université de BORDEAUX

Thèse présentée pour obtenir le grade de

Docteur de
l'Université de Bordeaux

École doctorale mathématiques et informatique
Spécialité mathématiques pures

Par Aurel Page

Méthodes explicites pour les groupes arithmétiques

Sous la direction de Karim Belabas
et de Andreas Enge

Soutenue le 15 juillet 2014 devant le jury composé de :

M. Kamal Khuri-Makdisi	Prof. American Univ. of Beirut	Président
M. John Voight	Prof. Dartmouth College	Rapporteur
M. Paul Gunnells	Prof. University of Massachusetts	Rapporteur
M. Karim Belabas	Prof. Université de Bordeaux	Directeur
M. Andreas Enge	DR INRIA Bordeaux Sud-Ouest	Directeur

Titre : Méthodes explicites pour les groupes arithmétiques

Résumé : Les algèbres centrales simples ont de nombreuses applications en théorie des nombres, mais leur algorithmique est encore peu développée. Dans cette thèse, j'apporte une contribution dans deux directions. Premièrement, je présente des algorithmes de complexité prouvée, ce qui est nouveau dans la plupart des cas. D'autre part, je développe des algorithmes heuristiques mais très efficaces dans la pratique pour les exemples qui nous intéressent le plus, comme en témoignent mes implantations. Les algorithmes sont à la fois plus rapides et plus généraux que les algorithmes existants. Plus spécifiquement, je m'intéresse aux problèmes suivants : calcul du groupe des unités d'un ordre et problème de l'idéal principal. Je commence par étudier le diamètre du domaine fondamental de certains groupes d'unités grâce à la théorie des représentations. Je décris ensuite un algorithme prouvé pour calculer des générateurs et une présentation du groupe des unités d'un ordre maximal dans une algèbre à division, puis un algorithme efficace qui calcule également un domaine fondamental dans le cas où le groupe des unités est un groupe kleinéen. Je donne en outre un algorithme de complexité prouvée qui détermine si un idéal d'un tel ordre est principal, et qui en calcule un générateur le cas échéant, puis je décris un algorithme heuristiquement sous-exponentiel pour résoudre le même problème dans le cas d'une algèbre de quaternions indéfinie.

Mots clés : algèbre à division, groupe d'unités, problème de l'idéal principal, algorithme, groupe de Kazhdan, géométrie hyperbolique, arbre de Bruhat–Tits.

Title: Explicit methods for arithmetic groups

Abstract: Central simple algebras have many applications in number theory, but their algorithmic theory is not yet fully developed. I present algorithms to compute effectively with central simple algebras that are both faster and more general than existing ones. Some of these algorithms have proven complexity estimates, a new contribution in this area; others rely on heuristic assumptions but perform very efficiently in practice.

Precisely, I consider the following problems: computation of the unit group of an order and principal ideal problem. I start by studying the diameter of fundamental domains of some unit groups using representation theory. Then I describe an algorithm with proved complexity for computing generators and a presentation of the unit group of a maximal order in a division algebra, and then an efficient algorithm that also computes a fundamental domain in the case where the unit group is a Kleinian group. Similarly, I present an algorithm with proved complexity that decides whether an ideal of such an order is principal and that computes a generator when it is. Then I describe a heuristically subexponential algorithm that solves the same problem in indefinite quaternion algebras.

Keywords: division algebra, unit group, principal ideal problem, algorithm, Kazhdan group, hyperbolic geometry, Bruhat–Tits tree.

