:k]\cdot\#\mathrm{M}$. On fait encore remarquer que si $\ell|k$ est quadratique, alors $\mathscr{R}_\ell$ est en bijection avec $\mathscr{R}$, ce qui améliore cette dernière borne. L'application produit (cartésien) des valeurs absolues normalisées :

$$\prod_{w\in\mathrm{M}_\ell}\tilde{w} \quad : \quad \mathbf{A} \quad \to \quad \mathbb{Z}^{\#\mathrm{M}_\ell} \tag{12.14}$$

induit un homomorphisme de $\mathbf{A}_{\mathfrak{n}}^{\mathrm{M}}/(\ell^{\times})^{\mathfrak{n}}$ vers $(\mathbb{Z}/\mathfrak{n}\mathbb{Z})^{\#\mathrm{M}_{\ell}}$ dont le noyau est $\mathbf{A}_{\mathfrak{n}}/(\ell^{\times})^{\mathfrak{n}}$. Cette application n'est pas surjective en général. En fait dans le cas où $\mathbf{L} = \left\{x \in \ell^{\times} | N_{\ell|k}(x) \in (k^{\times})^{\mathfrak{n}}\right\}$, la relation

$$\tilde{v}(N_{\ell|k}(x)) \quad = \quad \sum_{w|v} [\mathbb{F}_w : \mathbb{F}_v]\ \tilde{w}(x)$$

permet de borner l'ordre de l'image de (12.14) (cette dernière égalité est la version additive du cas général de (5.10)). Pour un tel $\mathbf{L}$, si l'on suppose en plus que $G$ n'est pas de type trialitaire, cela permet de voir qu'on a la borne :

$$q \quad \leq \quad \mathfrak{n}^{\#\hat{\mathrm{T}}} \tag{12.15}$$

Cette borne reste valable pour les cas où $\ell = k$ (à l'exception du type ${}^1\mathrm{D}_{2m}$ qu'on a exclu). Pour $G$ une forme externe de type $\mathrm{D}_{2m}$ (y compris le cas des formes trialitaires), on a la borne :

$$q \quad \leq \quad 2^{\#\mathscr{R}} 4^{\#\hat{\mathrm{T}}} \tag{12.16}$$

On renvoie le lecteur à [BP89, §5] pour les détails qui concernent ces deux bornes pour $q$.

## §12.6 Calcul de l'ordre de $\mathbf{A}_{\mathfrak{n}}/(\ell^{\times})^{\mathfrak{n}}$

Pour calculer l'ordre du groupe $\mathbf{A}_{\mathfrak{n}}/(\ell^{\times})^{\mathfrak{n}}$, on généralise quelque peu l'argumentation utilisée dans la preuve de [BP89, prop. 0.12].

Pour $U_{\ell}$ le groupe des unités entières de $\ell$, on note par $U_{\mathbf{A}}$ son sous-groupe $\mathbf{A} \cap U_{\ell}$. Notons encore par $\mathcal{P}_{\mathbf{A}}$ le groupe des idéaux fractionnaires principaux qui possèdent un représentant dans $\mathbf{A}$. De même que $\mathbf{A}$ contient $(\ell^{\times})^{\mathfrak{n}}$, on a également l'inclusion $U_{\ell}^{\mathfrak{n}} \subset U_{\mathbf{A}}$. On montre facilement l'existence de la suite exacte suivante :

$$1 \to U_{\mathbf{A}}/U_{\ell}^{\mathfrak{n}} \to \mathbf{A}/(\ell^{\times})^{\mathfrak{n}} \to \mathcal{P}_{\mathbf{A}}/\mathcal{P}_{\ell}^{\mathfrak{n}} \to 1.$$

On a clairement $U_{\mathbf{A}} \subset \mathbf{A}_{\mathfrak{n}}$. On peut remplacer $\mathbf{A}$ par $\mathbf{A}_{\mathfrak{n}}$ dans cette suite sans en changer le début. Décrivons alors l'image de $\ell_{\mathfrak{n}}$ dans $\mathcal{P}_{\ell}$ : $(x) \in \mathcal{P}_{\ell}$ est l'image d'un élément de $\ell_{\mathfrak{n}}$ si et seulement si $(x) = \mathfrak{a}^{\mathfrak{n}}$ pour un idéal fractionnaire $\mathfrak{a} \in \mathcal{J}_{\ell}$. On obtient de la sorte une nouvelle suite exacte :

$$1 \to U_{\mathbf{A}}/U_{\ell}^{\mathfrak{n}} \to \mathbf{A}_{\mathfrak{n}}/(\ell^{\times})^{\mathfrak{n}} \to (\mathcal{P}_{\mathbf{A}} \cap \mathcal{J}_{\ell}^{\mathfrak{n}})/\mathcal{P}_{\ell}^{\mathfrak{n}} \to 1. \tag{12.17}$$

Pour un élément $(x) = \mathfrak{a}^{\mathfrak{n}} \in \mathcal{P}_{\ell} \cap \mathcal{J}_{\ell}^{\mathfrak{n}}$ le corollaire 4.3 montre que l'idéal $\mathfrak{a} \in \mathcal{J}_{\ell}^{\mathfrak{n}}$ est déterminé de façon unique par $(x)$. On considère alors l'application :

$$\begin{array}{rcl} \mathcal{P}_{\mathbf{A}} \cap \mathcal{J}_{\ell}^{\mathfrak{n}} & \to & \mathscr{C}_{\ell} \\ (x) = \mathfrak{a}^{\mathfrak{n}} & \mapsto & \mathfrak{a}\mathcal{P}_{\ell}. \end{array}$$

On observe que son noyau vaut $\mathcal{P}_{\ell}^{\mathfrak{n}}$, et on notera par $\mathscr{C}_{\mathbf{A}}$ son image dans le groupe des classes $\mathscr{C}_{\ell}$. La suite exacte (12.17) devient alors :

$$1 \to U_{\mathbf{A}}/U_{\ell}^{\mathfrak{n}} \to \mathbf{A}_{\mathfrak{n}}/(\ell^{\times})^{\mathfrak{n}} \to \mathscr{C}_{\mathbf{A}} \to 1. \tag{12.18}$$

En particulier on a la borne suivante :

$$\#\mathbf{A}_{\mathfrak{n}}/(\ell^{\times})^{\mathfrak{n}} \quad \leq \quad h_{\ell} \cdot \#U_{\mathbf{A}}/U_{\ell}^{\mathfrak{n}}. \tag{12.19}$$

# Chapitre 13. Réseaux arithmétiques hyperboliques

Ce chapitre a pour but d'appliquer la théorie présentée jusqu'à présent sur le cas de la géométrie hyperbolique. On travaille avec les espaces hyperboliques $\mathbb{H}^n$ pour $n \geq 4$, et dans l'optique du traitement des résultats discutés en §1.4, on va se restreindre assez tôt au cas des dimensions $n$ impaires.

## §13.1 Groupes admissibles pour $\mathrm{Isom}^+(\mathbb{H}^n)$

Le groupe $\mathrm{Isom}(\mathbb{H}^n)$ des isométries hyperboliques s'identifie avec le groupe $\mathrm{PO}(n,1)$ des transformations projectives qui conservent la forme quadratique réelle de signature $(n,1)$. Son sous-groupe $\mathrm{Isom}^+(\mathbb{H}^n)$ des transformations qui préservent l'orientation s'identifie alors avec la composante connexe $\mathrm{PO}(n,1)^\circ$. Ce dernier groupe est isomorphe à $\mathscr{G} := \mathrm{SO}(n,1)^\circ$, et c'est avec cette dernière représentation de $\mathrm{Isom}^+(\mathbb{H}^n)$ que nous allons travailler.

Dès maintenant $G$ désignera toujours un $k$-groupe algébrique simplement connexe admissible pour $\mathscr{G} = \mathrm{SO}(n,1)^\circ$ (cf. définition 3.17), et on reprend des chapitres précédents les notations standard qui accompagnent $G$. L'exemple 7.23 avec la proposition 7.31 nous donne le type du groupe de Lie $\mathscr{G}$ en fonction de la dimension[1] : $\mathrm{B}_r$ pour $n = 2r \geq 4$ et $\mathrm{D}_r$ pour $n = 2r-1 \geq 5$ . Comme ces types sont irréductibles, on voit que le type de $\mathscr{G}$ correspond au type de $G$ et que $\mathcal{S}$ ne contient qu'un seul élément, nécessairement réel. On notera par $v_0$ cette unique place de $\mathcal{S}$, et on supposera (sans restriction) qu'elle correspond au plongement $k \to \mathbb{R}$ donné par l'identité. Les deux notations $G(\mathbb{R})$ ou $G_{\mathcal{S}}$ sont alors équivalentes. Comme les places dans $\mathcal{S} \smallsetminus \{v_0\}$ sont nécessairement réelles, le corps $k$ doit être totalement réel. La proposition 7.32 permet d'affirmer que $G|k_{v_0}$ est isomorphe au $\mathbb{R}$-groupe $\mathrm{Spin}_{n,1}$. Pour les places archimédiennes $v \neq v_0$ le groupe $G|k_v$ correspond à la forme compacte réelle $G_{\mathrm{u}} = \mathrm{Spin}_{n+1}$.

**Remarque 13.1.** Pour $n = 3$ le groupe $\mathscr{G}$ est de type $\mathrm{A}_1 \times \mathrm{A}_1$ avec un rang réel de 1, ce qui impose au groupe admissible $G$ d'être une $k$-forme de $\mathrm{SL}_2$, avec $k$ qui possède exactement une place complexe $v_0$. Les $k$-formes de $\mathrm{SL}_2$ se construisent comme certains sous-groupes multiplicatifs dans des algèbres de quaternions. C'est effectivement le point de vue usuel pour traiter les réseaux arithmétiques de $\mathrm{Isom}^+(\mathbb{H}^3)$. Ce sujet est largement couvert dans la littérature, e.g. dans [MR03]. La distinction entre le cas $n = 3$ et $n > 3$ peut donc se comprendre par le choix fait en §3.3 de travailler avec des groupes algébriques qui sont absolument simples.

[1] L'entier $n$ désignera maintenant exclusivement la dimension de l'espace hyperbolique considéré. L'espace quadratique de signature $(n,1)$ associé est de dimension $n+1$.

La proposition 3.20 montre clairement que si $k \neq \mathbb{Q}$, alors les sous-groupes arithmétiques de $G_{\mathcal{S}} = G(\mathbb{R})$ sont cocompacts. On peut en fait montrer que l'inverse est également correct, ce qui nous permettra dans la suite d'identifier le cas cocompact avec la situation $k \neq \mathbb{Q}$ :

**Proposition 13.2.** *Soit $G$ un $k$-groupe admissible pour $\mathscr{G} = \mathrm{Isom}^+(\mathbb{H}^n)$ (avec $n \geq 4$), tel que $G(\mathscr{O}_k)$ n'est pas cocompact. Alors $k = \mathbb{Q}$.*

Le résultat est détaillé dans [LM93, §1 et §2]. Il se base sur une classification des groupes algébriques de types $\mathrm{B}_r$ et $\mathrm{D}_r$, laquelle suit de [Tit66].

**13.3 Classification des groupes admissibles.** Nous décrivons ici brièvement la classification dont il est question ci-haut. Chaque groupe simplement connexe de type $\mathrm{B}_r$ s'obtient comme groupe $\mathrm{Spin}_f$ pour une forme quadratique $f$ de dimension $2r+1$. Les groupes de la forme $\mathrm{Spin}_f$ avec $f$ de dimension $2r$ sont de types $\mathrm{D}_r$. Mais ce ne sont pas les seuls : il est possible de créer des groupes de type $\mathrm{D}_r$ à partir de formes hermitiennes plutôt que quadratiques. Pour le type $\mathrm{D}_4$ il existe encore une construction basée sur des algèbres de Cayley qui donne des formes trialitaires ${}^3\mathrm{D}_4$ et ${}^6\mathrm{D}_4$. Chacune de ces familles permet effectivement de construire des réseaux hyperboliques. La construction la plus évidente (la seule dont nous aurons besoin) est celle qui apparaît essentiellement dans les exemples 3.10 et 3.15 : si $f$ est une forme quadratique définie sur un corps de nombres $k$ totalement réel, et que :

- $f$ est de signature $(n,1)$ sur une place archimédienne $v_0$ ;
- $f$ est de signature $(n+1,0)$ sur les places dans $V_\infty \smallsetminus \{v_0\}$,

alors $\mathrm{Spin}_f$ est admissible pour $\mathscr{G}$. En particulier pour $n$ pair cette construction est à la base de tous les réseaux arithmétiques de $\mathrm{Isom}(\mathbb{H}^n)$. Pour $n$ impair cette construction avec $k = \mathbb{Q}$ donne tous les réseaux de $\mathcal{AQ}^n_{\mathbf{nc}}$. En particulier les formes trialitaires ne permettent pas la construction de réseaux hyperboliques non cocompacts : celles-ci ne peuvent s'obtenir à partir de formes quadratiques. Cela suit par exemple de la discussion en §14.1.

**Remarque 13.4.** Si la preuve de la proposition 13.2 est effectivement basée (tout au moins dans [LM93]) sur une description explicite des constructions des réseaux arithmétiques hyperboliques, il ne nous sera pas nécessaire au chapitre 15 de connaître la classification 13.3 (une fois 13.2 admis). La connaissance de la structure des groupes admissibles, sans une description concrète de chacun de ceux-ci, suffira en effet pour la preuve des théorèmes 1.3 et 1.4, qui examinera bien tous les cas de réseaux arithmétiques hyperboliques.

**Remarque 13.5.** On s'attend clairement à ce que la question du volume des quotients orientables arithmétiques de $\mathbb{H}^n$ soit plus délicate pour $n$ impair que pour $n$ pair (traité dans [Bel04]). Deux aspects interviennent ici. D'une part il existe pour le type $\mathrm{D}_r$ des formes externes (et même trialitaires pour $r = 4$). Nous verrons plus bas (proposition 13.6) que dans la plupart des cas les groupes admissibles pour $\mathrm{Isom}^+(\mathbb{H}^n)$ (avec $n$ impair) sont de type externe. La formule de volume des sous-groupes arithmétiques est dans cette situation plus élaborée, avec le rôle joué par l'extension $\ell|k$. D'autre part le centre C d'un groupe algébrique simplement connexe de type $\mathrm{D}_r$ (et a fortiori pour un type externe) est plus compliqué que le centre dans le cas du type $\mathrm{B}_r$. Or le problème du calcul de l'indice d'un sous-groupe principal dans son normalisateur passe

par des calculs impliquant $H^1(k, \mathrm{C})$, qui seront plus difficiles à maîtriser pour les dimensions impaires.

Nous nous restreignons dès maintenant au cas des dimensions $n \geq 5$ impaires. Cette restriction sera admise dans tout le reste de cette thèse. Le centre C du groupe admissible $G$ diffère selon la parité du rang $r = (n+1)/2$ (cf. §12.4). On aura souvent besoin de distinguer le cas $r$ pair du cas $r$ impair. On utilisera les notations $r = 2m$ et $r = 2m+1$ pour faire cette distinction.

Le fait que le groupe $G$ soit admissible pour $\mathscr{G}$ permet de montrer qu'il doit respecter certaines conditions plutôt évidentes, qui le distingue d'un groupe de type $\mathrm{D}_r$ quelconque. Voici un premier résultat :

**Proposition 13.6.** *Soit $G$ un $k$-groupe admissible pour $\mathrm{Isom}^+(\mathbb{H}^n)$, avec $n \geq 5$ impair. Si $k \neq \mathbb{Q}$, alors $G$ doit être une forme externe (i.e de type ${}^2\mathrm{D}_r$ ou ${}^{3,6}\mathrm{D}_4$). Si $k = \mathbb{Q}$ alors $G$ est de l'un des types suivants : ${}^1\mathrm{D}_{2m+1}$, ${}^2\mathrm{D}_{2m+1}$ ou ${}^2\mathrm{D}_{2m}$.*

Preuve. L'exemple 7.52, associé à la discussion en §14.1, affirme que $\mathrm{Spin}_{(n,1)}$ est une forme interne (sur $\mathbb{R}$) exactement lorsque $(-1)^r = -1$, c'est-à-dire lorsque $r = 2m+1$. Cela empêche $G$ d'être de type ${}^1\mathrm{D}_{2m}$ (si $G$ est externe sur $k_v$, alors $G$ doit déjà être une forme externe sur $k$). La forme compacte $\mathrm{Spin}_{n+1}$ est elle externe lorsque $r = 2m+1$. Donc pour $k \neq \mathbb{Q}$ et $r = 2m+1$ le type doit aussi être externe. Comme nous l'avons mentionné au point 13.3, les formes trialitaires admissibles n'apparaissent pas pour $k = \mathbb{Q}$. □

## §13.2 Notations et conditions pour $\ell$

On voit par la proposition 13.6 que dans la plupart des cas il faudra compter sur une extension $\ell|k$ non triviale (cf. 9.9 pour la définition de $\ell$). On peut donner des conditions nécessaires que $\ell$ doit respecter pour que $G$ soit admissible. Nous commençons par fixer une notation pour les places archimédiennes de $k$ et $\ell$.

Nous noterons par $v_i$ $(i = 0, \ldots, d-1)$ les places réelles de $k$, où $d$ désigne donc désormais le degré $[k : \mathbb{Q}]$. On rappelle que selon notre choix fait en §13.1 $v_0$ correspond au plongement identité $k \subset \mathbb{R}$, et que $\mathcal{S} = \{v_0\}$. Pour les notations qu'on introduit maintenant on suppose que $[\ell : k] = 2$. Pour $v_i \in V_\infty(k)$ fixé il y a alors deux possibilités. Soit il existe deux places (réelles) de $V_\infty(\ell)$ qui divise $v_i$ ; ou alors il existe une seule place (complexe) qui divise $v_i$. Dans le premier cas de figure on note par $\sigma_i$ et $\sigma_i'$ les deux plongements $\ell \to \mathbb{R}$ qui correspondent aux places ; dans le deuxième cas on note par $\sigma_i : \ell \to \mathbb{C}$ un plongement complexe (uniquement déterminé à conjugaison près). Ces plongements indexent donc les places archimédiennes de $\ell$. Si $\sigma_i$ est réel, alors $\ell_{v_i} = \mathbb{R} \oplus \mathbb{R}$ où $\ell$ est inclus dans $\mathbb{R} \oplus \mathbb{R}$ grâce à l'application $\sigma_i \times \sigma_i'$. Si $\sigma_i$ est complexe, on a $\sigma_i : \ell \to \mathbb{C} = \ell_{v_i}$. Ces deux situations déterminent pour $[\ell : k] = 2$ la signature de $\ell$, qu'on notera dans tous les cas par $(s_1, s_2)$.

**Proposition 13.7.** *Soit $G$ admissible pour $\mathrm{Isom}^+(\mathbb{H}^n)$. On suppose que $G$ est une forme externe.*

1. *Si $r = 2m+1$, alors $(s_1, s_2) = (2, d-1)$.*
2. *Si $r = 2m$ et $G$ n'est pas de type ${}^{3,6}\mathrm{D}_4$, alors $(s_1, s_2) = (2d-2, 1)$.*

*3. Si $k \neq \mathbb{Q}$ alors dans tous les cas $\ell$ possède au moins une place réelle. En particulier les seules racines de l'unité dans $\ell$ sont $\pm 1$.*

PREUVE. Si $G$ n'est pas de type ${}^6\mathrm{D}_4$, alors $\ell$ est le corps minimal de déploiement de $G'$ et est donc le corps minimal pour lequel $G|\ell$ est une forme interne (cf. définition de $\ell$ au point 9.9 et remarque 7.51). Ainsi pour une place $v \in V_\infty(k)$ on a que $G|k_v$ est interne si et seulement si $\ell \hookrightarrow k_v$. Or $k_v$ est toujours isomorphe à $\mathbb{R}$ ($k$ est totalement réel), et pour autant que $[\ell : k] = 2$ (ce qui n'exclut que le cas ${}^3\mathrm{D}_4$) ceci correspond à dire que $\ell$ possède deux places réelles au-dessus de $v$. A l'inverse si $G|k_v$ est une forme externe, $\ell_v$ doit être une extension de corps non triviale de $k_v$, i.e. $\ell_v = \mathbb{C}$. On utilise alors comme dans le preuve de la proposition 13.6 la structure de $\mathrm{Spin}_{(n,1)}$ et $\mathrm{Spin}_{n+1}$ (formes externes ou internes en fonction du rang) pour obtenir les deux premières affirmations. On voit que dans ces deux cas on obtient immédiatement la troisième affirmation (où pour $r = 2m$ on a besoin de l'hypothèse $d > 1$, i.e. $k \neq \mathbb{Q}$). Il reste à prouver l'affirmation *3* pour les types ${}^{3,6}\mathrm{D}_4$. Pour cela on utilise le fait que $\sum_{w|v}[\ell_w : k_v] = [\ell : k] = 3$. Ainsi pour $v \in V_\infty$ fixé il existe nécessairement une extension $\ell_w|k_v$ triviale, i.e. avec $\ell_w \cong \mathbb{R}$. □

## §13.3 Mesure normalisée et volume hyperbolique

La mesure $\mu$ sur $\mathscr{G} = \mathrm{SO}(n,1)^\circ$ définie en §9.3 n'a pas la même normalisation que le volume hyperbolique $\mathrm{vol}_{\mathbb{H}}$. Rappelons que la mesure $\mathrm{vol}_{\mathbb{H}}$ sur $\mathbb{H}^n$ est définie par la métrique riemannienne sur $\mathbb{H}^n$, normalisée par la condition que la courbure sectionnelle est constante égale à $-1$. Nous établissons dans ce paragraphe la relation entre $\mu$ et $\mathrm{vol}_{\mathbb{H}}$.