Remerciements

Je tiens tout d'abord à exprimer ma gratitude envers mes directeurs Karim et Andreas, pour leur grande disponibilité malgré leurs nombreuses contraintes et pour leurs précieux conseils. Merci à tous les membres de l'IMB pour leur excellent accueil, tout particulièrement les membres de l'équipe LFANT qui m'ont beaucoup appris sur la théorie algorithmique des nombres. Je tiens à remercier aussi tous les mathématiciens avec qui j'ai discuté durant cette thèse, et notamment John Voight et Nicolas Bergeron dont l'aide a été très précieuse dans mon travail. J'ai aussi une pensée pour tous les professeurs qui m'ont enseigné les maths depuis le collège, en particulier mes professeurs de prépas Franz Ridde et Alain Chillès. Je salue tous les doctorants mathématiciens de Bordeaux pour la bonne ambiance qui a toujours régné au laboratoire, pour les excellentes soirées Lambda et les non moins excellentes soirées non-officielles, et je salue tout particulièrement Nicolas Mascot avec qui j'ai partagé le bureau 360 et avec qui j'ai passé de très bons moments (mention spéciale pour les soirées raclette-Civilization sur vidéoprojecteur). Merci à tous mes amis pour leur soutien constant, en particulier ceux que j'ai vu le plus durant ces trois ans : Louis, Mingan, Sisi, Stéphanie et Thomas à Bordeaux, Guillaume, Maëlle et Samuel à Paris. Merci au Carpe Diem, au Melisone et au 48 de m'avoir nourri, et merci à leur personnel pour leur bonne humeur !

Merci à mes parents Michèle et Denis, du fond du cœur, pour l'éducation et l'amour que vous m'avez donnés, je ne serais jamais arrivé jusque là sans vous ! Merci aussi à mon frère Alexis, mon parrain Bruno, ma marraine Chantal, et à toute ma famille pour votre soutien. Mes pensées les plus tendres vont à ma chérie Néphéli : merci pour toutes ces années et ces moments extraordinaires que nous avons passés ensemble ! Ce sont tes encouragements et ton réconfort qui m'ont permis d'aller au bout de cette thèse ! Merci aussi à ta famille pour leur accueil chaleureux. Je n'ai pas de mots pour dire à quel point vous comptez tous pour moi !

Enfin, merci à toi, lecteur, d'être venu m'encourager si tu es en train de m'écouter parler à ma soutenance, ou de t'intéresser à mon travail si tu es en train d'ouvrir cette thèse pour la lire.

Résumé substantiel

Théorie algébrique des nombres. La théorie algébrique des nombres telle qu'elle existe aujourd'hui a été développée pour résoudre certains problèmes arithmétiques, parmi lesquels:

(i) Équation de Pell–Fermat : quelles sont les solutions x, y en nombres entiers de $x^2 - dy^2 = \pm 1$ lorsque d n'est pas un carré ?
(ii) Conjecture de Fermat : l'équation $x^n + y^n = z^n$ possède-t-elle des solutions entières $x, y, z > 0$ lorsque $n \geq 3$?
(iii) Résolubilité par radicaux : quand est-il possible d'exprimer les solutions d'une équation polynomiale $P(x) = 0$ uniquement à l'aide des quatre opérations arithmétiques et des extractions de racines ?
(iv) Un entier positif n étant fixé, quels sont les nombres premiers qui peuvent s'écrire $x^2 + ny^2$ avec x, y entiers ?

L'étude de ces problèmes a progressivement amené la notion de *corps de nombres algébriques* F, c'est-à-dire l'ensemble des nombres formés par addition et multiplication à partir des nombres rationnels $\mathbb{Q}$ auxquels on ajoute une racine d'un polynôme à coefficients entiers. Par exemple, les problèmes précédents invitent respectivement à étudier (i) $F = \mathbb{Q}(\sqrt{d})$, (ii) $F = \mathbb{Q}(\zeta)$ où ζ est une racine n-ème de l'unité non-triviale: $\zeta^n = 1$, (iii) $F = \mathbb{Q}(\alpha)$, où α est une racine du polynôme $P(x)$, et (iv) $F = \mathbb{Q}(\sqrt{-n})$. Les questions précédentes se posant en termes de nombres entiers et non en termes de nombres rationnels, on a besoin d'un analogue pour les corps de nombres de ce que sont les entiers $\mathbb{Z}$ pour les rationnels $\mathbb{Q}$: c'est l'*anneau des entiers algébriques* $\mathbb{Z}_F$ de F.

Les problèmes que nous avons présentés conduisent à l'étude d'objets importants attachés aux corps de nombres. Ainsi, l'équation de Pell–Fermat (i) se ramène à l'étude d'un premier invariant important du corps de nombres F: le *groupe des unités* $\mathbb{Z}_F^\times$, c'est-à-dire des éléments de $\mathbb{Z}_F$ dont l'inverse est aussi un élément de $\mathbb{Z}_F$:

$$\frac{1}{x + \sqrt{d}y} = \frac{x - \sqrt{d}y}{(x + \sqrt{d}y)(x - \sqrt{d}y)} = \frac{x + \sqrt{d}y}{x^2 - dy^2} = \pm(x + \sqrt{d}y).$$

Une des premières approches de la conjecture de Fermat a consisté à factoriser l'équation en

$$x^n = z^n - y^n = (z - y)(z - \zeta y)(z - \zeta^2 y) \cdots (z - \zeta^{n-1} y),$$

et à factoriser les deux côtés de l'équation en produit de nombres « premiers ». Malheureusement, dans des anneaux tels que $\mathbb{Z}_F = \mathbb{Z}[\zeta]$, la propriété de factorisation

unique en produit de nombres premiers n'est plus valide. On a recours à un substitut sophistiqué de cette propriété. Par exemple, deux entiers ont toujours un plus grand diviseur commun ou PGCD, et on aimerait trouver de même le PGCD de deux éléments a et b de $\mathbb{Z}_F$. Un tel PGCD n'existe pas toujours dans $\mathbb{Z}_F$, mais on peut imaginer un « nombre idéal » α qui soit le PGCD de a et b. Ce « nombre idéal » n'a pas de sens, mais on peut donner un sens à l'ensemble de ses multiples, c'est ce qu'on appelle l'idéal $\mathfrak{a} = (a, b)$ engendré par a et b. La question de savoir si a et b ont vraiment un PGCD revient à se demander si l'idéal $\mathfrak{a}$ est principal, c'est-à-dire si c'est l'ensemble des multiples $\mathfrak{a} = (d)$ d'un seul élément d qui est alors effectivement un plus grand diviseur commun de a et b. En regroupant dans une même classe les idéaux qu'on peut obtenir les uns à partir des autres en multipliant par un idéal principal, on obtient un deuxième invariant important, le *groupe des classes* $\mathrm{Cl}(F)$ qui mesure à quel point la propriété de factorisation unique échoue dans F.

Le problème de la résolubilité par radicaux se ramène à étudier le *groupe de Galois* $\mathrm{Gal}(F/\mathbb{Q})$ qui encode les symmétries de l'équation $P(x) = 0$. Les groupes de symmétries les plus simples sont appelés abéliens, et ceux qui se décomposent en groupes abéliens sont appelés résolubles, en référence au problème de la résolubilité par radicaux.

Le problème de déterminer si un nombre premier p est de la forme $x^2 + ny^2$ revient à déterminer si les idéaux divisant p dans $F = \mathbb{Q}(\sqrt{-n})$ sont principaux. Cette propriété est analysée par la *théorie des corps de classes*, qui décrit un lien profond entre deux types d'objets : d'une part les extensions de F, c'est-à-dire les corps de nombres contenant F, dont le groupe de Galois est abélien; et d'autre part les groupes de classes de rayon, qui généralisent le groupe des classes $\mathrm{Cl}(F)$. En particulier, il existe une extension H de F appelée *corps de classe de Hilbert*, tel que $\mathrm{Gal}(H/F) \cong \mathrm{Cl}(F)$, et qui contrôle l'ensemble des nombres premiers p qui sont solutions de (iv).