La mesure $\mu$ est considérée aussi bien comme mesure sur $\mathrm{SO}(n,1)^\circ$ que comme mesure sur le revêtement $\mathrm{Spin}(n,1)$. De plus $\mu$ peut être vue comme une mesure sur la forme compacte réelle $\mathrm{Spin}(n+1)$, ainsi que sur le groupe $\mathrm{SO}(n+1)$ dont elle est le revêtement (cf. §9.3). Par définition $\mu$ est normalisée par la relation :

$$\mu\left(\mathrm{Spin}(n+1)\right) \quad = \quad 1.$$

Comme le revêtement $\mathrm{Spin}(n+1) \to \mathrm{SO}(n+1)$ est double (et bien surjectif), on obtient : $\mu(\mathrm{SO}(n+1)) = 1/2$.

Notons ici par $\mathfrak{g}$ l'algèbre de Lie de $\mathscr{G}$. L'espace hyperbolique peut s'écrire comme espace symétrique sous la forme $\mathbb{H}^n = \mathscr{G}/\mathrm{SO}(n)$. A ce quotient correspond une décomposition $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$, où $\mathfrak{k}$ est l'algèbre de Lie de $\mathrm{SO}(n)$, et l'espace vectoriel $\mathfrak{p}$ peut s'identifier avec l'espace tangent de $\mathbb{H}^n$ au « point » $\mathrm{SO}(n)$. Considérons alors $\omega^1$ la forme multilinéaire altérnée sur $\mathfrak{p}$ qui correspond à la mesure $\mathrm{vol}_{\mathbb{H}}$, ainsi que la forme alternée de degré maximal $\omega^0$ sur $\mathrm{SO}(n)$, normalisée par $\int_{\mathrm{SO}(n+1)} \omega^0 = 1$. La mesure de Haar $\mu_{\mathbb{H}}$ déterminée par $\omega^0 \wedge \omega^1$ est alors telle que :

$$\mathrm{vol}_{\mathbb{H}}(\mathbb{H}^n/\Gamma) \quad = \quad \mu_{\mathbb{H}}(\mathscr{G}/\Gamma),$$

pour chaque réseau $\Gamma$ de $\mathscr{G}$.

On utilise à présent la dualité entre l'espace hyperbolique et l'espace sphérique, explicitée dans [Hel62, Ch.V §2]. L'algèbre $\mathfrak{k}\oplus i\mathfrak{p}$ (où $i^2=-1$) est l'algèbre de Lie (réelle) du groupe compact $\mathrm{SO}(n+1)$, et cette algèbre possède la même complexification que $\mathfrak{g}$. Ceci permet de voir $\omega^0\wedge\omega^1$ comme une forme multilinéaire sur $\mathrm{SO}(n+1)$, plus précisément comme la forme qui induit sur le quotient $\mathrm{SO}(n+1)/\mathrm{SO}(n)$ la mesure de la sphère, normalisée par le fait que la courbure sectionnelle vaut $+1$. Comme $\omega^0$ donne mesure 1 sur $\mathrm{SO}(n)$, on obtient :

$$\mu_{\mathbb{H}}(\mathrm{SO}(n+1)) \quad = \quad \mathrm{vol}(\mathbb{S}^n),$$

le volume (surface) standard de la sphère unité. En comparant avec l'évaluation de $\mu$ sur $\mathrm{SO}(n+1)$ on a finalement :

$$\mu_{\mathbb{H}} \quad = \quad 2\,\mathrm{vol}(\mathbb{S}^n)\,\mu. \tag{13.1}$$

La formule du volume de $\mathbb{S}^n$ diffère en fonction de la parité de $n$. Pour $n=2r-1$ impair, on obtient :

$$\mu_{\mathbb{H}} \quad = \quad \frac{4\pi^r}{(r-1)!}\,\mu. \tag{13.2}$$

**Remarque 13.8.** Pour $n$ pair le covolume des réseaux est proportionnel à la valeur absolue de la caractéristique d'Euler. En utilisant ce fait on peut obtenir dans ce cas la correspondance (13.1) d'une seconde manière (cf. [BP89, 3.4]).

## §13.4 Calcul du volume

Soit $\Gamma$ un sous-groupe arithmétique maximal de $G_{\mathcal{S}}=G(\mathbb{R})$, avec $G$ admissible pour $\mathscr{G}=\mathrm{Isom}^+(\mathbb{H}^n)$ ($n\geq 5$ et impair). La discussion en §13.3 permet de ramener le calcul du volume hyperbolique du quotient $\mathbb{H}^n/\Gamma$ à la considération de la mesure $\mu$. Selon (9.8) on a $\mu(\mathscr{G}/\Gamma)=\mu(G_{\mathcal{S}}/\Gamma)$. Comme il est supposé maximal, $\Gamma$ s'écrit comme normalisateur d'un sous-groupe arithmétique principal $\Lambda$ (cf. théorème 10.4) :

$$\Gamma \quad = \quad N_{G_{\mathcal{S}}}(\Lambda).$$

Le covolume de $\Gamma$ est donc donné par :

$$\mu(G_{\mathcal{S}}/\Gamma) \quad = \quad \frac{1}{[\Gamma:\Lambda]}\,\mu(G_{\mathcal{S}}/\Lambda).$$

Le calcul du covolume de $\Lambda$ est donné par la formule de Prasad (théorème 9.16) :

$$\mu(G_{\mathcal{S}}/\Lambda) \quad = \quad \mathscr{D}_k^{r^2-r/2}\,\mathscr{D}_{\ell|k}^{r-1/2}\,C(r)^d\,\mathscr{E}(\mathscr{P}), \tag{13.3}$$

où $\mathscr{P}$ est la collection cohérente attachée à $\Lambda$, et la constante $C(G)$ ne dépend que du rang de $G$ ($G$ admissible est de type $\mathrm{D}_r$), et sera ainsi désormais notée $C(r)$ dans ce contexte. De plus, selon les exemples 9.18 et 9.19, on peut réécrire cette formule sous la forme :

$$\mu(G_{\mathcal{S}}/\Lambda) \quad = \quad \mathscr{D}_k^{r^2-r/2}\,\mathscr{D}_{\ell|k}^{r-1/2}\,C(r)^d\,L_{\ell|k}(r)\prod_{i=1}^{r-1}\zeta_k(2i)\prod_{v\in\mathrm{T}}\lambda_v, \tag{13.4}$$

avec $L_{\ell|k} := \zeta_k$ si $\ell = k$. On rappelle encore la valeur de la constante $C(r)$, selon le point 9.10 :

$$C(r) \quad = \quad \frac{(r-1)!}{(2\pi)^r} \prod_{i=1}^{r-1} \frac{(2i-1)!}{(2\pi)^{2i}}. \tag{13.5}$$

On termine ce paragraphe avec quelques considérations à propos des facteurs lambda. On va supposer que $G$ n'est pas une forme trialitaire. De plus on note dans la suite par $r_v$ le $\hat{k}_v$-rang de $G$. Selon [Pra89, 2.10] on a pour tout $v \in \mathrm{T}$ :

$$\frac{q_v^{(\dim \overline{\mathrm{M}}_v + \dim \overline{\mathscr{M}}_v)/2}}{\#\overline{\mathrm{M}}_v(\mathbb{F}_v)} \quad \geq \quad \frac{q_v^{r_v+1}}{q_v+1}. \tag{13.6}$$

Cette borne est valable plus généralement dans n'importe quel groupe absolument simple, et peut être améliorée lorsqu'on travaille (comme nous) avec un cas particulier. Elle sera cependant suffisante pour nos besoins. Si $G$ est déployé sur $\hat{k}_v$, i.e $r = r_v$, le groupe $\overline{\mathscr{M}}_v$ est de type ${}^1\mathrm{D}_r$ ou ${}^2\mathrm{D}_r$ (cf. exemples 9.18 et 9.19), et on a donc selon les tableaux 7.1 et 9.3 :

$$\frac{\#\overline{\mathscr{M}}_v(\mathbb{F}_v)}{q_v^{\dim \overline{\mathscr{M}}_v}} \quad = \quad (1 \pm q_v^{-r}) \prod_{j=1}^{r-1} \left(1 - q_v^{-2j}\right). \tag{13.7}$$

En combinant (13.6) et (13.7) et en utilisant $q_v \geq 2$, on obtient aisément dans ce cas la borne suivante pour $\lambda_v$ (cf. définition en (9.15)) :

$$\begin{aligned} \lambda_v \quad &\geq \quad \frac{q_v}{q_v+1} q_v^r \left(1 - q_v^{-2}\right)^r \\ &\geq \quad \frac{2}{3} \left(\frac{3}{4} q_v\right)^r. \end{aligned} \tag{13.8}$$

Pour $v \in \mathrm{T}$ avec $G$ qui n'est pas déployé sur $\hat{k}_v$ (et donc $v \in \mathscr{R}$) on a $r_v = r-1$ et $\overline{\mathscr{M}}$ est de type $\mathrm{B}_{r-1}$. Un même calcul que le précédent montre alors que dans cette situation :

$$\lambda_v \quad \geq \quad \frac{2}{3} \left(\frac{3}{4} q_v\right)^{r-1}. \tag{13.9}$$

**Remarque 13.9.** Les bornes (13.8) et (13.9) permettent de voir (pour $G$ non trialitaire) que $\lambda_v > 1$ si $v \in \mathrm{T}$. On rappelle pour cela qu'on travaille avec $r \geq 3$. Ainsi l'apparition de facteurs lambda dans (13.4) implique une augmentation du covolume pour les sous-groupes arithmétiques principaux. D'après la remarque 9.14, pour obtenir un volume faible il s'agit de considérer un $k$-groupe admissible $G$ qui est quasi-déployé sur chaque complété $\mathfrak{p}$-adique $k_v$. Un tel groupe n'existe cependant pas dans toutes les situations.

## §13.5 Calcul de l'indice $[\Gamma : \Lambda]$

On applique ici dans le cas hyperbolique les connaissances du chapitre 12 pour calculer (ou du moins borner) l'indice $[\Gamma : \Lambda]$, pour $\Gamma$ et $\Lambda$ comme ci-dessus. On reprend librement les notations qui y ont été introduites. Il nous

faudra faire usage des distinctions de cas amenées par les propositions 13.6 et 13.7. Avec ces cas varie notamment la description du centre C de $G$ (cf. §12.4). Or celui-ci joue un rôle central dans le calcul de l'indice. On rappelle dans le tableau 13.1 la description du centre C de $G$ pour les cas qui apparaissent dans la proposition 13.6, ainsi que d'éventuelles restrictions sur $k$.

| type de $G$ | C | restriction pour $k$ |
|---|---|---|
| ${}^1\mathrm{D}_{2m+1}$ | $\mu_4$ | $k = \mathbb{Q}$ |
| ${}^2\mathrm{D}_{2m+1}$ | $\mathbf{R}^{(\mathbf{1})}_{\ell\vert k}(\mu_4)$ | |
| ${}^2\mathrm{D}_{2m}$ | $\mathbf{R}_{\ell\vert k}(\mu_2)$ | |
| ${}^{3,6}\mathrm{D}_4$ | $\mathbf{R}^{(\mathbf{1})}_{\ell\vert k}(\mu_2)$ | $k \neq \mathbb{Q}$ |

Tab. 13.1 – Centres des groupes admissibles

On suppose ici que $\Gamma$ possède un covolume minimal parmi les sous-groupes arithmétiques de $G(\mathbb{R}) = G_{\mathcal{S}}$. Ainsi $\Lambda$ possède la propriété de la proposition 12.4, et son indice dans $\Gamma$ est donné par :

$$[\Gamma : \Lambda] \quad = \quad \#(\mathcal{Z}/\mathrm{C}(k)) \cdot \#A_\xi.$$

Sur les places archimédiennes, le centre C de $G$ admissible pour $\mathrm{Isom}^+(\mathbb{H}^n)$ ne dépend que du rang $r$. On calcule facilement que $\mathrm{C}(\mathbb{R}) = \mathcal{Z}$ possède un ordre égal à 2, aussi bien pour un rang pair que pour un rang impair. On voit aisément que $\mathrm{C}(k) = \pm 1$ pour les cas où $G$ n'est pas une forme trialitaire. Par contre pour une forme trialitaire, le fait que $[\ell : k] = 3$ permet d'obtenir $\mathrm{C}(k) = 1$. Ce qui nous donne :

$$[\Gamma : \Lambda] \quad = \quad \begin{cases} 2 \cdot \#A_\xi & \text{si } G \text{ est de type } {}^{3,6}\mathrm{D}_4; \\ \#A_\xi & \text{sinon.} \end{cases} \tag{13.10}$$

La seconde étape pour le calcul qui nous occupe est de décrire le groupe $A$, à l'aide de son image $\mathbf{A}/(\ell^\times)^{\mathfrak{n}}$. On rappelle que $\mathbf{A}$ est sous-groupe de $\mathbf{L} \subset \ell^\times$, où $\mathbf{L}$ prend des formes variées en fonction du type de $G$ (cf. §12.5). On a avec les notations pour $\ell$ introduites dans §13.2 :

**Proposition 13.10.** *Pour chacun des types admissibles non trialitaires, le groupe* $\mathbf{A}$ *est donné comme suit :*

1. *Si* $G$ *est de type* ${}^1\mathrm{D}_{2m+1}$ *:* $\mathbf{A} = \{\, x \in \mathbb{Q}^\times \mid x > 0\}$.
2. *Si* $G$ *est de type* ${}^2\mathrm{D}_{2m}$ *:* $\mathbf{A} = \{\, x \in \ell^\times \mid \sigma_i(x), \sigma'_i(x) > 0 \ \ \forall\, i \neq 0\}$.
3. *Si* $G$ *est de type* ${}^2\mathrm{D}_{2m+1}$ *:* $\mathbf{A} = \{\, x \in \mathbf{L} \mid \sigma_0(x) > 0\}$.

Preuve. Commençons par expliquer le cas le plus simple : $G$ de type ${}^1\mathrm{D}_{2m+1}$ et donc nécessairement $k = \mathbb{Q}$. Alors $A$ est donné par définition (cf. (12.7)) par le noyau de

$$\mathbb{Q}^\times/(\mathbb{Q}^\times)^4 \quad \to \quad \mathbb{R}^\times/(\mathbb{R}^\times)^4 = \mathbb{R}/\mathbb{R}_{>0},$$

et $\mathbf{A}$ est l'image inverse dans $\mathbb{Q}^\times$ de ce noyau. Ceci donne la première affirmation. Pour le reste on s'appuie notamment sur la matière présentée en §11.5. Pour

le deuxième cas, on a que $\mathbf{L} = \ell^\times/(\ell^\times)^2$ et $\mathbf{A}$ se décrit comme l'image inverse dans $\ell^\times$ du noyau de

$$\ell^\times/(\ell^\times)^2 \quad \to \quad \prod_{v\in V_\infty} \ell_v^\times/(\ell_v^\times)^2$$

Selon la discussion en §13.2, $\ell_{v_0} = \mathbb{C}$ et donc $\ell_{v_0}^\times/(\ell_{v_0}^\times)^2$ est trivial. Par contre aux places $v_i$ avec $i \neq 0$ on a $\ell_{v_i} = \mathbb{R}\oplus\mathbb{R}$ et cela détermine les conditions données en *2*. Pour le type ${}^2\mathrm{D}_{2m+1}$ le raisonnement similaire s'applique avec

$$\mathbf{L} \quad = \quad \left\{x \in \ell^\times \mid N_{\ell|k}(x) \in (k^\times)^4\right\}.$$

Pour ce type on a $\ell_{v_0} = \mathbb{R}\oplus\mathbb{R}$ et $\ell_{v_i} = \mathbb{C}$ pour $i \neq 0$. Ces places $v_i \neq v_0$ n'apportent aucune condition pour être dans $\mathbf{A}/(\ell^\times)^4$. En $v_0$, on doit considérer le noyau du produit

$$\left(\mathbb{R}^\times/\mathbb{R}_{>0}\right) \times \left(\mathbb{R}^\times/\mathbb{R}_{>0}\right) \quad \stackrel{\cdot}{\longrightarrow} \quad \mathbb{R}^\times/\mathbb{R}_{>0}.$$

L'élément trivial de ce noyau est $\mathbb{R}_{>0}\times\mathbb{R}_{>0}$. Un élément $x \in \mathbf{L}$ représente cet élément si et seulement si $\sigma_0(x) > 0$ (ou de façon équivalente $\sigma_0'(x) > 0$). □

L'ordre du groupe $A_\xi$ est relié à l'ordre de $\mathbf{A}_{\mathfrak{n}}/(\ell^\times)^{\mathfrak{n}}$ par les entiers $\bar{q}, q$ et $q'$ (cf. §12.5). Plus précisément :

$$\#A_\xi \quad = \quad \frac{\bar{q}\cdot q}{q'}\,\#\mathbf{A}_{\mathfrak{n}}/(\ell^\times)^{\mathfrak{n}} \tag{13.11}$$

Parmi les cas qui nous intéressent, $\bar{q}$ peut être différent de 1 pour le type ${}^2\mathrm{D}_{2m+1}$. La détermination précise de $\bar{q}$ (voir le point 12.8) nécessite de calculer l'ordre du noyau de

$$\mu_4(k)/N_{\ell|k}(\mu_4(\ell)) \quad \longrightarrow \quad \prod_{v\in V_\infty} \mu_4(k_v)/N_{\ell_v|k_v}(\mu_4(\ell_v))$$

On voit immédiatement, comme $\mu_4(k) = \pm 1$, que cet ordre vaut au plus 2. Si $k \neq \mathbb{Q}$ il existe une place $v_i \neq v_0$, pour laquelle on doit avoir $\ell_{v_0} = \mathbb{C}$. Pour une telle place $v = v_i$ on remarque que le groupe

$$\mu_4(k_v)/N_{\ell_v|k_v}(\mu_4(\ell_v)) \tag{13.12}$$

est égal à $\{\pm 1\}$. Ainsi l'existence d'une telle place montre que $\bar{q} = 1$, ou de façon équivalente : $A \cong \mathbf{A}/(\ell^\times)^{\mathfrak{n}}$ si $k \neq \mathbb{Q}$. Par contre pour la place $v = v_0$ le groupe (13.12) est trivial, ce qui montre que pour $k = \mathbb{Q}$ et $G$ de type ${}^2\mathrm{D}_{2m+1}$ on a $\bar{q} = 2$, ce nombre étant l'ordre de $\mu_4(k)/N_{\ell|k}(\mu_4(\ell))$. En résumé :

$$\bar{q} \quad = \quad \begin{cases} 2 & \text{si } G \text{ est de type } {}^2\mathrm{D}_{2m+1} \text{ avec } k = \mathbb{Q}\,; \\ 1 & \text{pour toutes les autres situations.} \end{cases} \tag{13.13}$$

Nous sommes prêts pour donner pour chaque type admissible une borne supérieure pour l'indice $[\Gamma : \Lambda]$. On rappelle qu'on note $d := [k : \mathbb{Q}]$.

**Proposition 13.11.**

1. *Pour $k \neq \mathbb{Q}$ :*
   (a) *Si $G$ est de type ${}^2\mathrm{D}_{2m+1}$ :* $[\Gamma : \Lambda] \leq 2^{d+1} 4^{\#\hat{\mathrm{T}}} h_\ell$.
   (b) *Si $G$ est de type ${}^2\mathrm{D}_{2m}$ :* $[\Gamma : \Lambda] \leq 2^{2d-2} 2^{\#\mathscr{R}} 4^{\#\hat{\mathrm{T}}} h_\ell$.
   (c) *Si $G$ est de type ${}^{3,6}\mathrm{D}_4$ :* $[\Gamma : \Lambda] \leq 2^{3d+1} 2^{\#\mathscr{R}} 4^{\#\hat{\mathrm{T}}} h_\ell$.
2. *Pour $k = \mathbb{Q}$ :*
   (a) *Si $G$ est de type ${}^1\mathrm{D}_{2m+1}$ :* $[\Gamma : \Lambda] \leq 4^{\#\hat{\mathrm{T}}}$.
   (b) *Si $G$ est de type ${}^2\mathrm{D}_{2m+1}$ :* $[\Gamma : \Lambda] \leq 8 \cdot 4^{\#\hat{\mathrm{T}}} h_\ell$.
   (c) *Si $G$ est de type ${}^2\mathrm{D}_{2m}$ :* $[\Gamma : \Lambda] \leq 4 \cdot 2^{\#\mathscr{R}} 4^{\#\hat{\mathrm{T}}} h_\ell$.