Notre but est d'étudier des généralisations non-commutatives de la théorie algébrique des nombres.

Généralisations non-commutatives et groupes arithmétiques.

Algèbres centrales simples. Une première manière de généraliser la théorie algébrique des nombres est d'autoriser la multiplication à ne pas être commutative: dans un corps de nombres, on a toujours $ab = ba$. Cette généralisation conduit à remplacer les corps de nombres par les algèbres centrales simples. Formellement, si F est un corps de nombres, une algèbre A sur F est un F-espace vectoriel muni d'une multiplication associative et possédant un élément neutre, compatible avec la structure d'espace vectoriel. Toutes les algèbres considérées seront de dimension finie. Une *algèbre centrale simple* est une algèbre dont le centre est égal à $F \cdot 1_A$ et qui n'a pas d'idéal bilatère non trivial. Les algèbres centrales simples apparaîssent naturellement:

- L'algèbre $\mathcal{M}_n(F)$ des matrices $n \times n$ est centrale simple.

- Si G est un groupe fini, l'algèbre de groupe $F[G]$, qui intervient dans la théorie des représentations de G, est centrale simple.
- L'anneau des endomorphismes d'une variété abélienne est une somme directe d'algèbres centrales simples.
- Toute algèbre à division sur $\mathbb{Q}$, c'est-à-dire telle que tout élément non nul admet un inverse, est simple et son centre est un corps de nombres.

Une algèbre centrale simple A possède un analogue de l'anneau des entiers $\mathbb{Z}_F$: un *ordre maximal* $\mathcal{O}$. Un ordre dans A est une « version entière » de A : formellement, un sous-$\mathbb{Z}$-module de type fini $\mathcal{O}$ qui contient 1, est stable par multiplication et tel que $F\mathcal{O} = A$. Un ordre est dit maximal s'il n'est pas contenu dans un ordre strictement plus grand. En revanche, à cause de la non-commutativité, les ordres maximaux ne sont pas uniques: il y a plusieurs ordres maximaux dans A (si $A \neq F$), il y en a même une infinité ! En effet on peut obtenir d'autres ordres $x^{-1}\mathcal{O}x$ en conjugant l'un d'entre eux. En revanche, il n'y a qu'un nombre fini de classes de conjugaison d'ordres maximaux.

Les invariants classiques de la théorie algébrique des nombres ont leur analogue dans ce contexte. On peut s'intéresser au groupe des unités $\mathcal{O}^\times$. On a une notion d'idéal I à droite de $\mathcal{O}$ (ou à gauche, mais ce n'est pas la même chose à cause de la non-commutativité), et d'idéal à droite principal $I = x\mathcal{O}$. On étudie alors l'ensemble $\mathrm{Cl}(\mathcal{O})$ des classes d'idéaux à droite. En revanche, à cause de la non-commutativité, $\mathrm{Cl}(\mathcal{O})$ n'est pas un groupe !

Formes automorphes et groupes arithmétiques. Je ne donnerai pas de définition précise dans cette section, qui n'est pas directement abordée dans la thèse. Une autre manière de généraliser la théorie algébrique des nombres est de s'intéresser à la théorie des corps de classes, qui donne une description des extensions abéliennes d'un corps de nombres F. On aimerait donc avoir un analogue décrivant les extensions de F dont le groupe de Galois n'est pas nécessairement commutatif. Comme on peut s'y attendre, c'est extrêmement difficile et est un domaine de recherche actif. Voici une manière d'aborder le problème. On peut voir la théorie des corps de classes comme décrivant les caractères du groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$, c'est-à-dire les morphismes continus

$$\mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathbb{C}^\times = \mathrm{GL}_1(\mathbb{C})$$

en termes de caractères de groupes de classes de rayon. On peut généraliser cela en se proposant d'étudier les représentations galoisiennes de dimension supérieure, c'est-à-dire les morphismes continus