Preuve. Les résultats établis dans (12.15), (12.16), (12.19), (13.10) et (13.13) ramènent le problème à borner l'ordre du groupe $U_{\mathbf{A}}/U_\ell^{\mathfrak{n}}$. Le théorème des unités de Dirichlet (théorème 4.24) permet directement de donner $\mathfrak{n}^{[\ell:k]\cdot d}$ comme borne de $\#U_\ell/U_\ell^{\mathfrak{n}}$. Mais plusieurs améliorations sont possibles au cas par cas pour la borne de $\#U_{\mathbf{A}}/U_\ell^{\mathfrak{n}}$. Ainsi les bornes énoncées sont démontrées à l'aide des considérations suivantes :

- La proposition 13.7 précise la signature du corps $\ell$ ainsi que l'ordre des racines de l'unité ; ceci permet au cas par cas d'appliquer le théorème 4.24 avec une plus grande précision.
- Pour le type ${}^2\mathrm{D}_{2m+1}$ (où $\mathbf{L} \neq \ell^\times$) on utilise le fait que $U_k^2 \subset N_{\ell|k}(U_\ell)$, ce qui permet d'améliorer la borne de $\#U_{\mathbf{L}}/U_\ell^4$ par un facteur $2^{d-1}$ ($= \#U_k^2/U_k^4$) par rapport à la borne pour $\#U_\ell/U_\ell^4$.
- Dans bien des cas la description de $\mathbf{A}$ donnée dans la proposition 13.10 permet une amélioration d'un facteur $1/2$ : lorsqu'elles apparaissent, les conditions de positivité montrent que $x, -x \in \mathbf{L}$ ne peuvent être simultanément dans $\mathbf{A}$.

□

# Chapitre 14. Candidats au volume minimal

Nous construisons dans ce chapitre pour chaque dimension $n$ impaire supérieure ou égale à 5 un réseau arithmétique hyperbolique cocompact (resp. non cocompact) dont le covolume à la même allure que le covolume qui apparaît dans l'énoncé du théorème 1.3 (resp. du théorème 1.4). Il sera clair par construction que les quotients orientables ainsi obtenus sont de sérieux candidats pour atteindre les minima $\nu_{\mathbf{c}}^n$ et $\nu_{\mathbf{nc}}^n$ des ensembles $\mathrm{vol}_{\mathbb{H}}(\mathcal{AQ}_{\mathbf{c}}^n)$ et $\mathrm{vol}_{\mathbb{H}}(\mathcal{AQ}_{\mathbf{nc}}^n)$. La preuve des théorèmes 1.3 et 1.4 au chapitre 15 s'appuiera sur l'existence de ces candidats.

Dans ce chapitre et le suivant, nous prendrons la liberté d'utiliser sans tout détailler certaines propriétés de corps de nombres explicitement donnés. Ces propriétés (calcul du nombre de classes, base de l'anneau des entiers, etc.) peuvent souvent pour nos exemples particuliers se calculer à la main. Nous le préciserons lorsque nous avons eu recours à l'utilisation du précieux système de calcul PARI/GP, disponible à l'adresse :

`http://pari.math.u-bordeaux.fr/`

## §14.1 Formes quadratiques

On va utiliser dans ce chapitre certaines propriétés bien connues des formes quadratiques et de leurs groupes Spin associés. On résume ici ces propriétés. Notre discussion porte essentiellement sur deux aspects. D'une part on va expliquer les implications qu'ont certaines propriétés d'une forme $f$ sur la stucture du groupe algébrique $\mathrm{Spin}_f$. Pour cette question le lecteur peut se référer à [Bor91, 23.4], où la structure de $\mathrm{SO}_f$ est explicitée (le cas de $\mathrm{Spin}_f$ étant similaire). L'autre aspect concerne la classification des formes quadratiques définies sur les corps $\mathfrak{p}$-adiques. Ce sujet est en principe couvert par n'importe quel ouvrage traitant de la théorie classique des formes quadratiques, par exemple [O'M63]. On va également utiliser les diverses informations et définitions que nous avons collecter jusqu'à présent dans les exemples concernant les formes quadratiques. On rappelle en particulier les conventions de la remarque 2.17. De plus, comme nous avons en tête des applications sur les espaces hyperboliques de dimensions impaires, on va considérer uniquement des formes quadratiques de dimensions paires.

Soit $k$ un corps de caractéristique $\neq 2$. Une forme quadratique $f$ est dite *anisotrope* (sur $k$) si pour chaque $x \in \mathbf{V}_f \smallsetminus \{0\}$ on a $f(x) \neq 0$. Dans le cas contraire $f$ est dite *isotrope*. La même terminologie s'applique aux espaces quadratiques associés. Si deux formes binaires (i.e. de dimension 2) sont isotropes, alors elles sont nécessairement équivalentes. On peut donc noter par $\mathbf{h}$ l'unique (à isomorphisme près) espace quadratique sur $k$ de dimension 2 correspondant aux

formes quadratiques isotropes. Le discriminant $\mathrm{d}(\mathbf{h})$ vaut $-1$ dans $k^\times/(k^\times)^2$. Une propriété fondamentale est la suivante : si $f$ est une forme isotrope (non dégénérée), alors $\mathbf{h}$ est un facteur direct orthogonal de $\mathbf{V}_f$. Cela peut bien sûr s'itérer jusqu'à décomposer $\mathbf{V}_f$ comme somme

$$\mathbf{V}_f \quad \cong \quad \mathbf{h}^s \perp \mathbf{D},$$

où $\mathbf{D}$ est un espace quadratique anisotrope. Pour une telle décomposition le discriminant est donné par :

$$\mathrm{d}(f) = (-1)^s \cdot \mathrm{d}(\mathbf{D}) \quad \in \quad k^\times/(k^\times)^2 \tag{14.1}$$

Comme nous l'avons déjà mentionné au point 13.3, le groupe algébrique $\mathrm{Spin}_f$ (avec $f$ de dimension $2r \geq 4$) est de type absolu $\mathrm{D}_r$. On sait que le $k$-groupe $\mathrm{Spin}_f$ est déployé exactement lorsque $\mathbf{V}_f \cong \mathbf{h}^r$. Le contenu de l'exemple 7.52 assure alors que $\mathrm{Spin}_f$ est une forme interne si et seulement si

$$\mathrm{d}(f) = \mathrm{d}(\mathbf{h})^r = (-1)^r \quad \text{dans} \quad k^\times/(k^\times)^2.$$

En particulier, le groupe $\mathrm{Spin}_f$ devient une forme interne lorsque considéré sur l'extension

$$\ell \quad := \quad k\left(\sqrt{(-1)^r \mathrm{d}(f)}\right), \tag{14.2}$$

qui est au plus quadratique. On constate alors que les formes trialitaires ne peuvent apparaître sous la forme de groupes Spin. On peut encore voir que $\mathrm{Spin}_f$ est quasi-déployé exactement lorsque $\mathbf{V}_f \cong \mathbf{h}^{r-1} \perp \mathbf{D}$ pour un espace quadratique $\mathbf{D}$ de dimension 2. Dans ce cas $\mathrm{Spin}_f$ n'est pas déployé exactement lorsque $\mathbf{D}$ est anisotrope.

Supposons à présent travailler avec une forme $f$ définie sur un corps de nombres $k$. Par extension on obtient pour chaque place $v \in V$ une forme $f$ définie sur le complété $k_v$. Pour les places $v \in V_\infty$ réelles, les formes quadratiques d'une dimension fixée sont complètement classifiées (à équivalence près) par leur signature. Pour les places finies on aura besoin d'un autre invariant, défini à l'aide du symbole de Hilbert. Pour chaque place $v \in V$, étant donné deux éléments $a, b \in k_v$, le *symbole de Hilbert* :

$$\left(\frac{a,b}{v}\right)$$

est défini comme valant 1 si l'équation $ax^2 + by^2 = 1$ possède une solution dans $k_v$, et $-1$ dans le cas contraire. Le symbole de Hilbert respecte la formule du produit : si $a$ et $b$ sont dans $k$, alors

$$\prod_{v \in V} \left(\frac{a,b}{v}\right) \quad = \quad 1.$$

Pour les unités sur une place finie, le symbole de Hilbert est trivial à condition que la place en question ne soit pas dyadique. En d'autres termes : si $v \in V_\mathrm{f}$ est telle que $v \nmid 2$ et si $a$ et $b$ sont dans $\mathscr{O}_v^\times$, alors $\left(\frac{a,b}{v}\right) = 1$. L'invariant de Hasse d'une forme quadratique est défini à partir du symbole de Hilbert comme suit.

A équivalence près, on peut supposer que la forme $f$ définie sur $k_v$ est écrite sous forme diagonale (cf. remarque 7.53) :

$$f(x_1, \ldots, x_{2r}) \quad = \quad \sum_{i=1}^{2r} a_i x_i^2.$$

Alors l'*invariant de Hasse* (ou *invariant de Hasse-Witt*) de $f$ (en $v$) est donné par :

$$\mathrm{H}_v(f) \quad := \quad \prod_{1 \leq i \leq j \leq 1} \left( \frac{a_i, a_j}{v} \right). \tag{14.3}$$

La formule du produit est donc là aussi respectée. Aux places finies l'invariant de Hasse complète le discriminant pour classifier les formes quadratiques. En effet, soient $f$ et $g$ deux formes quadratiques de même dimension définies sur $k_v$, avec $v \in V_{\mathrm{f}}$. Alors $f$ et $g$ sont équivalentes (sur $k_v$) si et seulement si :

$$\mathrm{d}(f) = \mathrm{d}(g) \quad \text{et} \quad \mathrm{H}_v(f) = \mathrm{H}_v(g).$$

Les discriminants $\mathrm{d}(f)$ et $\mathrm{d}(g)$ sont ici des éléments dans $k_v^\times/(k_v^\times)^2$. Notons encore que, comme pour le discriminant, il existe d'autre normalisation de l'invariant de Hasse.

La classification donnée ci-dessus pour les formes définies sur les corps $\mathfrak{p}$-adiques repose en fait sur le résultat suivant : toute forme quadratique de dimension $\geq 5$ sur un corps $\mathfrak{p}$-adique $k_v$ est isotrope. Ceci implique que sur $k_v$ avec $v \in V_{\mathrm{f}}$, l'espace quadratique $\mathbf{V}_f$ est nécessairement de l'une des trois formes suivantes :

$$\mathbf{V}_f \quad \cong \quad \begin{cases} \mathbf{h}^r \\ \mathbf{h}^{r-1} \perp \mathbf{D}_2 \\ \mathbf{h}^{r-2} \perp \mathbf{D}_4 \end{cases} \tag{14.4}$$

où $\mathbf{D}_i$ $(i = 2, 4)$ est un espace anisotrope de dimension $i$. Un autre fait remarquable intervient alors : il n'existe à isomorphisme près sur $k_v$ qu'un seul espace quadratique anisotrope $\mathbf{D}_4$ de dimension 4, et celui-ci possède un discriminant égal à 1. Si $\mathbf{V}_f \cong \mathbf{h}^{r-2} \perp \mathbf{D}_4$, $\mathrm{Spin}_f$ est alors une forme interne non déployée. On voit alors aussi que si $\mathrm{Spin}_f$ est une forme externe sur $k_v$, celle-ci doit nécessairement être quasi-déployée.

## §14.2 Candidat cocompact

Pour la dimension $n$ impaire, on fixe l'entier $r$ par la relation $n = 2r - 1$. Soit la forme quadratique $f_0$ définie sur $k_0 := \mathbb{Q}(\sqrt{5})$, donnée par

$$f_0(x_0, \ldots, x_n) \quad = \quad \left( (-1)^r \cdot 3 - 2\sqrt{5} \right) x_0^2 \; + \; x_1^2 \; + \; \cdots \; + \; x_n^2, \tag{14.5}$$

Le $k_0$-groupe $G_0 := \mathrm{Spin}_{f_0}$ est alors admissible pour $\mathrm{Isom}^+(\mathbb{H}^n)$ et suit notre convention admise en §13.1 que l'identité $k_0 \to \mathbb{R}$ correspond à l'unique place qui compose $\mathcal{S}$. On peut donc écrire $G_0(\mathbb{R})$ plutôt que $G_{0\mathcal{S}}$. Une base libre de

l'anneau $\mathscr{O}_{k_0}$ est donnée par 1 et $\omega := \frac{1+\sqrt{5}}{2}$. On sait aussi que $h_{k_0} = 1$. Comme $\pm\mathrm{d}(f_0)$ n'est pas un carré dans $k_0$, on a selon §14.1 que $G_0$ est de type ${}^2\mathrm{D}_r$. Tout sous-groupe arithmétique dans $G_0(\mathbb{R})$ est cocompact.

Par (14.2) on voit que le corps de déploiement de la forme interne quasi-déployée $G_0'$ est donné par :

$$\ell_0 := k_0(\sqrt{\alpha}), \tag{14.6}$$

où $\alpha := 3 - (-1)^r \cdot 2\sqrt{5}$. A isomorphisme près ce corps ne dépend pas du rang $r$. Une base libre de $\mathscr{O}_{\ell_0}$ sur $\mathscr{O}_{k_0}$ est donnée par 1 et $\tau_1 := \frac{1+\sqrt{\alpha}}{2}$. On en déduit que $\mathscr{D}_{\ell_0|k_0} = 11$, ou de façon équivalente $\mathscr{D}_{\ell_0} = 275$.

**Remarque 14.1.** Ce choix de $G_0$ est motivé par la volonté de minimiser l'expression du volume donnée par (13.3). Si on laisse dans un premier temps de côté la considération du facteur $C(r)^d\mathscr{E}(\mathscr{P})$, il s'agit de minimiser $\mathscr{D}_k$ et $\mathscr{D}_\ell$. Or $k_0$ est le corps totalement réel dont le discriminant est le plus petit, et $\ell_0$ est le corps de signature $(2,1)$ (condition de la proposition 13.7) de plus petit discriminant (en valeur absolue). On peut obtenir cette dernière information en interrogeant par exemple la base de données QAOS (cf. remarque 15.1).

En plus de la minimisation des discriminants, il faut s'assurer que le groupe $G_0$ contienne des sous-groupes arithmétiques principaux pour lesquels le produit d'Euler $\mathscr{E}(\mathscr{P})$ reste faible. D'après la remarque 13.9, cela est vérifié par ce résultat :

**Proposition 14.2.** *$G_0$ est quasi-déployé sur chaque complété $\mathfrak{p}$-adique de $k_0$.*

PREUVE. On utilise la structure de $\mathrm{Spin}_f$ sur les corps $\mathfrak{p}$-adiques, explicitée en §14.1. On a $\mathrm{d}(f_0) = \pm\alpha$, et cet élément engendre un idéal premier de $\mathscr{O}_{k_0}$. Il s'agit de l'unique place finie où $\ell_0|k_0$ est ramifié. Grâce à la proposition 9.5 on voit que le groupe $G_0$ est nécessairement de type externe sur le complété de $k_0$ en $(\alpha)$, et donc y est quasi-déployé selon §14.1. Aux places $v \in V_{\mathrm{f}}(k_0)$ qui sont non dyadiques, $-1$ tout comme $\pm\alpha$ sont dans $\mathscr{O}_v^\times$, ce qui implique que $\mathrm{H}_v(f_0) = \mathrm{H}_v(\mathbf{h}^r)$, prouvant là aussi que $G_0|k_v$ est quasi-déployé. Il reste à examiner l'unique place dyadique de $k$, donnée par l'idéal premier $(2) \subset \mathscr{O}_{k_0}$. On contrôle que l'équation

$$x^2 \quad = \quad \alpha$$

ne possède pas de solution modulo (8) dans l'anneau $\mathscr{O}_{k_0}$, ce qui empêche encore $G_0$ d'être une forme interne sur le complété de $G_0$ en (2). □

Soit alors $\Lambda_0 = \Lambda^{\mathfrak{m}}$ un sous-groupe arithmétique principal de $G_0$ de covolume minimal (on se réfère à §12.3 pour la construction et les propriétés de $\Lambda^{\mathfrak{m}}$). Notre proposition montre que l'ensemble T défini dans la remarque 9.14 et qui indexe les facteurs lambda dans la formule du volume, est en fait vide pour $\Lambda_0$. On obtient selon (13.4) le covolume :

$$\mu(G_0(\mathbb{R})/\Lambda_0) \quad = \quad 5^{r^2-r/2} \cdot 11^{r-1/2} \cdot C(r)^2 \, L_{\ell_0|k_0}(r) \prod_{j=1}^{r-1} \zeta_k(2j) \tag{14.7}$$

La proposition 12.4 montre que le normalisateur :

$$\Gamma_0 \quad := \quad N_{G_0(\mathbb{R})}(\Lambda_0) \tag{14.8}$$

est de covolume minimal parmi les sous-groupes arithmétiques de $G_0(\mathbb{R})$. Il s'agit de calculer l'indice $[\Gamma_0 : \Lambda_0]$, à l'aide du matériel présenté en §13.5. Comme le nombre de classe $h_{\ell_0}$ vaut 1, la suite exacte (12.18) montre que $\mathbf{A}_{\mathfrak{n}}/(\ell_0^\times)^{\mathfrak{n}}$ est isomorphe à $U_{\mathbf{A}}/U_{\ell_0}^{\mathfrak{n}}$. Une base pour le groupe $U_{\ell_0}$ est donnée par les deux éléments :

$$\tau_1 := \frac{1+\sqrt{\alpha}}{2} \quad ; \quad \tau_2 := \frac{1-\sqrt{\alpha}}{2}.$$

On peut alors identifier les éléments du groupe $U_{\ell_0}/U_{\ell_0}^{\mathfrak{n}}$ avec le système de représentants :

$$\left\{ \pm \tau_1^i \tau_2^j \;\middle|\; 0 \leq i,j \leq \mathfrak{n}-1 \right\}.$$

Il faut alors distinguer le cas $r = 2m$ du cas $r = 2m+1$ pour appliquer la proposition 13.10. Celle-ci nous montre que le sous-groupe $U_{\mathbf{A}}/U_{\ell_0}^{\mathfrak{n}}$ est représenté par les éléments :

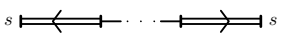
$$\begin{array}{cc} 1, \tau_1^2\tau_2^2, -\tau_1\tau_2^3, -\tau_1^3\tau_2 & \text{si} \quad r = 2m+1; \\ 1, -\tau_1\tau_2 & \text{si} \quad r = 2m, \end{array}$$

ce qui nous donne

$$\#U_{\mathbf{A}}/U_{\ell_0}^{\mathfrak{n}} \;=\; \begin{cases} 4 & \text{si } r = 2m+1; \\ 2 & \text{si } r = 2m. \end{cases} \tag{14.9}$$

Pour obtenir la valeur de $[\Gamma_0 : \Lambda_0]$ il nous faut encore connaître les valeurs des entiers $\bar{q}, q$ et $q'$. Selon (13.13) on a $\bar{q} = 1$. La proposition 14.2 montre que l'ensemble de places $\hat{\mathrm{T}}$ est vide dans le cas qu'on examine. En particulier, par (12.15) on voit immédiatement que $q = 1$ si $r = 2m+1$. Comme l'ensemble $\mathscr{R} = \mathrm{M}$ contient l'unique place correspondante à l'idéal premier $(\alpha)$, on voit par (12.16) que $q \leq 2$ si $r = 2m$. Mais dans ce cas il est également aisé de déterminer $q$ avec précision : l'élément $\tau_1\sqrt{\alpha}$ appartient à $\mathbf{A}_2^{\mathrm{M}}$ sans être dans $\mathbf{A}_2$. On en déduit que l'indice $q$ de $\mathbf{A}_2/(\ell_0^\times)^2$ dans $\mathbf{A}_2^{\mathrm{M}}/(\ell_0^\times)^2$ vaut 2.

La détermination de $q'$ est plus problématique (aussi bien avec $r = 2m$ que $r = 2m+1$). Pour l'unique place finie $v = (\alpha)$ qui compose $\mathscr{R}$, le diagramme local $\Delta_v$ est donné par (cf. exemple 8.9) :




et ce diagramme possède une seule symétrie non triviale. La discussion dans [Tit79, 2.5] montre qu'on a effectivement $\#\Xi_v = 2$ dans cette situation. Ainsi $q'$ est soit égal à 1, soit égal à 2 (et a priori cette valeur peut dépendre de $r$). Aucun élément présenté dans cette thèse ne permet de lever cette incertitude, et on se contentera donc ici du résultat :

$$[\Gamma_0 : \Lambda_0] \;=\; 2 \text{ ou } 4. \tag{14.10}$$

Cette indice achève avec (14.7) le calcul du volume $\mu(G_0(\mathbb{R})/\Gamma_0)$. A l'aide de §13.3 on constate que le quotient $\mathbb{H}^n/\Gamma_0$ possède un volume hyperbolique qui a la même forme que la valeur $\nu_{\mathbf{c}}^n$ donnée dans notre théorème 1.3.

**Remarque 14.3.** Dans cette thèse nous ne prétendrons pas que $\mathrm{vol}_{\mathbb{H}}(\mathbb{H}^n/\Gamma_0)$ est égal à $\nu_{\mathbf{c}}^n$ (même si l'on s'attend à avoir ce résultat). Les valeurs $\mathrm{vol}_{\mathbb{H}}(\mathbb{H}^n/\Gamma_0)$ et $\nu_{\mathbf{c}}^n$ sont toutes deux déterminées à un facteur 2 près, et a priori ce facteur ne doit pas être égal.

**Remarque 14.4.** Pour déterminer $q'$ il faudrait savoir si dans notre cas $A_{\xi,\mathscr{R}} \cong \mathbf{A}_{\mathfrak{n}}^{\mathscr{R}}/(\ell_0^\times)^{\mathfrak{n}}$ opère trivialement ou non sur le diagramme $\Delta_v$ (où $\{v\} = \mathscr{R}$). Ce problème nécessite d'expliciter l'opération de $H^1(k, \mathrm{C})$ sur $\Delta_v$ pour $v \in \mathscr{R}$, dans la même idée que le lemme 12.7 le fait pour les places $v \notin \mathrm{M}$. L'article [BP89] ne donne pas de moyen de le faire (les auteurs n'en ont du reste pas besoin). En travaillant avec un cas particulier, il semble cependant possible de parvenir au calcul de $q'$, spécialement dans le cas de $G_0$, où le groupe est quasi-déployé (et donc pas trop compliqué) sur le complété de $k_0$ en l'unique place $v = (\sqrt{\alpha})$ de $\mathscr{R}$. Un argument tout à fait similaire à celui que l'on recherche apparaît dans la prépublication [MSG] pour le cas des groupes de type A. Si les auteurs parviennent à adapter cet argument au cas qui nous intéresse, la version finale de [BE] devrait contenir le calcul de $q'$. Cette thèse n'examine pas plus loin le problème du calcul de $q'$, lequel nécessite un examen de la structure de $G|k_v$ plus détaillé que celui que nous avons donné. Toutefois nous verrons au paragraphe §14.4 des considérations de nature géométrique qui peuvent laisser penser que pour $n = 5$ on a $[\Gamma_0 : \Lambda_0] = 2$ et donc $q' = 2$ dans ce cas.

## §14.3 Candidat non cocompact

On procède maintenant à la construction de candidats non cocompacts, c'est-à-dire qu'on travaille avec $k = \mathbb{Q}$. Pour unifier la notation avec le cas cocompact on va parfois noter $k_1 := \mathbb{Q}$. Contrairement au cas cocompact, nous devons faire des distinctions de cas en fonction du rang. Pour chaque rang $r \geq 3$, soit la forme quadratique :

$$f_1(x_0, \ldots, x_n) \quad = \quad \begin{cases} -x_0^2 + x_1^2 + \cdots + x_n^2 & \text{si } r = 2m+1; \\ -3x_0^2 + x_1^2 + \cdots + x_n^2 & \text{si } r = 2m. \end{cases} \tag{14.11}$$

On considère le groupe admissible $G_1 := \mathrm{Spin}_{f_1}$ associé. Le corps de déploiement $\ell$ de la forme interne quasi-déployée de $G$ vaut :

$$\ell_1 \quad := \quad \begin{cases} \mathbb{Q} & \text{si } r = 2m+1; \\ \mathbb{Q}(\sqrt{-3}) & \text{si } r = 2m. \end{cases} \tag{14.12}$$

En particulier, pour $r = 2m+1$ le groupe $G_1$ est une forme interne. Le discriminant de $\mathbb{Q}(\sqrt{-3})$ vaut 3. De façon similaire au cas compact (remarque 14.1), ce corps $\ell_1$ est celui de plus petit discriminant parmi les corps $\ell$ des groupes admissibles. L'analogue de la proposition 14.2 demande aussi une différentiation des cas :

**Proposition 14.5.**

1. *Soit $r = 2m+1$. Si $m$ est pair, alors $G_1$ est déployé sur le corps p-adique $\mathbb{Q}_p$ pour chaque nombre premier $p$. Si $m$ est impair, alors $G_1$ est déployé sur $\mathbb{Q}_p$ si et seulement si $p \neq 2$ ($p$ premier).*
2. *Pour $r = 2m$ le groupe $G_1$ est quasi-déployé sur chaque corps p-adique.*

PREUVE. La deuxième partie de l'énoncé se démontre de manière tout à fait analogue à la proposition 14.2. Soit alors $r = 2m+1$. Dans ce cas $G_1$ est une forme interne sur chaque complété $\mathbb{Q}_p$. L'invariant de Hasse $\mathrm{H}_p(f_1) := \mathrm{H}_{(p)}(f_1)$ contrôle si $G_1$ est déployé ou non sur $\mathbb{Q}_p$ ($p$ premier). Pour $p \neq 2$ on voit que cet invariant est trivial, comme pour $\mathbf{h}^r$. Ainsi $G_1|\mathbb{Q}_p$ est déployé lorsque $p \neq 2$. D'après la formule du produit pour le symbole de Hilbert, on a $\left(\frac{-1,-1}{2}\right) = -1$. On calcule alors que $\mathrm{H}_2(f_1) = -1$, tandis que $\mathrm{H}_2(\mathbf{h}^{2m+1}) = (-1)^{m+1}$. Ceci termine la preuve de la première partie. □

Soit $\Lambda_1 = \Lambda^{\mathfrak{m}}$ un sous-groupe arithmétique principal de covolume minimal dans $G_1$ (cf. §12.3). La proposition 14.5 montre que si $r$ est pair ou $r = 2m+1$ avec $m$ impair, alors la formule du volume (13.4) pour $G_1$ ne contient pas de facteurs lambda : $\mathrm{T} = \emptyset$. Si par contre $r = 2m+1$ avec $m$ impair, on a $\mathrm{T} = \{(2)\}$. Ceci nous donne la formule suivante pour le covolume :

$$\mu(G_1(\mathbb{R})/\Lambda_1) \quad = \quad \begin{cases} \lambda_2\, C(r)\zeta(r)\prod_{j=1}^{r-1}\zeta(2j) & \text{si } r = 2m+1; \\ 3^{r-1/2}C(r)L_{\ell_1|\mathbb{Q}}(r)\prod_{j=1}^{r-1}\zeta(2j) & \text{si } r = 2m, \end{cases} \tag{14.13}$$

où pour $r = 2m+1$ on a $\lambda_2 := 1$ si $m$ est pair et $\lambda_2 := \lambda_{(2)}$ si $m$ est impair.

On procède pour le cas $r = 2m+1$ avec $m$ impair au calcul de $\lambda_2$. On traite de façon séparée le cas $r = 3$, où $G_1$ est de type ${}^1\mathrm{D}_3 = {}^1\mathrm{A}_3$. Dans ce cas $G_1$ possède sur $\mathbb{Q}_2$ le type ${}^1\mathrm{A}_{3,1}$ (cf. §14.1). L'exemple 8.26 permet alors la description du $\mathbb{F}_2$-groupe $\overline{\mathrm{M}}_2 := \overline{\mathrm{M}}_{(2)}$. Il s'agit en effet d'un produit presque direct entre le tore $\overline{T} := \mathbf{R}^{(\mathbf{1})}_{\mathbb{F}_4|\mathbb{F}_2}(\mathbf{G}_{\mathrm{m}})$ et le groupe semi-simple $\overline{\mathcal{G}}_2^{\mathrm{ss}} := \mathbf{R}_{\mathbb{F}_4|\mathbb{F}_2}(H)$, où $H$ est un $\mathbb{F}_4$-groupe semi-simple de type $\mathrm{A}_1$. Avec le théorème 7.56 on voit que $\#\overline{\mathrm{M}}_2(\mathbb{F}_2)$ s'obtient comme le produit des ordres de $\overline{T}(\mathbb{F}_2)$ et $\overline{\mathcal{G}}_2^{\mathrm{ss}}(\mathbb{F}_2)$. Le paragraphe §7.9 contient toute la matière pour obtenir ces ordres, tandis que le tableau 9.3 permet de déterminer la dimension de $\overline{\mathrm{M}}_2$. On voit facilement que le groupe $\overline{\mathscr{M}}_{(2)}$ est quant à lui semi-simple et de type ${}^1\mathrm{A}_3$. En insérant ces données dans la formule (9.15), on obtient finalement :

$$\lambda_2 \quad = \quad \frac{(2^r-1)(2^{r-1}-1)}{3} \tag{14.14}$$

Même si ce calcul a été effectué pour $r$ égal à 3, nous laissons le $r$ tel quel dans cette formule à dessein : le calcul de $\lambda_2$ pour les rangs supérieurs montre en effet que (14.14) reste valable pour ces cas. Ce calcul pour le type ${}^2\mathrm{D}_{r,r-2}$ est analogue au cas ${}^2\mathrm{A}_{3,1}$. Nous nous passons de le présenter ici.

On définit le normalisateur

$$\Gamma_1 \quad := \quad N_{G_1(\mathbb{R})}(\Lambda_1), \tag{14.15}$$

qui est de covolume minimal parmi les sous-groupes arithmétiques de $G_1(\mathbb{R})$. Le calcul de l'indice $[\Gamma_1 : \Lambda_1]$ est assez similaire au cas cocompact. On doit là aussi distinguer les cas $r = 2m$ et $r = 2m+1$. Pour ce dernier la parité de $m$ joue aussi un rôle : si $m$ est pair alors $\mathrm{M} = \hat{\mathrm{T}} = \emptyset$, tandis que pour $m$ impair on a $\mathrm{M} = \hat{\mathrm{T}} = \{(2)\}$. Pour $r = 2m$ on a $\mathrm{M} = \mathscr{R} = \{(3)\}$. Dans tous les cas on a $h_{\ell_1} = 1$, ce qui ramène le calcul de $\mathbf{A}_{\mathfrak{n}}/(\ell_1^{\times})^{\mathfrak{n}}$ au calcul de $U_{\mathbf{A}}/U_{\ell_1}^{\mathfrak{n}}$. Que $\ell_1$ soit égal à $\mathbb{Q}$ ou à $\mathbb{Q}(\sqrt{-3})$ on a $U_{\ell_1} = \{\pm 1\}$, ce qui avec la proposition 13.10 montre facilement que

$$\#U_{\mathbf{A}}/U_{\ell_1}^{\mathfrak{n}} \quad = \quad \begin{cases} 1 & \text{si } r = 2m+1; \\ 2 & \text{si } r = 2m. \end{cases}$$

Dans tous les cas on a $A \cong \mathbf{A}/(\ell_1^\times)^{\mathfrak{n}}$, et donc $\bar{q} = 1$. Pour $r = 2m+1$ avec $m$ pair, comme $\hat{\mathrm{T}} = \emptyset$ on obtient immédiatement $q = q' = 1$. Si $r = 2m+1$ on a $\#\hat{\mathrm{T}} = 1$, et donc $q$ vaut au plus 4. Mais $2, 4$ et $8$ sont des éléments de $\mathbb{Q}_4^{\mathrm{M}}$ qui représentent trois éléments distincts dans $\mathbf{A}_4^{\mathrm{M}}/(\mathbb{Q}^\times)^4 \smallsetminus \mathbf{A}_4/(\mathbb{Q}^\times)^4$. Ainsi $q$ est égal à 4. On procède de manière similaire pour le cas $r = 2m$, où $q$ est a priori égal à 1 ou 2 : $\sqrt{-3}$ représente un élément de $A_{\xi,\mathrm{M}}$ qui n'est pas dans $(\ell_1)_2/(\ell_1^\times)^2$ et donc $q = 2$ dans ce cas. Tout comme dans le cas cocompact, on fait référence à [Tit79, 2.5] pour s'assurer du fait que, aussi bien dans le cas $r = 2m$ que dans le cas $r = 2m+1$ avec $m$ impair, on a $\#\Xi_v = 2$ pour l'unique place $v \in \mathrm{M}$. Toutes ces considérations permettent l'énoncé :

$$[\Gamma_1 : \Lambda_1] \quad = \quad \begin{cases} 1 & \text{si } r = 2m+1 \text{ avec } m \text{ pair;} \\ 2 \text{ ou } 4 & \text{sinon.} \end{cases} \tag{14.16}$$

On en déduit que le volume hyperbolique de $\mathbb{H}^n/\Gamma_1$ a la même forme que le $\nu_{\mathbf{nc}}^n$ donné dans le théorème 1.4. Contrairement au cas cocompact, la discussion au paragraphe §15.7 montrera que $\mathrm{vol}_{\mathbb{H}}(\mathbb{H}^n/\Gamma_1)$ est bien égal à $\nu_{\mathbf{nc}}^n$.

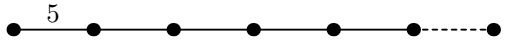
**Remarque 14.6.** On peut reprendre pour le cas non compact le contenu de la remarque 14.4. Une différence est toutefois à relever : le calcul de $q'$ pour $r = 2m+1$ et $m$ impair sera sans doute plus difficile, comme le groupe $G_1$ n'est pas quasi-déployé sur $\mathbb{Q}_2$. D'autre part, on peut faire remarquer que c'est avec certitude que le contenu du paragraphe §14.4 donnera la valeur de $q'$ pour les rang $r = 3$ et $r = 4$.

## §14.4 Comparaison avec les résultats géométriques

Nous avons déjà mentionné en §1.4 la possibilité de comparer nos résultats dans le cas non compact avec ceux de [Hil07]. Comme il sera vu en §15.7 que $\mathrm{vol}_{\mathbb{H}}(\mathbb{H}^n/\Gamma_1) = \nu_{\mathbf{nc}}^n$, on peut notamment déduire du théorème 1.4 la valeur exacte de $[\Gamma_1 : \Lambda_1]$ pour $r = 3$ et $r = 4$. En fait on peut même utiliser cette comparaison sans avoir recours à notre théorème. En effet, les quotients non compacts (non orientables) de $\mathbb{H}^5$, $\mathbb{H}^7$ et $\mathbb{H}^9$ qui possèdent le volume minimal sont formés par des réseaux qui sont commensurables avec des groupes de Coxeter simpliciaux. Il est connu (cf. [JKRT99, §5]) que ces groupes de Coxeter s'obtiennent à commensurabilité près comme stabilisateurs de la forme quadratique $f_1$ donnée en (14.11). Ce stabilisateur est commensurable avec $\Gamma_1$. Comme $\Gamma_1$ est par construction de covolume minimal dans sa classe de commensurabilité (dans $\mathrm{Isom}^+(\mathbb{H}^n)$), on en déduit que pour $n = 5, 7, 9$ le quotient orientable $\mathbb{H}^n/\Gamma_1$ est de même volume que le revêtement double du quotient minimal donné dans [Hil07] (cf. remarque 1.2). En comparant alors le covolume de $\mathbb{H}^n/\Gamma_1$ avec les volumes minimaux donnés chez Hild, en plus de constater la cohérence de nos calculs avec les résultats connus, on peut déduire que $[\Gamma_1 : \Lambda_1] = 2$ et donc $q' = 2$ pour $r = 3$ et $r = 4$.

Pour le cas compact, on ne dispose pas de résultats géométriques aussi forts que dans le cas non compact. Il existe cependant pour les dimensions 5 et 7 des groupes de Coxeter cocompacts, et ceux d'entre eux qui possèdent une présentation particulièrement simple apparaissent comme candidats naturels à réaliser le covolume minimal dans le cas non orientable. Ainsi on considère le groupe de

Coxeter hyperbolique suivant :




(14.17)

Il s'agit d'un groupe arithmétique, opérant dans $\mathbb{H}^5$ de manière cocompacte, avec un domaine fondamental qui est un 5-orthoschème tronqué. Le problème du calcul analytique du covolume d'un groupe discret devient difficile en dimension 5, quand bien même il s'agisse d'un groupe de Coxeter. En utilisant la différentielle de Schläfli et des calculs volumétriques pour les 3-faces de (14.17) [Kel89], Ruth Kellerhals a toutefois pu nous communiquer le covolume hyperbolique suivant pour (14.17) :

$$\frac{1}{16}\int_{\pi/5}^{\frac{1}{2}\mathrm{Acos}(1/5)} \Big(\text{Л}(b(x)+t(x)) - \text{Л}(b(x)-t(x)) + \text{Л}(\pi/6-t(x)) \\ - \text{Л}(\pi/6+t(x)) + \text{Л}(\pi/3+t(x)) \\ - \text{Л}(\pi/3-t(x)) + 2\text{Л}(\pi/2-t(x))\Big)dx, \tag{14.18}$$

où Л est la *fonction de Lobatchevsky* (qui est définie à partir de la fonction dilogarithme, cf. par exemple [Hil07, §1]), et les fonctions $b$ et $t$ sont données ici par :

$$\begin{aligned} b(x) &= \mathrm{Acos}\left(\frac{\sin(x)}{\sqrt{4\sin(x)^2-1}}\right); \\ t(x) &= \mathrm{Re}\left(\mathrm{Atan}\left(\sqrt{1-2\tan(b(x))^2}\right)\right), \end{aligned}$$

avec $\mathrm{Re}(\mathrm{Atan}(x)) \in ]-\pi/2, \pi/2[$. Si l'on prend la peine de donner le covolume de (14.17) c'est à cause du fait suivant : en utilisant PARI/GP nous pouvons contrôler que la valeur numérique de (14.18) coïncide avec la valeur numérique de $\frac{1}{4}\mathrm{vol}_{\mathbb{H}}(\mathbb{H}^5/\Lambda_0)$ . Nous nous sommes satisfaits d'un contrôle jusqu'à 50 décimales significatives.

**Remarque 14.7.** Pour le calcul numérique de (14.18) il est important (en tout cas sous PARI/GP) d'intégrer séparément sur les intervalles $[\frac{\pi}{5}, \frac{1}{2}\mathrm{Acos}(1/4)]$ et $[\frac{1}{2}\mathrm{Acos}(1/4), \frac{1}{2}\mathrm{Acos}(1/5)]$. La valeur $\frac{1}{2}\mathrm{Acos}(1/4)$ est en effet en quelque sorte singulière dans le calcul de Kellerhals, et une perte très importante en précision suit d'une intégration numérique qui ne prend pas en compte cet aspect.

Il apparaît ainsi quasiment sûr que le covolume de (14.17) est commensurable au covolume de $\Lambda_0$. Il est très probable que $\mathbb{H}^5/\Gamma_0$ soit le revêtement orientable du quotient de $\mathbb{H}^5$ par le groupe de Coxeter (14.18). Dans ce cas on aurait $q' = 2$ dans le calcul de $[\Gamma_0 : \Lambda_0]$.

**Remarque 14.8.** La très probable égalité entre (14.18) et $\frac{1}{4}\mathrm{vol}_{\mathbb{H}}(\mathbb{H}^5/\Lambda_0)$ est à notre connaissance difficile à déduire par un calclul analytique direct. Elle permet d'exprimer le produit des évaluations des fonctions zêta et de la fonction $L$ qui apparaît dans (14.7) en termes de fonctions impliquant des polylogarithmes. Le problème général d'une correspondance entre *valeurs spéciales* de fonctions zêta ou fonctions $L$ et polylogarithmes est l'object des *conjectures de Zagier* (voir par exemple [Oes93]).

# Chapitre 15. Preuve des théorèmes

Nous présentons dans ce dernier chapitre la preuve des résultats énoncés en §1.4. La preuve suit le même raisonnement pour le cas compact (théorème 1.3) et non compact (théorème 1.4). La méthode, ainsi que la plupart des techniques qui interviennent dans cette démonstration, apparaissent dans [Bel04].

Dans ce chapitre $G$ sera toujours un $k$-groupe admissible pour $\mathrm{Isom}^+(\mathbb{H}^n)$ (avec $n \geq 5$ et impair) et dont un sous-groupe arithmétique $\Gamma < G(\mathbb{R})$ atteint le covolume minimal $\nu_{\mathbf{c}}^n$ si $k \neq \mathbb{Q}$, respectivement $\nu_{\mathbf{nc}}^n$ si $k = \mathbb{Q}$. On rappelle que selon la proposition 13.2 le cas cocompact s'identifie à la situation $k \neq \mathbb{Q}$, et le cas non cocompact à la situation $k = \mathbb{Q}$. Comme d'habitude on désigne par $\ell$ le corps attaché à $G$ selon le point 9.9. De manière générale on admet pour $G$ et $\Gamma$ les notations qui ont été introduites aux chapitres 9, 12 et 13. L'hypothèse $n \geq 5$ implique que le rang $r = (n+1)/2$ de $G$ vaut au minimum 3. Le sous-groupe $\Gamma$ s'écrit comme le normalisateur $\Gamma = N_{G(\mathbb{R})}(\Lambda)$, où $\Lambda = \Lambda^{\mathfrak{m}}$ est un sous-groupe arithmétique principal comme dans la proposition 12.4.