$$\mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_n(\mathbb{C}).$$

C'est ce point de vue qui est abordé par un vaste ensemble de conjectures connues sous le nom de programme de Langlands. Dans ce programme, les objets qu'on propose pour remplacer les caractères des groupes de classes sont les *formes automorphes*, qui sont des fonctions analytiques qui se transforment d'une manière

prescrite sous l'action de *groupes arithmétiques*. Les groupes arithmétiques sont essentiellement les ensembles des points entiers de groupes algébriques définis sur $\mathbb{Q}$. Plus précisément, soit $\mathbb{G} \subset \mathrm{GL}_n$ un groupe algébrique défini sur $\mathbb{Q}$, c'est-à-dire un sous-groupe défini par des équations polynomiales à coefficients rationnels. On peut alors définir $\mathbb{G}(\mathbb{Z}) = \mathbb{G}(\mathbb{Q}) \cap \mathrm{GL}_n(\mathbb{Z})$. Un sous-groupe $\Gamma \subset \mathbb{G}(\mathbb{Q})$ est dit *arithmétique* s'il est commensurable avec $\mathbb{G}(\mathbb{Z})$, c'est-à-dire si l'intersection $\Gamma \cap \mathbb{G}(\mathbb{Z})$ est d'indice fini dans chacun des deux groupes. L'exemple le plus classique de groupe arithmétique est $\mathrm{SL}_2(\mathbb{Z})$, qui joue un rôle central dans la théorie des formes modulaires. Un autre exemple important de groupe arithmétique auquel nous nous intéressons particulièrement dans cette thèse est le groupe des unités $\mathcal{O}^\times$ d'un ordre dans une algèbre centrale simple.

Le lien entre les représentations galoisiennes et les formes automorphes s'exprime au moyen des *fonctions L*. Les fonctions L sont des fonctions d'une variable complexe généralisant la fonction zêta de Riemann. Elles sont formées à partir d'un type de séries génératrices adaptées aux questions arithmétiques. Étant donnée une représentation galoisienne ou une forme automorphe « propre », on peut lui associer une fonction L, et on conjecture que les fonctions L provenant des constructions galoisiennes et automorphes sont en fait les mêmes.

Notre but est de proposer des algorithmes pour étudier les algèbres centrales simples ainsi que les groupes arithmétiques et les formes automorphes qui leur sont attachés.

Méthodes explicites.

Démarche. Dans tous les problèmes auxquels nous nous intéressons dans cette thèse, nous proposons deux types d'algorithmes:

- des algorithmes dont on prouve la complexité mais qui ne sont pas efficaces en pratique;
- des algorithmes déterministes ou probabilistes, efficaces en pratique mais dont la complexité est heuristique, dans des cas particuliers intéressants.

Cette dichotomie reflète le fait que les problèmes que nous abordons sont difficiles: pour le moment on ne sait pas décrire des algorithmes rapides et prouver qu'ils le sont. Notons que pour ces problèmes, les analyses de complexité sont rares dans la littérature. Dans cette thèse, les complexités des algorithmes sont des *complexités binaires* : on compte le nombre d'opérations binaires élémentaires en fonction de la taille binaire de l'entrée. Par ailleurs, nous avons implanté tous les algorithmes efficaces en Magma, et nous les avons comparés aux implantations et algorithmes existants lorsque c'était possible. Les algorithmes que nous décrivons sont à la fois plus rapides et plus généraux que les algorithmes préexistants.

Générateurs des S-unités. Soit S un ensemble fini de places d'un corps de nombres F. Le premier problème que nous abordons consiste à se demander si le groupe des S-unités $\mathcal{O}_S^\times$ d'un ordre maximal $\mathcal{O}$ dans une algèbre centrale simple A sur F peut être engendré par des éléments de petite hauteur, où « petite » signifie logarithmique en le discriminant de A. En effet, l'exemple des corps quadratiques réels

montre que les unités peuvent être de hauteur de l'ordre d'une puissance du discriminant, ce qui proscrit l'écriture de ces unités comme combinaisons linéaires des vecteurs d'une base d'entiers: on doit avoir recours à une représentation compacte comme produit de S-unités. Ce problème est abordé par Lenstra [**Len92**] pour le cas des corps de nombres. En utilisant des techniques de géométrie des nombres, il prouve le théorème suivant.