L'idée de la preuve est de s'appuyer sur les constructions des sous-groupes $\Gamma_0$ et $\Gamma_1$ du chapitre 14, et d'utiliser l'inégalité (comme $\Gamma$ est supposé de covolume minimal)

$$\mu(G(\mathbb{R})/\Gamma) \quad \leq \quad \begin{cases} \mu(G_0(\mathbb{R})/\Gamma_0) & \text{si } k \neq \mathbb{Q} \\ \mu(G_1(\mathbb{R})/\Gamma_1) & \text{si } k = \mathbb{Q} \end{cases} \tag{15.1}$$

afin de déduire des bornes pour $\mathscr{D}_k$ (pour le cas compact) et pour $\mathscr{D}_\ell$. En améliorant progressivement les bornes pour $\mathscr{D}_k$ et $\mathscr{D}_\ell$ on pourra finalement déduire que si $\Gamma$ est cocompact alors $k = k_0$ et $\ell = \ell_0$, tandis que $\ell = \ell_1$ (défini en (14.12)) si $\Gamma$ n'est pas cocompact. Pour conclure la démonstration il suffira de montrer qu'aucun $k_i$-groupe algébrique $G$ pour lequel $\ell = \ell_i$ ($i = 0$, resp. $i = 1$) ne peut produire un covolume inférieur à la plus basse valeur possible de $\nu_{\mathbf{c}}^n$ (resp. de $\nu_{\mathbf{nc}}^n$) donnée dans le théorème 1.3 (resp. dans le théorème 1.4).

Notre présentation de la preuve est un peu particulière et mérite d'être expliquée. Pour des raisons techniques, il est plus agréable de distinguer les cas $r = 2m+1$ et $r = 2m$, et naturellement les cas $k = \mathbb{Q}$ et $k \neq \mathbb{Q}$. La parité de $m$ joue aussi un rôle lorsque $k = \mathbb{Q}$. Mais il n'y a pas de grande différence conceptuelle entre le traitement de ces différents cas. Ainsi nous nous contenterons de donner les détails de la preuve pour le rang $r = 2m+1$ avec $k \neq \mathbb{Q}$ (cas compact). Chacun des paragraphes §15.1 à §15.7 correspond à une étape bien délimitée de la preuve pour ce cas. Les paragraphes §15.8 et §15.9 montreront comment la démonstration s'adapte pour les cas restants. Pour ceux-ci la routine de plusieurs argumentations nous autorise à ne pas tout détailler, en insistant par contre sur les éléments nouveaux lorsqu'il y en a.

## §15.1 Première borne inférieure pour $\mu(G(\mathbb{R})/\Gamma)$

On suppose jusqu'à la fin du paragraphe §15.7 que $G$ est de rang $r = 2m+1$ et $k \neq \mathbb{Q}$. Ainsi $G$ est de type ${}^2\mathrm{D}_{2m+1}$ et le sous-groupe arithmétique $\Gamma < G(\mathbb{R})$ est cocompact. Comme d'habitude on note par $d$ le degré $[k : \mathbb{Q}]$. Selon la proposition 13.11 (borne pour $[\Gamma : \Lambda]$) et la formule de volume (13.3) pour $\Lambda$, on peut borner comme suit le covolume de $\Gamma$ :

$$\mu(G(\mathbb{R})/\Gamma) \quad \geq \quad \frac{1}{2^{d+1}4^{\#\hat{\mathrm{T}}}h_\ell}\mathscr{D}_k^{r^2-r/2}\mathscr{D}_{\ell|k}^{r-1/2}C(r)^d\mathscr{E}(\mathscr{P}), \tag{15.2}$$

où $\mathscr{P}$ désigne la collection cohérente qui détermine le sous-groupe principal $\Lambda$ dont $\Gamma$ est le normalisateur. Nous allons voir ici qu'on peut simplifier dans cette borne le facteur $4^{-\#\hat{\mathrm{T}}}\mathscr{E}(\mathscr{P})$.

Suivant la notation de [BP89], on définit pour chaque place $v \in V_\mathrm{f} = V_\mathrm{f}(k)$ le facteur $f_v$ comme suit :

$$f_v \quad := \quad \begin{cases} e_v & \text{si } v \in V_\mathrm{f} \smallsetminus \hat{\mathrm{T}}; \\ 4^{-1} \cdot e_v & \text{si } v \in \hat{\mathrm{T}}, \end{cases} \tag{15.3}$$

où

$$e_v \quad := \quad \frac{q_v^{(\dim \overline{\mathrm{M}}_v + \dim \overline{\mathscr{M}}_v)/2}}{\#\overline{\mathrm{M}}_v(\mathbb{F}_v)}$$

sont les facteurs locaux pour lesquels $\mathscr{E}(\mathscr{P}) = \prod_{v\in V_\mathrm{f}} e_v$ (cf. théorème 9.16) et $\hat{\mathrm{T}}$ est défini en 12.5. Il a déjà été contrôlé dans [BP89, Appendix C] qu'on a l'inégalité (plus généralement dans tout groupe absolument simple) :

$$f_v \quad > \quad 1 \qquad (\forall\, v \in V_\mathrm{f}). \tag{15.4}$$

Dans le cas où $G$ est de type $\mathrm{D}_r$, cette affirmation suit facilement de la remarque 9.15 et de (13.6). On déduit immédiatement de (15.4) :

$$\frac{1}{4^{\#\hat{\mathrm{T}}}}\mathscr{E}(\mathscr{P}) \quad > \quad 1, \tag{15.5}$$

et ainsi la borne simplifiée pour le covolume de $\Gamma$ :

$$\mu(G(\mathbb{R})/\Gamma) \quad \geq \quad \frac{1}{2^{d+1}h_\ell}\mathscr{D}_k^{r^2-r/2}\mathscr{D}_{\ell|k}^{r-1/2}C(r)^d. \tag{15.6}$$

## §15.2 Borne supérieure pour $h_\ell$

Afin de rendre la borne (15.6) utilisable, il nous faut borner $h_\ell$ par une expression qui va dépendre du discriminant $\mathscr{D}_\ell$. Le problème général qui consiste à donner une borne supérieure pour $h_\ell$ ne semble pas connaître de réponse pleinement satisfaisante. Il faudra se contenter d'une borne qui est sans doute loin d'être optimale. Notre discussion est largement inspirée de [BP89, §6].

En utilisant certains éléments de la preuve du théorème de Brauer-Siegel [Lan86, Ch. XVI §1], on peut obtenir l'inégalité suivante, donnée dans [BP89, §6 (1)] et valable pour tout $t > 1$ :

$$h_\ell \mathrm{R}_\ell \quad \leq \quad \#\mu(\ell) \cdot t(t-1) 2^{-s_1}\, \Gamma(t/2)^{s_1}\, \Gamma(t)^{s_2} \left(2^{-2s_2} \pi^{-[\ell:\mathbb{Q}]} \mathscr{D}_\ell\right)^{t/2} \zeta_\ell(t),$$

où l'on rappelle que $\mu(\ell)$ désigne le groupe des racines de l'unité dans $\ell$ et $(s_1, s_2)$ est la signature de $\ell$ (en particulier : $s_1 + 2s_2 = [\ell : \mathbb{Q}]$). Ici $\mathrm{R}_\ell$ désigne le *régulateur* de $\ell$ [Lan86, Ch.V §1] et $t \mapsto \Gamma(t)$ est la *fonction Gamma d'Euler* (en particulier $\Gamma(1) = \Gamma(2) = 1$). On remplace $t$ par 2 dans cette inégalité, et en utilisant

$$\zeta_\ell(2) \quad \leq \quad \zeta(2)^{[\ell:\mathbb{Q}]} = \left(\frac{\pi^2}{6}\right)^{[\ell:k]d},$$

valable selon (4.7), on obtient :

$$h_\ell \mathrm{R}_\ell \quad \leq \quad \#\mu(\ell) \cdot 2 \left(\frac{\pi}{12}\right)^{[\ell:k]d} \mathscr{D}_\ell. \tag{15.7}$$

On utilise alors le résultat de [Fri89], qui dit qu'à l'exception de trois corps totalement imaginaires le régulateur doit être $\geq 1/4$. Or selon la proposition 13.7 aucun de ces trois corps exceptionnels ne peut apparaître comme le corps $\ell$ d'un $k$-groupe admissible pour $\mathrm{Isom}^+(\mathbb{H}^n)$. Pour le cas cocompact $k \neq \mathbb{Q}$, on a selon cette même proposition que $\mu(\ell) = \{\pm 1\}$. Ce qui nous donne finalement :

$$h_\ell \quad \leq \quad 16 \left(\frac{\pi}{12}\right)^{2d} \mathscr{D}_\ell. \tag{15.8}$$

On introduit alors l'inégalité (15.8) dans (15.6). En prenant également en considération la proposition 4.21 (dont on tire notamment : $\mathscr{D}_\ell \geq \mathscr{D}_k^2$), on obtient les bornes :

$$\mu(G(\mathbb{R})/\Gamma) \quad \geq \quad \frac{1}{32} \mathscr{D}_k^{r^2 - 5r/2 + 1} \mathscr{D}_\ell^{r - 3/2} a(r)^d \tag{15.9}$$

$$\geq \quad \frac{1}{32} \mathscr{D}_k^{r^2 - r/2 - 2} a(r)^d, \tag{15.10}$$

avec

$$a(r) \quad := \quad \frac{1}{2} \left(\frac{12}{\pi}\right)^2 C(r). \tag{15.11}$$

## §15.3 Le cas des rangs élevés

Pour un $r = 2m + 1$ fixé, la borne (15.10) est adéquate pour comparer le covolume de $\Gamma$ (qu'on suppose atteindre $\nu_{\mathbf{c}}^n$) avec le covolume de $\Gamma_0$. On veut cependant obtenir une preuve pour une infinité de $r$, raison pour laquelle on va rendre la comparaison avec $\Gamma_0$ indépendante du $r$, du moins pour $r$ suffisamment grand.

On observe facilement grâce à sa définition (13.5), que la constante $C(r)$ tend vers l'infini pour $r \to \infty$. Ainsi pour $r$ suffisamment grand la constante

$a(r)$ est supérieure à 1. Plus concrètement on vérifie que $a(r) > 1$ pour $r \geq 15$. Dans ce cas on peut remplacer le facteur $a(r)^d$ par $a(r)^2$ dans (15.9) et (15.10) sans changer la validité des inégalités. Pour des rangs suffisamment grands le degré $d = [k : \mathbb{Q}]$ ne sera donc pas un problème pour notre preuve.

D'après le calcul d'indice (14.10) et la formule (14.7) pour le covolume de $\Lambda_0$, on a la borne supérieure pour $\mu(G_0(\mathbb{R})/\Gamma_0)$ :

$$\mu(G_0(\mathbb{R})/\Gamma_0) \quad \leq \quad \frac{5^{r^2-r/2} \cdot 11^{r-1/2} C(r)^2}{2} \underbrace{L_{\ell_0|k_0}(r) \prod_{j=1}^{r-1} \zeta_k(2j)}_{(*)}, \quad (15.12)$$

le produit $(*)$ dépendant également de $r$. Selon la discussion dans [Bel04, §4 : p.769] on a pour tout $r$ l'inégalité :

$$\prod_{j=2}^{r-1} \zeta(2j) \quad < \quad e^{1/6}. \quad (15.13)$$

On peut alors utiliser les relations (4.7) et (4.8) pour obtenir l'estimation :

$$(*) \quad \leq \quad \zeta_{k_0}(r) \cdot \zeta_{k_0}(2) \cdot e^{1/3}.$$

La fonction $s \mapsto \zeta_{k_0}(s)$ est décroissante sur $s > 1$, ce qui permet de remplacer $\zeta_{k_0}(r)$ par $\zeta_{k_0}(3)$ dans cette borne. Par une évaluation numérique (par exemple sur PARI/GP) on constate qu'on a $(*) < 1.7$ (pour tout $r \geq 3$).

Pour $r \geq 15$ les deux discussions précédentes montrent que la comparaison (15.1) entre les covolumes de $\Gamma$ et $\Gamma_0$ permet l'inégalité :

$$\begin{aligned} \frac{1}{32} \mathscr{D}_k^{r^2-r/2-2} a(r)^2 \quad &\overset{(15.10)}{\leq} \quad \mu(G(\mathbb{R})/\Gamma) \quad (15.14) \\ &\leq \quad \mu(G_0(\mathbb{R})/\Gamma) \quad \leq \quad \frac{1.7}{2} 5^{r^2-r/2} \cdot 11^{r-1/2} C(r)^2, \end{aligned}$$

qui par des transformations élémentaires débouche sur

$$\left( \frac{\mathscr{D}_k}{5 \cdot 11^{1/r}} \right)^{r^2-r/2-2} \quad \leq \quad (1.7) \cdot 64 \left( \frac{\pi}{12} \right)^4 5^2 \cdot 11^{2/r}. \quad (15.15)$$

Ceci donne une borne supérieure pour $\mathscr{D}_k$, la plus mauvaise s'obtenant en posant $r = 15$. Elle suffit pour voir que pour chaque $r \geq 15$ on a $\mathscr{D}_k \leq 5$ (le discriminant est un entier). Le seul corps $k$ totalement réel qui peut respecter cette inégalité au niveau du discriminant est $k = k_0$ (avec $\mathscr{D}_{k_0} = 5$). On peut dès lors remplacer dans (15.14) l'inégalité (15.10) par (15.9) avec $\mathscr{D}_k = 5$, afin d'obtenir une inégalité analogue à (15.15) mais impliquant $\mathscr{D}_\ell$ cette fois-ci. Elle permet de voir avec $r \geq 15$ que $\mathscr{D}_\ell \leq 396$. Selon QAOS (remarque 15.1), il existe trois corps $\ell$ de signature $(2, 1)$ (cf. proposition 13.7) dont le discriminant est borné par cette valeur. Mais seul $\ell = \ell_0$ est une extension de $k_0$. Ainsi dans le cas $r \geq 15$ (cocompact et $r = 2m + 1$), pour que $\Gamma$ réalise le covolume minimal $\nu_{\mathbf{c}}^n$ on doit nécessairement avoir $(k, \ell) = (k_0, \ell_0)$. Pour ce cas le contenu du paragraphe §15.7 suffit à l'achèvement de la démonstration.

**Remarque 15.1.** Pour déterminer les possibilités pour $\ell$, nous interrogeons la base de données QAOS, accessible en ligne à l'adresse :

`http://qaos.math.tu-berlin.de`

Il s'agit d'une base de données contenant pour chaque degré jusqu'à 7 (compris), la liste des corps de nombres jusqu'à une valeur limite du discriminant (valeur limite en fonction du degré). La base de données contient entre autres pour chaque corps la valeur du discriminant (avec signe), la signature et le nombre de classes. Des recherches peuvent notamment être faites en spécifiant la signature et une borne pour le discriminant. Nous aurons fréquemment recours à QAOS dans la suite du chapitre. De telles listes de corps de nombres sont également disponibles dans un format lisible par PARI/GP, à l'adresse

`http://megrez.math.u-bordeaux.fr/pub/numberfields/`

**Remarque 15.2.** Il est assez remarquable que la démonstration de notre théorème est nettement plus aisée dans les dimensions élevées que dans les dimensions basses. C'est là une particularité du cas arithmétique, diamétralement opposé au cas général pour cet aspect (cf. §1.3).

## §15.4 Exclusion des degrés $[k : \mathbb{Q}]$ élevés

Selon le paragraphe qui précède il nous reste à examiner les rangs $r = 3, 5, \ldots, 13$. Pour ceux-ci la constante $a(r)$ définie en (15.11) est inférieure à 1. On ne peut plus alors se débarrasser du $a(r)^d$ qui apparaît dans (15.10) de manière aussi simple qu'en §15.3. On fait ici appel au résultat énoncé dans [Odl90, table 4], qui donne des bornes pour le discriminant $\mathscr{D}_k$ en fonction du degré. On a ainsi pour $k$ totalement réel :

| | |
|---|---|
| $d = 5 :$ | $\mathscr{D}_k \geq (6.5)^d$ |
| $d = 6 :$ | $\mathscr{D}_k \geq (7.9)^d$ |
| $d \geq 7 :$ | $\mathscr{D}_k \geq (9.3)^d$ |

TAB. 15.1 – Bornes d'Odlyzko pour $k$ totalement réel

On vérifie pour $r = 3, 5, \ldots 13$ que $(9.3)^{r^2 - r/2 - 2} a(r) > 1$, ce qui nous permet de voir à partir de (15.10) que si $d \geq 7$ (cf. tableau 15.1), alors

$$\mu(G(\mathbb{R})/\Gamma) \quad > \quad \frac{1}{32} \left( 9.3^{r^2 - r/2 - 2} a(r) \right)^7 . \tag{15.16}$$

En utilisant (15.12) on voit pour chaque $r = 3, 5, \ldots, 13$ que le covolume de $\Gamma_0$ est inférieur à la borne (15.16). On en déduit que pour atteindre le covolume minimal, on doit avoir $d = [k : \mathbb{Q}] \leq 6$.

## §15.5 Examen des $\mathscr{D}_k$ et $\mathscr{D}_\ell$ possibles

Pour chaque rang $r = 3, 5, \ldots, 13$ il reste à examiner les situations $d = 2, 3, 4, 5, 6$. La procédure est la suivante. La comparaison de la borne (15.10) avec (15.12) (où l'on peut vérifier numériquement que $(*) < 1.17$ pour $r = 3, 5, \ldots, 13$) permet d'obtenir pour chaque rang $r$ et chaque degré $d = 2, 3, \ldots, 6$ une borne supérieure pour $\mathscr{D}_k$. Les bornes qu'on obtient pour $\mathscr{D}_k$ sont suffisantes pour exploiter la base de donnée QAOS. On peut pour chaque degré et chaque rang lister les corps $k$ totalement réel pour lequel $\Gamma$ peut encore espérer avoir un covolume inférieur à celui de $\Gamma_0$. L'idée est d'ensuite utiliser l'inégalité (15.9) pour trouver pour chaque $r, d$ et $\mathscr{D}_k$ encore possibles une borne supérieure pour $\mathscr{D}_\ell$, qui doit nous permettre d'obtenir une liste de corps $\ell$ possibles, et dont on peut obtenir la valeur $h_\ell$. Le maximum de ces valeurs $h_\ell$ est sensiblement inférieur à la borne donnée par (15.8), et l'on a avantage avec cette connaissance à revenir à l'inégalité (15.6). On applique alors la même procédure que précédemment pour borner $\mathscr{D}_k$ et $\mathscr{D}_\ell$ avec cette meilleure borne pour $\mu(G(\mathbb{R})/\Gamma)$. Pour les cas $r = 5, 7, \ldots, 13$ tout peut se faire à l'aide de QAOS, pour obtenir finalement $\mathscr{D}_k = 5$ et $\mathscr{D}_\ell = 275$. Le cas $r = 3$ demande plus d'effort, et nous allons donc le détailler.

Soit donc $r = 3$. Grâce au bornes (15.10) et (15.12) (avec $(*) < 1.17$) on obtient à partir de la comparaison (15.1) pour chaque degré $d = 2, \ldots, 6$ une borne supérieure pour $\mathscr{D}_k$ :

$$\begin{aligned} d = 2 &\quad : \quad \mathscr{D}_k \leq 22; \\ d = 3 &\quad : \quad \mathscr{D}_k \leq 198; \\ d = 4 &\quad : \quad \mathscr{D}_k \leq 1\,778; \\ d = 5 &\quad : \quad \mathscr{D}_k \leq 15\,956; \\ d = 6 &\quad : \quad \mathscr{D}_k \leq 143\,195. \end{aligned}$$

En interrogeant QAOS on obtient la liste complète des corps $k$ totalement réel dont le discriminant respecte la borne donnée ci-dessus. Nous donnons dans le tableau 15.2 la liste des discriminants $\mathscr{D}_k$ de ces corps. Pour tous ces cas le discriminant $\mathscr{D}_k$ détermine uniquement le corps $k$. Pour chacun de ces degrés $d$, en remplaçant $\mathscr{D}_k$ dans (15.9) par sa plus petite valeur possible (5 pour $d = 2$, 49 pour $d = 3$, etc.), on obtient par comparaison avec la borne (15.12) une borne supérieure pour $\mathscr{D}_\ell$. Pour les degrés $d = 2, 3$ on peut vérifier avec QAOS que tous les corps $\ell$ possibles (avec signature donnée par la proposition 13.7) possèdent un nombre de classes $h_\ell$ égal à 1. Mais contrairement aux cas $r = 5, 7, \ldots, 13$, notre liste intermédiaire de possibilités pour $k$ contient des corps de degrés $d \geq 4$, pour lesquels on a $[\ell : \mathbb{Q}] > 7$. On sort alors des limites de la base de données QAOS (et des bases de données disponibles pour PARI/GP).