THÉORÈME (Lenstra). *Soit F un corps de nombres avec r_2 places complexes et de discriminant Δ_F. Soit $\mathbb{Z}_F$ l'anneau des entiers de F, et soit S un ensemble fini de places de F contenant toutes les places infinies et toutes les places finies $\mathfrak{p}$ telles que*

$$N(\mathfrak{p}) \leq (2/\pi)^{r_2}|\Delta_F|^{1/2}.$$

Soit m_S le maximum des normes des idéaux premiers de S, ou $m_S = 1$ s'il n'en existe pas. Alors le groupe des S-unités $\mathbb{Z}_{F,S}^{\times}$ est engendré par l'ensemble de ses éléments dont la hauteur logarithmique est inférieure ou égale à

$$\frac{1}{2}\log|\Delta_F| + \log m_S + r_2\log\Big(\frac{2}{\pi}\Big).$$

Dans un article récent [**CS12**], Chinburg et Stover définissent une notion de hauteur sur une algèbre à division, et en utilisant la même technique ils prouvent une généralisation aux algèbres à division sur $\mathbb{Q}$. Dans les deux théorèmes suivants, on note F un corps de nombres de degré n et A une algèbre à division centrale de degré d sur F, de discriminant absolu Δ_A, telle que r places réelles de F ramifient dans A, et $\mathcal{O}$ est un ordre maximal dans A. Pour un ensemble fini S de places de F on note m_S le maximum des normes des idéaux premiers de S, ou $m_S = 1$ s'il n'en existe pas. Les constantes explicites mentionnées au début des théorèmes ne dépendent que de n et d.

THÉORÈME (Chinburg–Stover). *Il existe des constantes explicites $f_1(n,d)$ and $f_2(n,d)$ vérifiant les propriétés suivantes. Définissons*

$$e = \frac{n}{d(2n-r)}.$$

On a $1/(2d) \leq e \leq 1/d$. Soit S un ensemble fini de places de F contenant toutes les places infinies et tous les idéaux premiers $\mathfrak{p}$ tels que

$$N(\mathfrak{p}) \leq f_1(n,d)\Delta_A^e.$$

Alors le groupe $\mathcal{O}_S^{\times}$ est engendré par l'ensemble de ses éléments dont la hauteur logarithmique est inférieure ou égale à

$$e\log(\Delta_A) + \log m_S + f_2(n,d).$$

En utilisant des propriétés de la théorie des représentations, nous prouvons de nouvelles bornes sur la taille de générateurs du groupe $\mathcal{O}_S^1$ des S-unités de norme réduite 1 pour des ensembles de places S arbitraires et pour le groupe $\mathcal{O}_S^{\times}$ pour des ensembles de places dépendant uniquement de F. Dans le chapitre 2, nous démontrons le théorème suivant (Théorème 2.4.2.4 et Théorème 2.4.3.4), dont nous donnons pour simplifier une version plus faible.