Pour poursuivre notre preuve sans disposer d'une meilleure borne que (15.8) pour $h_\ell$, il nous est essentiel de pouvoir lister les extensions $\ell|k$ possibles, afin de connaître les valeurs qui peuvent apparaître pour $h_\ell$. Or, l'extension $\ell|k$ est quadratique et donc abélienne, et la *théorie des corps de classes* [Neu99, Ch.VI] classifie les extensions abéliennes d'un corps $k$ fixé. Il est donc théoriquement possible d'obtenir pour chacun des quatre corps $k$ avec $d = 4, 5$ du tableau 15.2, une liste des $\ell$ possibles. Pour être candidat un corps $\ell$ doit avoir la signature

| $[k:\mathbb{Q}]$ | $\mathscr{D}_k$ |
|---|---|
| $d=2$ | 5, 8, 12, 13, 17, 21 |
| $d=3$ | 49, 81, 148, 169 |
| $d=4$ | 725, 1 125, 1 600 |
| $d=5$ | 14 641 |
| $d=6$ | – |

TAB. 15.2 – Première liste finie des $\mathscr{D}_k$ possibles pour $r=3$

donnée par la proposition 13.7, et doit posséder un discriminant inférieur à la borne qu'on obtient pour $\mathscr{D}_\ell$ en comparant (15.9) (où la valeur $\mathscr{D}_k$ est déterminée par le choix de $k$) avec le covolume de $\Gamma_0$. Les aspects algorithmiques qui permettent une résolution concrète du problème de lister les extensions $\ell|k$ possibles, sont expliqués dans [Coh00, Ch. 4]. Nous pouvons utiliser PARI/GP, où sont implémentées toutes les procédures nécessaires[1], pour obtenir la liste des corps $\ell$ possibles dans notre cas. Nous trouvons que pour le corps $k$ de degré $d=5$, aucune extension $\ell|k$ ne satisfait aux conditions. Il en est de même pour les deux cas quartiques $\mathscr{D}_k = 1\,125$ et $\mathscr{D}_k = 1\,600$. Il existe par contre pour $\mathscr{D}_k = 725$ deux corps $\ell$ de signature $(2,3)$ respectant la borne obtenue pour $\mathscr{D}_\ell$. Ces deux corps sont donnés par les polynômes :

$$x^8 - x^7 + x^6 - 2x^5 + x^4 - 2x^3 + x^2 - x + 1;$$
$$x^8 - 2x^7 + 2x^6 - 3x^5 + 3x^4 - 3x^3 + 2x^2 - 2x + 1.$$

Toujours avec PARI/GP on peut alors contrôler que ces deux corps possèdent un nombre de classes $h_\ell$ égal à 1.

**Remarque 15.3.** Il vaut la peine de relever le caractère général de cette dernière technique exposée pour obtenir une liste de corps $\ell$ possibles. En effet, à la seule exception du type ${}^6\mathrm{D}_4$, l'extension $\ell|k$ associée à un $k$-groupe semi-simple est galoisienne et de degré au plus 3. Ainsi pour tous ces cas $\ell|k$ est une extension abélienne. Pour un corps $k$ fixé, après l'obtention d'une borne supérieure pour $\mathscr{D}_\ell$ on peut en déduire une liste de $\ell$ possibles. Pour obtenir une liste de corps $k$ permettant d'atteindre une certaine valeur minimale pour le covolume il faut par contre pouvoir exclure les cas $d = [k:\mathbb{Q}] > 7$, afin de pouvoir utiliser les bases de données de corps de nombres.

Pour toutes les possibilités restantes pour $(k,\ell)$ on a $h_\ell = 1$, information que l'on insère dans (15.6) pour obtenir une meilleure borne inférieure pour $\mu(G(\mathbb{R})/\Gamma)$. Ceci permet en comparant avec le covolume de $\Gamma_0$ d'obtenir de meilleures bornes pour $\mathscr{D}_k$. Les possibilités sont alors réduites à $\mathscr{D}_k = 5, 8, 12$ (pour $d=2$) et $\mathscr{D}_k = 49$ (pour $d=3$). Pour chacun de ces discriminants on déduit de même une borne pour $\mathscr{D}_\ell$, qui nous laisse finalement avec les trois possibilités $\mathscr{D}_\ell = 275, 400, 475$, toutes avec $k = k_0$.

[1] Nous remercions Henri Cohen, qui en réponse à un courrier nous a éclairé sur ce point.

## §15.6 Calcul d'indice pour les derniers cas

Pour le cas $r = 3$ le processus d'optimisation des bornes pour $\mathscr{D}_\ell$ ne permet pas d'exclure les possibilités $\mathscr{D}_\ell = 400$ et $\mathscr{D}_\ell = 475$. Pour ce faire il faut calculer pour ces cas particuliers une meilleure borne pour l'indice $[\Gamma : \Lambda]$ que ne donne la proposition 13.11. Le calcul s'effectue de façon similaire à ce qui est fait dans §14.2 pour $[\Gamma_0 : \Lambda_0]$ avec $r = 2m + 1$.

Les données pour le calcul sont les suivantes. Les deux corps $\ell$ avec $\mathscr{D}_\ell = 400$ et $\mathscr{D}_\ell = 475$ sont donnés par $\ell = k_0(\sqrt{\omega})$ et $\ell = k_0(\sqrt{\beta})$, avec

$$\omega = \frac{1+\sqrt{5}}{2} \quad \text{et} \quad \beta = -1 + 2\sqrt{5}.$$

Un système d'unités fondamentales est donné respectivement par $\{\sqrt{\omega}, 1+\sqrt{\omega}\}$ et $\left\{\frac{1+\sqrt{\beta}}{2}, \frac{1-\sqrt{\beta}}{2}\right\}$. Ces informations permettent de calculer (de façon tout à fait analogue à ce qui est fait en §14.2 avec $\ell_0$) pour chacun de ces deux cas :

$$\#\mathbf{A}_4/(\ell^\times)^4 \quad = \quad 4.$$

D'après la discussion en §13.5 on peut en déduire la nouvelle borne $[\Gamma : \Lambda] \leq 4 \cdot 4^{\#\hat{\mathrm{T}}}$, qui présente une amélioration d'un facteur $1/2$ par rapport à la proposition 13.11. Ceci améliore pour ces cas la borne inférieure (15.6) pour le covolume de $\Gamma$, dont on peut à présent vérifier qu'il dépasse celui de $\Gamma_0$.

## §15.7 Preuve lorsque $(k, \ell) = (k_0, \ell_0)$

On termine dans ce paragraphe la preuve du cas cocompact ($k \neq \mathbb{Q}$) avec $r = 2m+1$. Selon les paragraphes précédents, pour que le covolume $\Gamma$ atteigne $\nu_{\mathbf{c}}^n$ on doit nécessairement avoir $(k, \ell) = (k_0, \ell_0)$. On observe alors que le covolume de $\Gamma$ ne peut différer de celui de $\Gamma_0$ que par l'indice $[\Gamma : \Lambda]$ et les facteurs lambda $\prod_{v \in \mathrm{T}} \lambda_v$ qui apparaissent éventuellement dans le covolume de $\Lambda$. Plus précisément, on considère le quotient :

$$\begin{aligned} \frac{\mu(G(\mathbb{R})/\Gamma)}{\mu(G_0(\mathbb{R})/\Gamma_0)} &= \frac{[\Gamma_0 : \Lambda_0]}{[\Gamma : \Lambda]} \prod_{v \in \mathrm{T}} \lambda_v \\ &\geq \frac{2}{4 \cdot 4^{\#\hat{\mathrm{T}}}} \prod_{v \in \mathrm{T}} \lambda_v, \end{aligned} \tag{15.17}$$

la borne $[\Gamma : \Lambda] \leq 4 \cdot 4^{\#\hat{\mathrm{T}}}$ se déduisant du calcul de $\mathbf{A}_4/(\ell_0^\times)^4$ (effectué en §14.2) et de la borne (12.15) pour l'entier $q$ pour $\Gamma$. Par définition, pour chaque place $v \in \hat{\mathrm{T}}$, le groupe $G|k_v$ n'est pas quasi-déployé et ainsi un facteur $\lambda_v$ doit apparaître. En d'autres termes : $\hat{\mathrm{T}} \subset \mathrm{T}$. Comme selon la remarque 13.9 on a $\lambda_v > 1$, l'inégalité (15.17) nous donne :

$$\mu(G(\mathbb{R})/\Gamma) \quad \geq \quad \frac{1}{2} \left( \prod_{v \in \hat{\mathrm{T}}} 4^{-1} \lambda_v \right) \mu(G_0(\mathbb{R})/\Gamma_0). \tag{15.18}$$

Il se trouve que les deux nombres premiers 2 et 3 sont inertes dans l'extension $k_0|\mathbb{Q}$. Ainsi pour le cas $k = k_0$, la cardinalité $q_v = [\mathbb{F}_v : \mathbb{F}_p]$ (où $v|p$) est toujours plus grande que $q_{(2)} = 4$. Pour $v \in \hat{\mathrm{T}}$, l'inégalité (13.8) pour $\lambda_v$ reste alors valable en remplaçant $q_v$ par 4. Avec $r \geq 3$ on obtient que $\lambda_v \geq 18$ pour tout $v \in \hat{\mathrm{T}}$. Cela est largement suffisant pour voir dans (15.18) que la seule situation où $\Gamma$ peut avoir un covolume inférieur ou égal à $\Gamma_0$ est lorsque $\hat{\mathrm{T}} = \emptyset$ (c'est la situation de $\Gamma_0$, selon la proposition 14.2). Mais dans ce cas l'indice $[\Gamma : \Lambda]$ vaut soit 2 soit 4 (même raisonnement que pour $[\Gamma_0 : \Lambda_0]$). Le covolume de $\Lambda$ est lui égal au covolume de $\Lambda_0$. Donc $\Gamma$ qui atteint le covolume minimal $\nu_{\mathbf{c}}^n$ est pour $r = 2m+1$ soit de même covolume que $\Gamma_0$, soit de covolume deux fois plus petit que celui de $\Gamma_0$ (cas avec $[\Gamma : \Lambda] = 4$ et $[\Gamma_0 : \Lambda_0] = 2$). Cela avec (13.2) achève la démonstration du théorème 1.3 lorsque $r = 2m + 1$.

**Remarque 15.4.** Notre preuve montre que $G$ doit être un $k_0$-groupe qui est isomorphe à $G_0$ sur chaque complété de $k_0$. Ceci permet facilement de voir que le covolume de $\Lambda$ est égal au covolume de $\Lambda_0$. Afin de voir que $[\Gamma : \Lambda] = [\Gamma_0 : \Lambda_0]$, il faut en plus pouvoir montrer que $G$ est $k_0$-isomorphe à $G_0$. Au vu de la propriété singulière donnée dans la proposition 14.2 nous pensons qu'un tel résultat d'unicité pour $G_0$ doit être valable, et les auteurs de [BE] s'efforceront de faire figurer une preuve pour ceci dans la version finale de l'article. Cela permettrait de ramener la question de la détermination de $N_0(r)$ au calcul précis de $[\Gamma_0 : \Lambda_0]$, lequel est envisageable selon notre remarque 14.4.

**Remarque 15.5.** L'unicité de $G_0$ proposée dans la remarque précédente ne suffit pas à prouver l'unicité (à isométrie près) du quotient arithmétique réalisant le volume minimal $\nu_{\mathbf{c}}^n$. La construction du sous-groupe arithmétique $\Gamma_0$ (et plus généralement celle de $\Gamma^{\mathfrak{m}}$ en §12.3) contient en effet une ambiguïté : en précisant le type global du sous-groupe arithmétique principal $\Lambda_0$ (ou $\Lambda^{\mathfrak{m}}$) on ne détermine pas ce groupe de façon unique (il y a une infinité de sous-groupes parahoriques d'un même type donné). Pour prouver l'unicité du quotient réalisant $\nu_{\mathbf{c}}^n$, il faut en plus de l'unicité de $G_0$, pouvoir montrer que les images dans $\mathrm{Isom}^+(\mathbb{H}^n)$ de tous les sous-groupes arithmétiques de la forme de $\Gamma^{\mathfrak{m}} = N_{G_0(\mathbb{R})}(\Lambda^{\mathfrak{m}})$ (pour un sous-groupe arithmétique principal $\Lambda^{\mathfrak{m}}$ de covolume minimal) sont conjuguées entre elles dans $\mathrm{Isom}^+(\mathbb{H}^n)$. La méthode pour aborder ce problème apparaît dans [Bel07] (pour les dimensions paires) ; elle est basée sur le concept de *nombre de classes d'un groupe algébrique.*

## §15.8 Preuve du cas compact de rang pair

Nous supposons à présent que le $k$-groupe $G$ est de rang $r = 2m$, toujours avec $k \neq \mathbb{Q}$. On traite donc les rangs restants pour compléter la preuve du théorème 1.3. Comme annoncé en début de chapitre, nous allons nous passer de présenter en détails les éléments de preuve qui sont analogues au cas $r = 2m+1$. Le cas du rang pair voit apparaître pour $r = 4$ les formes trialitaires comme possibilités de groupes admissibles pour $\mathrm{Isom}^+(\mathbb{H}^7)$. Notre preuve va montrer, en fin de paragraphe, que celles-ci ne sont pas responsables pour le volume minimal. Pour l'instant nous supposerons (pour $r = 4$) que $G$ n'est pas une forme trialitaire.

La principale différence entre le cas $r = 2m + 1$ et $r = 2m$ pour la borne de l'indice $[\Gamma : \Lambda]$ (proposition 13.11) est l'apparition du facteur $2^{\#\mathscr{R}}$ lorsque $r = 2m$. On fait alors usage de l'inégalité :

$$2^{\#\mathscr{R}} \quad \leq \quad \mathscr{D}_{\ell|k}, \tag{15.19}$$

qu'on obtient par [Pra89, Appendix : theorem A], à l'aide de la remarque 12.6. Grâce à ceci et à la discussion dans §15.1 pour éliminer $4^{-\#\hat{\mathrm{T}}}$, on peut obtenir une première borne inférieure pour $\mu(G(\mathbb{R})/\Gamma)$ similaire à (15.6) (mais a priori un peu moins bonne). La discussion de §15.2 pour borner $h_\ell$ est valable dans le cas $r = 2m$ ; en particulier on peut utiliser la même inégalité (15.8). Il en découle pour une constante $a(r)$ analogue à (15.11) des bornes correspondantes à (15.9) et (15.10). Tout comme dans §15.3 on peut alors par comparaison avec $\mu(G_0(\mathbb{R})/\Gamma_0)$ facilement prouver pour les rangs élevés (plus exactement pour $r \geq 16$) qu'on doit avoir $(k, \ell) = (k_0, \ell_0)$.

On travaille alors avec les cas $r = 4, \ldots, 14$. Pour chacun d'entre eux on montre comme dans §15.4, grâce à la borne d'Odlyzko $\mathscr{D}_k \geq (6.5)^d$ si $d \geq 5$ (cf. tableau 15.1), que le groupe $G$ doit être défini sur $k$ avec $d = [k : \mathbb{Q}] \leq 4$. Pour chaque $r$ et chaque $d$ on utilise alors la borne inférieure pour $\mu(G(\mathbb{R})/\Gamma)$ impliquant $\mathscr{D}_k$ (resp. $\mathscr{D}_k$ et $\mathscr{D}_\ell$) pour déduire en comparant avec le covolume de $\Gamma_0$ des bornes supérieures pour $\mathscr{D}_k$ et $\mathscr{D}_\ell$. Ces bornes sont toutes suffisantes pour obtenir de QAOS une liste finie de possibilités pour $(k, \ell)$ (avec $\ell$ qui doit avoir la signature donnée par la proposition 13.7). Comme c'était le cas avec $r = 3$ pour les rangs impairs, c'est ici pour $r = 4$ que la liste est la plus étendue. Dans cette liste on a toujours $h_\ell \leq 2$, et l'on revient à la borne pour le covolume de $\Gamma$ impliquant $h_\ell$ pour avoir une estimation plus précise. Ceci donne de meilleures bornes supérieures pour $\mathscr{D}_k$ et $\mathscr{D}_\ell$, écartant plusieurs possibilités pour $(k, \ell)$. En particulier dans cette liste épurée on a $h_\ell = 1$. A nouveau, en améliorant les bornes pour $\mathscr{D}_k$ et $\mathscr{D}_\ell$, ceci écarte plusieurs possibilités, ne laissant que $k = k_0$, et $\mathscr{D}_\ell = 275, 400, 475$ ou $775$ (pour $r = 4$, qui comme pour $r = 3$, est le cas le plus fastidieux).

Pour tous ces quatre corps $\ell$ restant on a $\#\mathscr{R} = 1$ (on peut le voir à l'aide du théorème 4.22), ce qui nous permet d'éviter la borne grossière (15.19) et d'améliorer encore la borne supérieure pour $\mathscr{D}_\ell$. On constate alors que pour les cas $\mathscr{D}_\ell = 475$ et $\mathscr{D}_\ell = 775$, le sous-groupe $\Gamma$ ne peut atteindre un covolume inférieur à celui de $\Gamma_0$. Pour le cas $\mathscr{D}_\ell = 400$ on doit procéder (pour $r = 4$) comme dans §15.6 au calcul de l'indice $[\Gamma : \Lambda]$. On calcule que $\#\mathbf{A}_2/(\ell^\times)^2 = 2$, ce qui permet l'amélioration $[\Gamma : \Lambda] \leq 4 \cdot 4^{\#\hat{\mathrm{T}}}$. Avec cela on peut exclure cette dernière possibilité $\mathscr{D}_\ell = 400$. Ainsi on doit avoir $k = k_0$ et $\ell = \ell_0$ pour atteindre le covolume minimal $\nu_{\mathbf{c}}^n$.

La fin de la preuve (formes trialitaires exclues), correspondante à §15.7, est tout à fait analogue au cas $r = 2m + 1$. En particulier les calculs en §14.2 montrent que la borne $[\Gamma : \Lambda] \leq 4 \cdot 4^{\#\hat{\mathrm{T}}} (= 2 \cdot 2^{\#\mathscr{R}} 4^{\#\hat{\mathrm{T}}})$ est également valable pour $r = 2m$, où l'on suppose désormais que $(k, \ell) = (k_0, \ell_0)$. L'inégalité (15.18) est alors aussi respectée. On en déduit que $\mu(G(\mathbb{R})/\Gamma)$ ne peut pas contenir de facteurs lambda s'il atteint $\nu_{\mathbf{c}}^n$, et qu'ainsi $G$ doit être quasi-déployé sur chaque complété non archimédien de $k_0$. Il s'ensuit que $\mu(G(\mathbb{R})/\Gamma)$ est au mieux la moitié de $\mu(G_0(\mathbb{R})/\Gamma_0)$. Les remarques 15.4 et 15.5 ont la même pertinence ici que pour le cas $r = 2m + 1$.

Il reste pour achever complètement la preuve du théorème 1.3 à exclure que

le volume minimal $\nu_{\mathbf{c}}^7$ est atteint à l'aide de formes trialitaires. Supposons donc que $G$ (dont $\Gamma$ est supposé atteindre $\nu_{\mathbf{c}}^7$) est de type ${}^{3,6}\mathrm{D}_4$. Comme $[\ell : k] = 3$, selon (15.7) on a la borne $h_\ell \leq 16(\pi/12)^{3d}\mathscr{D}_\ell$. De manière tout à fait similaire aux cas précédemment traités (en utilisant aussi l'inégalité (15.19)), on obtient des bornes inférieures pour $\mu(G(\mathbb{R})/\Gamma)$ analogues à (15.8) et (15.9). Il faut faire attention d'utiliser ici l'égalité $\mathscr{D}_{\ell|k} = \mathscr{D}_\ell/\mathscr{D}_k^3$. Pour $d = [k : \mathbb{Q}] \geq 5$ la borne d'Odlyzko $\mathscr{D}_k \geq (6.5)^d$ suffit à voir que le covolume de $\Gamma_0$ est plus petit que celui de $\Gamma$. Pour $d = 2, 3$ et 4 on compare $\mu(G(\mathbb{R})/\Gamma)$ avec $\mu(G_0(\mathbb{R})/\Gamma_0)$ pour obtenir des bornes supérieures pour $\mathscr{D}_k$ et $\mathscr{D}_\ell$. Pour $d = 4$ aucun corps ne peut respecter la condition obtenue sur $\mathscr{D}_k$. Pour $d = 2$ et $d = 3$ plusieurs possibilités de corps $k$ apparaissent et avec $\mathscr{D}_k = 5$ (pour $d = 2$) et $\mathscr{D}_k = 49$ (pour $d = 3$) on obtient les plus mauvaises bornes pour $\mathscr{D}_\ell$ :

$$\begin{aligned} d = 2 \quad &: \quad \mathscr{D}_\ell \leq 445\,619; \\ d = 3 \quad &: \quad \mathscr{D}_\ell \leq 7.7 \cdot 10^6. \end{aligned}$$

Pour exclure le cas $d = 3$ on utilise une borne d'Odlyzko disponible sur [Odl]. Dans ces tables, la deuxième colonne du tableau 2 donne une borne de discriminant (en fonction du degré) valable pour tout corps de nombres. Notamment pour le degré $[\ell : \mathbb{Q}] = 9$ on a : $\mathscr{D}_\ell \geq (6.1)^9$. C'est plus grand que notre borne supérieure pour $\mathscr{D}_\ell$, ce qui exclut le cas $d = 3$. Pour le degré $d = 2$ on a $[\ell : \mathbb{Q}] = 6$, ce qui permet l'utilisation de QAOS. Dans la liste des possibilités pour $\ell$ qu'on obtient (avec la condition que $\ell$ possède au moins un plongement réel selon 13.7), on a toujours $h_\ell = 1$. Ceci améliore la borne : $\mathscr{D}_\ell \leq 20\,165$, et pour celle-ci il n'existe aucun $\ell$ satisfaisant. Les sous-groupes arithmétiques des formes trialitaires admissibles possèdent donc tous un covolume supérieur à celui de $\Gamma_0$.

## §15.9 Preuve du cas non compact

Le cas non compact (théorème 1.4) est sensiblement plus simple que le cas compact. On a en effet ici $k = \mathbb{Q}$ et la preuve se réduit pour l'essentiel à prouver que $\ell = \ell_1$. Pour le rang $r = 2m + 1$ avec $m$ impair, l'apparition d'un facteur lambda est par contre une nouveauté par rapport au cas compact. Dans ce paragraphe le $\mathbb{Q}$-groupe $G$ est tel qu'un de ses sous-groupes arithmétiques $\Gamma$ atteint le covolume minimal $\nu_{\mathbf{nc}}^n$. On rappelle (cf. point 13.3) que $G$ est nécessairement de la forme $G = \mathrm{Spin}_f$ pour une forme quadratique $f$ (définie sur $\mathbb{Q}$), et que $G$ ne peut pas être une forme trialitaire.

On commence par le cas le plus facile : $r = 2m + 1$ avec $m$ pair (et donc $r \geq 5$). Il s'agit dans un premier temps de prouver que $\ell = \mathbb{Q}$. Supposons que ce ne soit pas le cas (i.e. $G$ est une forme externe). La proposition 13.7 montre alors que $\ell$ est un corps quadratique réel. Ainsi $\mu(\ell) = \{\pm 1\}$ et selon (15.7) la borne (15.8) pour $h_\ell$ est valable dans notre situation. Tout comme dans §15.1 on peut utiliser l'inégalité $4^{-\#\hat{\mathrm{T}}}\mathscr{E}(\mathscr{P}) > 1$. Avec la borne pour l'indice $[\Gamma : \Lambda] \leq 8 \cdot 4^{\#\hat{\mathrm{T}}} h_\ell$ donnée dans la proposition 13.11 et la formule (13.3) pour le covolume de $\Lambda$, on obtient :

$$\mu(G(\mathbb{R})/\Gamma) \quad \geq \quad \frac{1}{8 \cdot 16} \left(\frac{12}{\pi}\right)^2 \mathscr{D}_\ell^{r-3/2} C(r). \tag{15.20}$$

La comparaison (15.1) entre le covolume de $\Gamma$ et celui de $\Gamma_1$ (donné par (14.13) et (14.16)) permet alors l'inégalité :

$$\frac{1}{128}\left(\frac{12}{\pi}\right)^2 \mathscr{D}_\ell^{r-3/2} \quad \leq \quad \underbrace{\zeta(r)\prod_{j=1}^{r-1}\zeta(2j)}_{(**)}. \tag{15.21}$$

Grâce à (15.13) on obtient la borne

$$(**) \ < \ \zeta(9)\zeta(2)e^{1/6} \ < \ 2,$$

valable pour chaque $r \geq 9$. Pour $r = 5$ on calcule directement (numériquement) que $(**) < 2$. L'inégalité (15.21) (avec $r \geq 5$) donne alors la borne $\mathscr{D}_\ell \leq 2$, ce qui montre que $\ell = \mathbb{Q}$. Ainsi $G$ ne peut pas être une forme externe. On suppose donc à présent que $G$ est une forme interne. Il nous faut voir que $\hat{\mathrm{T}} = \emptyset$. Comme $G = \mathrm{Spin}_f$, il y a exactement trois possibilités pour $G|\mathbb{Q}_p$, chacune donnée par (14.4). En particulier si $v = (p) \in \hat{\mathrm{T}}$, alors $G|\mathbb{Q}_p$ ne peut être que l'unique forme interne non déployée. De plus le sous-groupe arithmétique $\Gamma$ est supposé être de covolume minimal, ce qui selon la proposition 12.4 implique que les sous-groupes parahoriques qui déterminent $\Lambda$ sont tous spéciaux. Il en résulte que pour chaque $v = (p) \in \hat{\mathrm{T}}$ on a l'unique possibilité :

$$\lambda_v \quad = \quad \frac{(p^r-1)(p^{r-1}-1)}{p+1}, \tag{15.22}$$

le calcul s'effectuant comme pour (14.14), mais avec $v = (p)$, plutôt que $v = (2)$. On observe avec $p \geq 2$ et $r \geq 3$ que $4^{-1}\lambda_v > 1$, et ainsi $\mu(G(\mathbb{R})/\Gamma)$ ne peut être inférieur à $\mu(G_1(\mathbb{R})/\Gamma_1)$ (ces deux volumes ne différant que par l'indice $[\Gamma : \Lambda] \leq 4^{\#\hat{\mathrm{T}}}$ et les facteurs lambda). Cela termine la preuve du théorème 1.4 pour le cas $r \equiv 1(4)$.

On traite à présent le cas $r = 2m+1$ avec $m$ impair. Il se distingue du cas précédent essentiellement par l'apparition dans le covolume de $\Gamma_1$ du facteur non trivial $\lambda_2$, donné par (14.14). De plus cette fois $[\Gamma_1 : \Lambda_1] \geq 2$. Ainsi dans l'inégalité (15.21) le terme sur la droite doit être remplacé par le produit entre $\lambda_2/2$ et $(**)$. Comme précédemment, on peut montrer que $(**) < 2$ pour tout $r \geq 7$. Par contre ce n'est pas le cas avec $r = 3$, où l'évaluation numérique nous donne toutefois $(**) < 2.2$. Le facteur lambda peut lui facilement être borné par $\lambda_2 < \frac{4^{r-1/2}}{3}$. Pour $r \geq 7$, cela nous donne :

$$\left(\frac{\mathscr{D}_\ell}{4}\right)^{r-3/2} \quad \leq \quad 512\left(\frac{\pi}{2}\right)^2,$$

dont on obtient : $\mathscr{D}_\ell \leq 6$. Cela nous limite aux possibilités $\mathscr{D}_\ell = 1$ et $\mathscr{D}_\ell = 5$. En particulier on peut remplacer la borne pour $h_\ell$ par la valeur $h_\ell = 1$. Ceci donne l'amélioration $\mathscr{D}_\ell \leq 4$, suffisante pour prouver que $G$ doit être une forme interne (i.e. $\ell = \mathbb{Q}$). On procède de la même façon pour $r = 3$ avec la valeur précise $\lambda_2 = 7$ et la borne $(**) < 2.2$. Dans ce cas la borne qu'on obtient pour $\mathscr{D}_\ell$ n'est pas suffisante pour exclure le cas $\mathscr{D}_\ell = 5$, qu'il nous faut examiner plus en détail. Pour cela, on remarque que comme pour le cas $r = 2m+1$ avec $m$ pair, si $v \in \hat{\mathrm{T}}$ alors le facteur lambda qui apparaît dans la formule du covolume de $\Gamma$

doit être de la forme (15.22). Là aussi on peut facilement voir que $4^{-1}\lambda_v > 1$. Ce qui montre (avec $h_\ell = 1$) que

$$\begin{aligned}\mu(G(\mathbb{R})/\Gamma) &\geq \frac{1}{8\cdot 4^{\#\hat{\mathrm{T}}}}\mathscr{D}_\ell^{r-1/2}C(r)\left(\prod_{v\in\hat{\mathrm{T}}}\lambda_v\right)L_{\ell|\mathbb{Q}}(r)\prod_{j=1}^{r-1}\zeta(2j)\\ &> \frac{1}{8}\mathscr{D}_\ell^{r-1/2}C(r)L_{\ell|\mathbb{Q}}(r)\prod_{j=1}^{r-1}\zeta(2j). \qquad (15.23)\end{aligned}$$

Pour le cas $\ell = \mathbb{Q}(\sqrt{5})$ (i.e. $\mathscr{D}_\ell = 5$) et $r = 3$, nous pouvons calculer en évaluant $L_{\ell|\mathbb{Q}}(r)$ sur PARI/GP que cette dernière borne est supérieure au covolume de $\Gamma_1$. Pour ce cas $r = 3$ on a donc aussi $\ell = \mathbb{Q}$. Il reste alors à voir que pour $G$ une forme interne, son sous-groupe arithmétique $\Gamma$ ne peut avoir un covolume inférieur à celui de $\Gamma_1$. On utilise pour cela le fait que $G = \mathrm{Spin}_f$. Comme $G$ est admissible, on calcule que l'invariant de Hasse $\mathrm{H}_\infty(f)$ à la place infinie doit être égale à $-1$. La formule du produit pour l'invariant de Hasse montre alors que $\mathrm{H}_v(f) = -1$ pour au moins une place $v = (p) \in V_{\mathrm{f}}$. Selon la discussion en §14.1 (cf. également la preuve de 14.5), pour cette place le groupe $G|\mathbb{Q}_p$ n'est pas déployé (et donc non plus quasi-déployé : $G$ est une forme interne). Ainsi il apparaît au moins un facteur lambda dans le covolume de $\Gamma$ (nécessairement pour une place de $\hat{\mathrm{T}}$). Or on observe facilement que pour chaque $v \neq (2) \in \hat{\mathrm{T}}$, on a $4^{-1}\lambda_v > 2\lambda_2$. Même si $[\Gamma : \Lambda] = 4$ (maximum possible selon §14.3) et $[\Gamma_1 : \Lambda_1] = 2$, on voit donc qu'un facteur lambda ailleurs qu'en $v = (2)$ implique un covolume plus grand que celui de $\Gamma_1$. Le covolume minimal est ainsi atteint avec $\hat{\mathrm{T}} = \{(2)\}$, comme pour $\Gamma_1$. Cela achève le cas $r = 2m + 1$.

Soit à présent $G$ de rang $r = 2m$ (avec $r \geq 4$), avec comme toujours $\Gamma < G(\mathbb{R})$ qui réalise le covolume minimal $\nu^n_{\mathbf{nc}}$. Comme il est admissible, $G$ doit être de type ${}^2\mathrm{D}_{2m}$. On cherche comme d'habitude à montrer que $\ell = \ell_1$ (ici $\ell_1 = \mathbb{Q}(\sqrt{-3})$). D'après la proposition 13.7 le corps $\ell$ est un corps quadratique imaginaire. Ainsi $\mu(\ell)$ peut contenir plus que deux éléments. Mais c'est le cas pour l'unique exception $\ell = \mathbb{Q}(\sqrt{-1})$, pour laquelle $h_\ell = 1$. En particulier on voit à partir de (15.7) que la borne (15.8) pour $h_\ell$ reste correcte ici (avec $d = 2$). Avec la borne pour l'indice $[\Gamma : \Lambda]$ donnée dans la proposition 13.11, et l'utilisation des inégalités (15.5) et (15.19), on a :

$$\mu(G(\mathbb{R})/\Gamma) \geq \frac{1}{64}\left(\frac{12}{\pi}\right)^2\mathscr{D}_\ell^{r-5/2}C(r). \qquad (15.24)$$

Le covolume de $\Gamma_1$ respecte lui (cf. §14.3) :

$$\mu(G_1(\mathbb{R})/\Gamma_1) \leq \frac{1}{2}3^{r-1/2}C(r)\underbrace{L_{\ell_1|\mathbb{Q}}(r)\prod_{j=1}^{r-1}\zeta(2j)}_{(***)}. \qquad (15.25)$$

De manière analogue à ce qui a été fait pour $(*)$ et $(**)$, on peut montrer que pour chaque $r \geq 4$ on a $(***) < 2$. Avec ceci la comparaison entre (15.24) et (15.25) donne la borne $\mathscr{D}_\ell \leq 13$ (obtenue avec le « pire cas » $r = 4$). Pour les corps $\ell$ possibles (on consulte par exemple QAOS), on a toujours $\#\mathscr{R} = 1$ et $h_\ell = 1$. Ceci améliore l'inégalité (15.24), dont on tire une nouvelle borne pour

$\mathscr{D}_\ell$. Pour $r \geq 6$ cela suffit à montrer que $\mathscr{D}_\ell = 3$ (i.e $\ell = \ell_1$). Pour $r = 4$, il nous reste en plus la possibilité $\mathscr{D}_\ell = 4$. Pour ce dernier cas $\ell = \mathbb{Q}(\sqrt{-1})$, on calcule facilement que $\#\mathbf{A}_2/(\ell^\times)^2 = 2$ (ici d'après la proposition 13.10 on a $\mathbf{A} = \ell^\times$), ce qui permet une amélioration d'un facteur $1/2$ par rapport à la borne générale pour $[\Gamma : \Lambda]$ telle que donnée dans la proposition 13.11. De plus en utilisant comme auparavant l'inégalité $4^{-1}\lambda_v > 1$ (également valable ici pour tout $v \in \hat{\mathrm{T}}$) on obtient une borne inférieure pour $\mu(G(\mathbb{R})/\Gamma)$ qui contient encore le produit d'Euler $L_{\ell|\mathbb{Q}}(3)\zeta(2)\zeta(4)\zeta(6)$ (de manière similaire à (15.23)). Par une estimation numérique de cette borne (sous PARI/GP), on voit qu'avec $\mathscr{D}_\ell = 4$ le covolume de $\Gamma$ serait supérieur à celui de $\Gamma_1$. On a donc également $\ell = \ell_1$ dans le cas $r = 4$. L'inégalité $4^{-1}\lambda_v \geq 35/4$ (où $35 = \lambda_v$ avec $r = 4$ et $v = (2)$ selon (15.22)) permet encore de prouver qu'avec $\ell = \ell_1$, le covolume minimal $\nu^n_{\mathbf{nc}}$ est atteint dans un groupe $G$ qui comme $G_1$ est quasi-déployé sur chaque corps $p$-adique. Cela suffit à prouver le cas $r = 2m$ du théorème 1.4.

**Remarque 15.6.** Dans les trois cas examinés notre preuve montre que si $G$ contient un sous-groupe $\Gamma$ qui atteint $\nu^n_{\mathbf{nc}}$, alors $G$ est isomorphe à $G_1$ sur chaque complété de $\mathbb{Q}$. Comme $G$ est de la forme $\mathrm{Spin}_f$ pour une forme quadratique, le théorème de Hasse-Minkowski (principe de Hasse pour les formes quadratiques) permet de voir que $G$ doit même être $\mathbb{Q}$-isomorphe à $G_1$. En particulier on a nécessairement $[\Gamma : \Lambda] = [\Gamma_1 : \Lambda_1]$, et donc $\Gamma_1$ réalise bien le minimum $\nu^n_{\mathbf{nc}}$. Comme signalé dans la remarque 15.5 pour le cas compact, un tel résultat d'« unicité » pour $G_1$ ne permet pas encore de déduire l'unicité du quotient arithmétique non compact de volume minimal.

# Bibliographie


[AB08] **P. Abramenko** et **K. S. Brown** : Buildings : Theory and applications. *Graduate text in mathematics*, vol. 248 (Springer, 2008)

[BE] **M. Belolipetsky** et **V. Emery** : On volumes of arithmetic quotients of PO$(n, 1)$, $n$ odd. *En préparation*

[Bel04] **M. Belolipetsky** : On volumes of arithmetic quotients of SO$(1, n)$. *Annali della Scuola Normale Superiore di Pisa - Classe di Scienze (S.5)* **3**(4) (2004), 749–770

[Bel07] ——— Addendum to : On volumes of arithmetic quotients of SO$(1, n)$. *Annali della Scuola Normale Superiore di Pisa - Classe di Scienze (S.5)* **6**(2) (2007), 263–268

[BHC62] **A. Borel** et **Harish-Chandra** : Arithmetic subgroups of algebraic groups. *Annals of mathematics* **75**(3) (1962), 485–535

[Bor63] **A. Borel** : Compact Clifford-Klein forms of symmetric spaces. *Topology* **2** (1963), 111–122

[Bor69] ——— Introduction aux groupes arithmétiques. *Actualités scientifiques et industrielles*, vol. 1341 (Hermann, 1969)

[Bor81] ——— Commensurability classes and volumes of hyperbolic 3-manifolds. *Annali della Scuola Normale Superiore di Pisa - Classe di Scienze (S.4)* **8**(1) (1981), 1–33

[Bor91] ——— Linear algebraic groups (2nd enlarged ed.). *Graduate texts in mathematics*, vol. 126 (Springer, 1991)

[BP89] **A. Borel** et **G. Prasad** : Finiteness theorems for discrete subgroups of bounded covolume in semi-simple groups. *Publications mathématiques IHES* **69** (1989), 119–171

[BT65] **A. Borel** et **J. Tits** : Groupes réductifs. *Publications mathématiques IHES* **27** (1965), 55–150

[BT72] **F. Bruhat** et **J. Tits** : Groupes réductifs sur un corps local I : Données radicielles valuées. *Publications mathématiques IHES* **41** (1972), 5–251

[BT84] ——— Groupes réductifs sur un corps local II : Schémas en groupes ; existence d'une donnée radicielle valuée. *Publications mathématiques IHES* **60** (1984), 1–194

[BT87] ——— Groupes algébriques sur un corps local III : Compléments et applications à la cohomologie. *Journal of the Faculty of Science, University of Tokyo, Sect. IA* **34** (1987), 671–698

[CF86] **T. Chinburg** et **E. Friedman** : The smallest arithmetic hyperbolic three-orbifold. *Inventiones mathematicae* **86**(3) (1986), 507–527

[Coh00] **H. Cohen** : Advanced topics in computational number theory. *Graduate texts in mathematics*, vol. 193 (Springer, 2000)

[DM86] **P. Deligne** et **G. D. Mostow** : Monodromy of hypergeometric functions and non-lattice integral monodromy. *Publications mathématiques IHES* **63** (1986), 5–89

[Fri89] **E. Friedman** : Analytic formulas for the regulator of a number field. *Inventiones mathematicae* **98** (1989), 599–622

[GM09] **F. W. Gehring** et **G. J. Martin** : Minimal co-volume hyperbolic lattices, I : The spherical points of a Kleinian group. *Annals of mathematics* **270**(1) (2009), 123–161

[Gou97] **F. Q. Gouvêa** : $p$-adic numbers (2nd edition). *Universitext* (Springer, 1997)

[GPS87] **M. Gromov** et **I. Piatetski-Shapiro** : Non-arithmetic groups in Lobachevsky spaces. *Publications mathématiques IHES* **66** (1987), 93–103

[Gro97] **B. H. Gross** : On the motive of a reductive group. *Inventiones mathematicae* **120**(2) (1997), 287–313

[Hel62] **S. Helgason** : Differential geometry and symmetric spaces. *Pure and applied mathematics*, vol. 12 (Academic Press, 1962)

[Hil07] **T. Hild** : The cusped hyperbolic orbifolds of minimal volume in dimensions less than ten. *Journal of algebra* **313**(1) (2007), 208–222

[HK07] **T. Hild** et **R. Kellerhals** : The FCC lattice and the cusped hyperbolic 4-orbifold of minimal volume : In memoriam H.S.M. Coxeter. *Journal of the London mathematical society* **75**(3) (2007), 677–689

[Hum75] **J. E. Humphreys** : Linear algebraic groups. *Graduate text in mathematics*, vol. 21 (Springer, 1975)

[Hum90] ——— Reflection groups and Coxeter groups. *Cambridge studies in advanced mathematics*, vol. 29 (Cambridge university press, 1990)

[IM65] **N. Iwahori** et **H. Matsumoto** : On some Bruhat decomposition and the structure of the Hecke rings of $p$-adic Chevalley groups. *Publications mathématiques IHES* **25** (1965), 5–48

[JKRT99] **N. W. Johnson** *et al.* : The size of a hyperbolic Coxeter simplex. *Transformation Groups* **4**(4) (1999), 329–353

[Kel89] **R. Kellerhals** : On the volume of hyperbolic polyhedra. *Mathematische Annalen* **285**(4) (1989), 541–569

[Lan86] **S. Lang** : Algebraic number theory. *Graduate texts in mathematics*, vol. 110 (Springer, 1986)

[LM93] **J.-S. Li** et **J. J. Millson** : On the first Betti number of a hyperbolic manifold with an arithmetic fundamental group. *Duke mathematical journal* **71**(2) (1993), 365–401

[Mak66] **V. S. Makarov** : A certain class of discrete Lobacevskii space groups with an infinite fundamental region of finite measure. *Soviet Mathematics, Doklady* **167**(1) (1966), 328–331

[Mar91] **G. A. Margulis** : Discrete subgroups of semisimple Lie groups. *Ergebnisse der Mathematik und ihrer Grenzgebiete (3. Folge)*, vol. 17 (Springer, 1991)

[Mey85] **R. Meyerhoff** : The cusped hyperbolic 3-orbifold of minimum volume. *Bulletin of the American mathematical society* **13**(2) (1985), 154–156

[Mor96] **P. Morandi** : Field and Galois theory. *Graduate texts in mathematics*, vol. 167 (Springer, 1996)

[MR86] **G. A. Margulis** et **J. Rohlfs** : On proportionality of covolumes of discrete subgroups. *Mathematische Annalen* **275** (1986), 197–205

[MR03] **C. Maclachlan** et **A. W. Reid** : The arithmetic of hyperbolic 3-manifolds. *Graduate texts in mathematics*, vol. 219 (Springer, 2003)

[MSG] **A. Mohammadi** et **A. Salehi Golsefidy** : Discrete vertex transitive actions on Bruhat-Tits buildings. *Prépublication*, disponible sur `http://www.math.princeton.edu/~asalehi/research.html`

[MT62] **G. D. Mostow** et **T. Tamagawa** : On the compactness of arithmetically defined homogeneous spaces. *Annals of mathematics* **76**(2) (1962), 446–463

[Neu99] **J. Neukirch** : Algebraic number theory. *Grundlehren der mathematischen Wissenschaften*, vol. 322 (Springer, 1999)

[Odl] **A. M. Odlyzko** : Discriminant bounds. Disponible sur `http://www.dtc.umn.edu/~odlyzko/unpublished/index.html`

[Odl90] ——— Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions : a survey of recent results. *Séminaire de théorie des nombres de Bordeaux (série II)* **2**(1) (1990), 119–141

[Oes93] **J. Oesterlé** : Polylogarithmes. *Séminaire Bourbaki* **35**(Exposé No. 762) (1992–1993), 49–67

[O'M63] **O. T. O'Meara** : Introduction to quadratic forms. *Grundlehren der mathematischen Wissenschaften*, vol. 117 (Springer, 1963)

[Ono66] **T. Ono** : On algebraic groups and discontinuous groups. *Nagoya mathematical journal* **27** (1966), 279–322

[OV94] **A. L. Onishchik** et **E. B. Vinberg** (Eds.) : Lie groups and Lie algebras III : Structure of Lie groups and Lie algebras. *Encyclopaedia of mathematical sciences*, vol. 41 (Springer, 1994)

[OV00] ——— Lie groups and Lie algebras II : I. Discrete subgroups of Lie groups. *Encyclopaedia of mathematical sciences*, vol. 21 (Springer, 2000)

[PR94] **V. Platonov** et **A. Rapinchuck** : Algebraic groups and number theory (engl. transl.). *Pure and applied mathematics*, vol. 139 (Academic Press, 1994)

[PR09] **G. Prasad** et **A. Rapinchuk** : Weakly commensurable arithmetic groups and isospectral locally symmetric spaces. *Publications mathématiques IHES* **109** (2009), 113–184

[Pra89] **G. Prasad** : Volumes of $S$-arithmetic quotients of semi-simple groups. *Publications mathématiques IHES* **69** (1989), 91–117

[Rag72] **M. S. Raghunathan** : Discrete subgroups of Lie groups. *Ergebnisse der Mathematik und ihrer Grenzgebiete (1. Folge)*, vol. 68 (Springer, 1972)

[RC97] **A. A. Ryzhkov** et **V. Chernousov** : On the classification of maximal arithmetic subgroups of simply connected groups. *Sbornik : mathematics* **188**(9) (1997), 1385–1413

[Roh79] **J. Rohlfs** : Die maximalen arithmetisch definierten Untergruppen zerfallender einfacher Gruppen. *Mathematische Annalen* **244** (1979), 219–231

[Sch85] **W. Scharlau** : Quadratic and hermitian forms. *Grundlehren der mathematischen Wissenschaften*, vol. 270 (Springer, 1985)

[Ser02] **J.-P. Serre** : Galois cohomology (transl. from French, corrected 2nd printing). *Springer monographs in mathematics* (Springer, 2002)

[Sie45] **C. L. Siegel** : Some remarks on discontinuous groups. *Annals of mathematics* **46**(4) (1945), 708–718

[Spr98] **T. A. Springer** : Linear algebraic groups (2nd ed.). *Progress in mathematics*, vol. 9 (Birkhäuser, 1998)

[Thu80] **W. P. Thurston** : The geometry and topology of 3-manifolds (notes of course, Princeton) (1980)

[Tit66] **J. Tits** : Classification of algebraic semisimple groups. *Dans :* Proceedings of symposia in pure mathematics, vol. 9, 33–62 (1966)

[Tit79] ——— Reductive groups over local fields. *Dans :* Proceedings of symposia in pure mathematics, vol. 33, 29–69 (1979)

[Vin67] **E. B. Vinberg** : Discrete groups generated by reflections in Lobacevskii spaces. *Mathematics of the USSR, Sbornik* **1**(3) (1967), 429–444

[Vin93] **E. B. Vinberg** (Ed.) : Geometry II : II. Discrete groups of motions of spaces of constant curvature. *Encyclopaedia of mathematical sciences*, vol. 29 (Springer, 1993)

[Vos98] **V. E. Voskresenskii** : Algebraic groups and their birational invariants. *Translations of mathematical monographs*, vol. 179 (American mathematical society, 1998)

[Wan72] **H. C. Wang** : Topics on totally discontinuous groups. *Dans :* Symmetric spaces (W. Boothby ed.) (M. Dekker, 1972)

[Wat79] **W. C. Waterhouse** : Introduction to affine group schemes. *Graduate texts in mathematics*, vol. 66 (Springer, 1979)

[Wei82] **A. Weil** : Adeles and algebraic groups. *Progress in mathematics*, vol. 23 (Birkhäuser, 1982)

[Zim84] **R. Zimmer** : Semisimple groups and ergodic theory. *Monographs in mathematics*, vol. 81 (Birkhäuser, 1984)

# Liste des symboles

| | |
|---|---|
| $\mathrm{Aut}(\Delta_v)$ | groupe des symétries de $\Delta_v$, page 91 |
| $A$ | certain sous-groupe de $H^1(k, \mathrm{C})$, voir équation (12.7), page 114 |
| $A_\xi$ | noyau de $\xi$ dans $A$, page 115 |
| $\mathrm{A}_r$ – $\mathrm{D}_r$ | types classiques, page 70 |
| C | centre de $G$, page 93 |
| $C(G)$, $C(G')$ | certaine constante associée au type de $G$, page 97 |
| $C(r)$ | $C(G)$ pour le type fixé $\mathrm{D}_r$, voir équation (13.5), page 126 |
| ${}^{3,6}\mathrm{D}_4$ | types trialitaires, page 77 |
| $\overline{G}$ | groupe adjoint de $G$, page 30 |
| $G^\sigma$ | groupe $\sigma(G)$ pour $\sigma : K \to \overline{k}$, page 27 |
| $G_{\mathbb{A}}$ | groupe adélique de $G$, page 61 |
| $G_\infty$ | produit des groupes $G(k_v)$ archimédiens (cf. aussi (3.4)), page 61 |
| $G_{\mathcal{S}}$ | produit des groupes $G(k_v)$ archimédiens non compacts (cf. aussi §3.4), page 93 |
| $G'$ | forme interne quasi-déployée de $G$, page 78 |
| $G_{\mathrm{u}}$ | forme compacte réelle de $G$, page 74 |
| $G^\circ$ | composante connexe de l'unité, page 24 |
| $\mathrm{Gal}(K\|k)$ | groupe de Galois, page 19 |
| $\mathrm{H}_v$ | invariant de Hasse, page 133 |
| $H^1(K, G)$ | ensemble (resp. groupe si $G$ est abélien) de cohomologie de dimension 1, page 108 |
| $\mathrm{Isom}^+(\mathbb{H}^n)$ | groupe des isométries de $\mathbb{H}^n$ préservant l'orientation, page 15 |
| $L_{\ell\|k}$ | fonction $L$ associée à l'extension quadratique $\ell\|k$, page 50 |
| $\overline{\mathrm{M}}_v$ | notation du $\mathbb{F}_v$-groupe $\overline{\mathcal{G}}_{P_v}^{\mathrm{red}}$ dans la formule du volume, avec $P_v \subset G(k_v)$ parahorique, page 98 |
| M | « mauvaises places » pour le calcul de l'indice $[\Gamma : \Lambda]$, page 118 |
| $N_G(H)$ | normalisateur, page 25 |
| $N_{K\|k}$ | norme (cf. aussi exemple 7.36), page 45 |
| $N_0(r)$ | imprécision sur $\nu_{\mathbf{c}}^n$, page 17 |
| $N_1(r)$ | imprécision sur $\nu_{\mathbf{nc}}^n$, page 17 |
| $\mathrm{SO}(n, 1)$ | groupe de Lie spécial orthogonal de signature $(n, 1)$, page 32 |

| | |
|---|---|
| $\mathrm{SO}_f$ | groupe spécial orthogonal, page 23 |
| $\mathrm{SO}_{(n,1)}$ | $\mathbb{R}$-groupe SO de signature $(n,1)$, page 32 |
| $\mathrm{Spin}(n,1)$ | groupe de Lie Spin de signature $(n,1)$, page 33 |
| $\mathrm{Spin}_f$ | groupe des spineurs, page 31 |
| $\mathrm{Spin}_{(n,1)}$ | $\mathbb{R}$-groupe Spin de signature $(n,1)$, page 33 |
| T | ensemble des places qui indicent les facteurs lambda dans la formule du volume, page 99 |
| $\hat{\mathrm{T}}$ | places finies $v \notin \mathscr{R}$ où $G\|k_v$ n'est pas quasi-déployé, page 118 |
| $U_k$ | groupe des unités, page 51 |
| $V = V_\mathrm{f} \cup V_\infty$ | places (finies et infinies) d'un corps, page 57 |
| $W(G,T)$ | groupe de Weyl absolu, page 68 |
| $W_I$ | sous-groupe du groupe de Coxeter $(W,S)$, engendré par $I \subset S$, page 72 |
| $X(k)$ | points $k$-rationnels de $X$, page 21 |
| $X\|K$ | variété $X$ considérée sur l'extension $K$, page 21 |
| $Z_G$ | centre, page 30 |
| $Z_G(H)$ | centralisateur, page 25 |

| | |
|---|---|
| $\mathrm{d}(f)$ | discriminant de la forme quadratique $f$, page 79 |
| $e_{\mathfrak{P}\|\mathfrak{p}}$ | indice de ramification, page 49 |
| $f_{\mathfrak{P}\|\mathfrak{p}}$ | degré d'inertie, page 49 |
| $h_k$ | nombre de classes, page 44 |
| $\overline{k}$ | clôture algébrique du corps $k$, page 19 |
| $\hat{k}_v$ | extension maximale non ramifiée, page 57 |
| $k_\infty$ | produit des $k_v$ archimédiens (cf. aussi (4.3)), page 55 |
| $k_v$ | complété de $k$ par rapport à $\|\cdot\|_v$, page 54 |
| $\ell$ | extension $\ell\|k$ associée à un $k$-groupe semi-simple, page 96 |
| $\ell_\mathfrak{n}$ | certain sous-groupe de $\ell^\times$, page 118 |
| $\ell_v$ | anneau $\prod_{w\|v} \ell_v$, page 54 |
| $q$,$q'$,$\bar{q}$ | entiers reliant $\#A_\xi$ à $\#\mathbf{A}_\mathfrak{n}/(\ell^\times)^\mathfrak{n}$, page 119 |
| $q_v$ | cardinalité de $\mathbb{F}_v$ $(v \in V_\mathrm{f})$, page 98 |
| $(s_1, s_2)$ | signature du corps $\ell$, page 123 |
| $\tilde{v}$ | valuation normalisée $(v \in V_\mathrm{f})$, page 58 |
| $\mathrm{vol}_\mathbb{H}$ | volume hyperbolique, page 15 |
| $w\|v$ | division de places, voir équation (5.1), page 54 |

| | |
|---|---|
| $\mathbf{A}$ | certain sous-groupe de $\mathbf{L}$ lié à $A$, page 118 |
| $\mathbf{A}_{\mathfrak{n}}$ | $\mathbf{A} \cap \ell_{\mathfrak{n}}$, page 118 |
| $\mathbf{A}_{\mathfrak{n}}^{\mathrm{M}}$ | certain sous-groupe de $\mathbf{A}$ contenant $\mathbf{A}_{\mathfrak{n}}$, page 119 |
| $\mathbf{G}_{\mathrm{a}}$ | groupe additif, page 23 |
| $\mathbf{G}_{\mathrm{m}}$ | groupe multiplicatif, page 23 |
| $\mathbf{L}$ | certain sous-groupe de $\ell^{\times}$, page 118 |
| $\mathbf{R}_{K\|k}(\,\cdot\,)$ | restriction des scalaires, page 27 |
| $\mathbf{R}_{\ell\|k}^{(\mathbf{1})}(\mathbf{G}_{\mathrm{m}})$ | noyau de $N_{\ell\|k}$ dans $\mathbf{R}_{\ell\|k}(\mathbf{G}_{\mathrm{m}})$, page 75 |
| $\mathbf{V}_f$ | espace quadratique, page 23 |
| $\mathbf{X} = \mathbf{X}(T)$ | groupes des caractères de $T$, page 67 |
| $\mathbf{h}$ | espace quadratique binaire isotrope, page 131 |

| | |
|---|---|
| $\mathcal{A}_k^n$ | espace affine sur $k$, page 20 |
| $\mathcal{AQ}_{\mathbf{c}}^n$ | quotients arithmétiques orientables compacts de $\mathbb{H}^n$, page 16 |
| $\mathcal{AQ}_{\mathbf{nc}}^n$ | quotients arithmétiques orientables non compacts de $\mathbb{H}^n$, page 16 |
| $\mathcal{J}_k$ | groupe des idéaux fractionnaires, page 44 |
| $\overline{\mathcal{G}}_P^{\mathrm{red}}$ | $\mathbb{F}_v$-groupe réductif associé au sous-groupe parahorique $P$, page 89 |
| $\overline{\mathcal{G}}_P^{\mathrm{ss}}$ | $\mathbb{F}_v$-groupe semi-simple associé au sous-groupe parahorique $P$, page 89 |
| $\mathcal{N}_{k\|\mathbb{Q}}$ | norme d'idéal, page 45 |
| $\mathcal{P}_k$ | groupe des idéaux fractionnaires principaux, page 44 |
| $\mathcal{T}_x X$ | espace tangent, page 21 |
| $\mathcal{Z}$ | centre de $G_{\mathcal{S}}$, page 93 |

| | |
|---|---|
| $\mathscr{C}_k$ | groupe des classes, page 44 |
| $\mathscr{D}_k$ | discriminant (valeur absolue), page 47 |
| $\mathscr{D}_{\ell\|k}$ | discriminant relatif, page 49 |
| $\mathscr{E}(\mathscr{P})$ | produit d'Euler dans la formule du volume, page 99 |
| $\overline{\mathscr{M}}_v$ | notation du $\mathbb{F}_v$-groupe $\overline{\mathcal{G}}_{P'_v}^{\mathrm{red}}$ dans la formule du volume, avec $P'_v \subset G'(k_v)$ parahorique, page 98 |
| $\mathscr{O}_{\mathfrak{p}}$ | anneau des entiers $\mathfrak{p}$-adiques, page 56 |
| $\mathscr{O}_k$ | anneau des entiers algébriques de $k$, page 43 |
| $\mathscr{R}$ | places finies $v$ où $G\|\hat{k}_v$ n'est pas déployé, page 94 |

| | |
|---|---|
| $\mathbb{A}$ | anneau des adèles, page 59 |
| $\mathbb{A}_{\mathrm{f}}$ | anneau des adèles finis, page 60 |
| $\mathbb{F}_{\mathfrak{p}}$, $\mathbb{F}_v$ | corps $\mathscr{O}_k/\mathfrak{p}$, avec $v=\mathfrak{p}$, page 46 |
| $\mathbb{F}_p$ | corps fini à $p$ éléments, page 56 |
| $\mathbb{H}^n$ | Espace hyperbolique, page 14 |
| | |
| $\mathfrak{g}$ | algèbre de Lie, page 28 |
| $\mathfrak{n}$ | entier qui sert à la description du centre C de $G$, page 117 |
| $\mathfrak{P}\|\mathfrak{p}$ | division d'idéaux, page 49 |
| $\mathfrak{s}$ | certain entier associé aux types externes, page 97 |
| | |
| $\Delta_v$ | diagramme de Dynkin local d'un $k_v$-groupe, page 86 |
| $\widehat{\Delta}_v$ | diagramme de Dynkin local sur $\hat{k}_v$, page 87 |
| $\Delta^0$ | éléments de la base absolue $\Delta$ envoyés par $j$ sur 0, page 75 |
| $\Phi(G,T)$ | système de racines par rapport à $T$, page 67 |
| $\Gamma^{\mathfrak{m}}$ | normalisateur de $\Lambda^{\mathfrak{m}}$, page 116 |
| $\Lambda^{\mathfrak{m}}$ | sous-groupe arithmétique principal de covolume minimal (dans sa classe de commensurabilité), page 116 |
| $\Lambda_{\mathscr{P}}$ | sous-groupe principal associé à la collection cohérente $\mathscr{P}$, voir équation (6.6), page 64 |
| $\Xi_v$ | image de $\xi_v$ dans $\mathrm{Aut}(\Delta_v)$, page 113 |
| | |
| $\gamma_v$ | certaines constantes (dans $\mathbb{R}_{>0}$) déterminées par une forme de Tamagawa, page 96 |
| $\lambda_v$ $(v\in \mathrm{T})$ | facteurs lambda dans la formule du volume, page 100 |
| $\mu_\infty$, $\mu_{\mathcal{S}}=\mu$ | produit des mesures $\mu_v$ ($v\in V_\infty$, resp. $v\in\mathcal{S}$), page 95 |
| $\mu_v$ | mesure de Haar sur $G(k_v)$ normalisée par $\mu_v(\mathbf{R}_{k_v\|\mathbb{R}}(G)_{\mathrm{u}})=1$, page 95 |
| $\mu(k)$ | groupe des racines de l'unités dans $k$, page 51 |
| $\nu^n_{\mathbf{c}}$ | minimum de $\mathrm{vol}_{\mathbb{H}}(\mathcal{AQ}^n_{\mathbf{c}})$, page 17 |
| $\nu^n_{\mathbf{nc}}$ | minimum de $\mathrm{vol}_{\mathbb{H}}(\mathcal{AQ}^n_{\mathbf{nc}})$, page 17 |
| $\nu_v$ | mesure normalisée sur $k_v$, page 59 |
| $\pi$ | projection $G\to\overline{G}$, page 30 |
| $\tau_\alpha$ | réflexion associée à la racine $\alpha$, page 68 |

| | |
|---|---|
| $\theta = (\theta_v)$ | type global d'un sous-groupe arithmétique principal, page 94 |
| $\omega_{\mathbb{A}}$ | mesure de Tamagawa, page 63 |
| $\xi$ | homomorphisme défini sur $H^1(k, \mathrm{C})$, voir équation (12.5), page 114 |
| $\zeta$ | fonction zêta de Riemann, page 50 |
| $\zeta_k$ | fonction zêta associé à $k$, page 50 |
| | |
| $\left(\frac{\cdot,\cdot}{v}\right)$ | symbole de Hilbert, page 132 |
| $[\sigma]$ | classe $\{\sigma, \overline{\sigma}\}$ d'un plongement archimédien, page 39 |
| $\lvert\cdot\rvert_v$ | valeur absolue normalisée ($v \in V$), page 58 |

# Index

# Curriculum Vitae

## Données personnelles

**Nom** Vincent Emery

**Date et lieu de naissance** 19 juin 1981, Sion

**Nationalité** Suisse

**Lieu d'origine** Lens (VS)

**Filiation** Jacques et Christine Emery-Pitteloud

**Etat civil** marié à Vanessa Emery-Carlen (29 juillet 2005)

**Adresse privée** Rue du Rawyl 27, 1950 Sion

## Formation

**1995 - 2000** Maturité scientifique au Lycée-Collège des Creusets (Sion)

**2000 - 2004** Diplôme de mathématiques, Université de Fribourg

**2004 - 2009** Doctorat en mathématiques, Université de Fribourg

## Langues

- français : langue maternelle
- anglais, allemand : parlés couramment

## Séjours à but scientifique

- Université de Durham (Angleterre), invité par Dr. Mikhail Belolipetsky (août - septembre 2006)
- Université du Michigan (Ann Arbor, USA), invité par Prof. Gopal Prasad (avril - mai 2008)

## Exposés

- *Finding hyperbolic arithmetic orbifolds of minimal volume*, Topology Seminar, University of Texas, 5 mai 2008
- *Arithmetic covolume of the modular group*, Geometry seminar, Durham (Angleterre), 5 février 2009

## Divers

**Informatique** Connaissance de Linux, Windows, LaTeX

**Armée** Ecole de recrues (été 2000) et de sous-officiers (été 2001) dans l'infanterie. Depuis 2007 incorporé au détachement de cryptologie de l'armée.

**Loisirs** marche en montagne, viti-viniculture, musique classique, lecture