THÉORÈME A. *Il existe des constantes explicites $g_1(n,d)$, $g_2(n,d)$, $g_3(n,d)$ et $g_4(n,d)$ vérifiant les propriétés suivantes. Supposons que A n'est pas une algèbre de quaternions totalement définie. Soit S un ensemble de places de F contenant toutes les places infinies. Alors le groupe $\mathcal{O}_S^1$ est engendré par l'ensemble de ses éléments dont la hauteur logarithmique est inférieure ou égale à*

$$g_1(n,d)\log(\Delta_A) + \log m_S + g_2(n,d),$$

et on a $2/d \leq g_1(n,d) \leq 803/d$. Supposons de plus que S contient toutes les places finies $\mathfrak{p}$ telles que

$$N(\mathfrak{p}) \leq (2/\pi)^{r_2}|\Delta_F|^{1/2}.$$

Alors le groupe $\mathcal{O}_S^\times$ est engendré par l'ensemble de ses éléments dont la hauteur logarithmique est inférieure ou égale à

$$g_3(n,d)\log(\Delta_A) + (r+1)\log m_S + g_4(n,d).$$

Calcul de groupes d'unités. Nous abordons ensuite le problème de calculer un groupe d'unités $\Gamma = \mathcal{O}^1$, où « calculer » signifie calculer une présentation finie de Γ avec un isomorphisme calculable, ce qui implique en particulier de calculer un ensemble de générateurs. Notons que dans certains cas, le groupe en question est fini: c'est par exemple le cas du groupe des unités de norme réduite 1 d'une algèbre de quaternions totalement définie. Du côté des algorithmes théoriques, Grunewald et Segal ont décrit un algorithme permettant de calculer un groupe arithmétique arbitraire [**GS80**], mais il est inutilisable en pratique et sa complexité n'est pas connue. Nous ne connaissons que deux travaux contenant un algorithme calculant un groupe d'unités et dont les auteurs prouvent la complexité. Le premier est dû à Swan [**Swa71**] qui décrit un algorithme permettant de calculer le groupe $\mathrm{SL}_2(\mathbb{Z}_F)$ où F est un corps quadratique imaginaire, et prouve que son temps de calcul est de l'ordre de $\Delta_F^{O(1)}$, ce qui est optimal à l'exposant près. Le second est attribué à Chalk dans un article de Jahangiri [**Jah10**]: il s'agit de certains groupes d'unités dans des algèbres de quaternions sur $\mathbb{Q}$, et la complexité est de la forme $\exp(O(\Delta_A))$. Dans le chapitre 3, en nous appuyant sur les bornes du chapitre précédent, nous présentons un algorithme (Algorithme 3.1.2.8) et démontrons le théorème suivant (Theorem 3.1.2.9).

THÉORÈME B. *Soit A une algèbre à division centrale de degré d sur un corps de nombres F. Supposons que A n'est pas une algèbre de quaternions totalement définie. Étant donné un ordre maximal $\mathcal{O}$ dans A, l'Algorithme 3.1.2.8 calcule un groupe de présentation finie Γ et deux isomorphismes de groupes calculables $\phi : \Gamma \to \mathcal{O}^1$ et $\psi : \mathcal{O}^1 \to \Gamma$, inverse l'un de l'autre. Cet algorithme termine en temps*

$$\exp\Big(O(d\log\Delta_A) + O_N(\log\log\Delta_A)\Big).$$

En ce qui concerne les algorithmes efficaces, il existe de nombreux travaux dont la plus grande partie ne traite que des cas où le groupe algébrique est isotrope, ce qui dans notre cas signifie que l'algèbre n'est pas à division. Pour ce qui est des algèbres à division, Voight [**Voi09**] propose un algorithme efficace dans le cas

fuchsien, c'est-à-dire lorsque $A \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathcal{M}_2(\mathbb{R}) \times \mathbb{H}^r$. Dans le cas général, le seul travail dont nous ayons connaissance est celui de Coulangeon et Nebe [**CN13**]. Nous décrivons un algorithme efficace (Algorithme 3.2.6.1) dans le cas kleinéen, c'est-à-dire lorsque $A \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathcal{M}_2(\mathbb{C}) \times \mathbb{H}^r$, qui généralise l'algorithme de Voight, et nous proposons une amélioration utilisant un algorithme probabiliste. Les données expérimentales suggèrent que notre algorithme a pour complexité en temps

$$(\Delta_A/\Delta_F)^{2+o(1)}$$

lorsque le degré du corps de base est fixé. Cet algorithme est l'objet d'un article [**Pag13**] à paraître dans Mathematics of Computation. Ce travail a déjà été utilisé par plusieurs auteurs:

- Luzzi, Othman et Belfiore l'ont utilisé pour construire une procédure de réduction efficace pour certains codes MIMO [**LOB12**].
- Rivin s'est intéressé aux aspects probabilistes de l'algorithme dans [**Riv13, Riv12**].
- Rahm, Berkove et Şengün l'ont utilisé pour compléter certains de leur calculs dans [**RŞ13, Rah13, BR13**].
- Calegari et Venkatesh l'ont utilisé pour calculer certains exemples dans leur livre [**CV12**].
- Guitart, Masdeu et Şengün l'ont utilisé pour calculer des points de Darmon dans [**GMcS14**].

Problème de l'idéal principal. Étant donné un idéal à droite I d'un ordre $\mathcal{O}$ dans une algèbre centrale simple A sur un corps de nombres F, le problème de décider si I est principal et d'en trouver un générateur le cas échéant est appelé *problème de l'idéal principal* que nous abordons dans le chapitre 4. Dans le cas où $A = F$ est un corps de nombres, ce problème possède déjà de nombreuses applications en théorie algorithmique des nombres, parmi lesquelles: calcul de groupes de Selmer et descente explicite [**CFO$^+$11**], théorie des corps de classes effective [**Coh00**], résolution d'équations de Thue [**BH96**]. Dans les algèbres de quaternions, on a besoin d'une solution pour le problème de l'idéal principal pour calculer des opérateurs de Hecke agissant sur des espaces de formes modulaires de Hilbert [**DV13**] ou pour calculer des points CM sur des courbes de Shimura [**Voi06**].

Dans un corps quadratique imaginaire, l'algorithme dû à Hafner et McCurley [**HM89**] permet de résoudre le problème de l'idéal principal en temps sous-exponentiel, sous l'hypothèse de Riemann généralisée. La généralisation de cet algorithme aux corps de nombres arbitraires, due à Buchmann [**Buc90**], est heuristiquement aussi sous-exponentielle. Dans une algèbre de matrices $\mathcal{M}_d(F)$, le problème de l'idéal principal se ramène au corps de base via la théorie des classes de Steinitz et les pseudo-matrices [**Coh93**]. En général, le problème se sépare en deux cas: les algèbres définies et indéfinies. Dans le cas défini, Dembélé et Donnelly ont décrit un algorithme dont Voight et Kirschmer [**KV10**] ont prouvé qu'il était polynomial quand le corps de base est fixé. Dans le cas indéfini, le problème de décision se ramène au corps de base, mais trouver un générateur est difficile. Kirschmer et

Voight décrivent un algorithme pour les algèbres de quaternions, mais ils n'analysent pas sa complexité. Nous décrivons un algorithme général (Algorithme 4.1.0.2) pour résoudre le problème de l'idéal principal dans une algèbre à division, et nous démontrons le théorème suivant (Théorème 4.1.0.4).

THÉORÈME C. *Étant donné un $\mathcal{O}$-ideal à droite d'un ordre maximal $\mathcal{O}$ dans une algèbre à division sur $\mathbb{Q}$ et un générateur λ de $\mathrm{nrd}(I)$ qui est positif à toutes les places réelles qui ramifient dans A, l'Algorithme 4.1.0.2 renvoie un générateur x de I. Il termine en temps au plus*

$$\exp(O(d \log \Delta_A) + O_N(\log \log \Delta_A))$$

multiplié par un polynôme en la taille de l'entrée.

Il est naturel de chercher à adapter l'algorithme de Buchmann aux algèbres non-commutatives. En revanche, le fait que l'ensemble des idéaux à droite d'un ordre ne forme pas un groupe rend ce projet difficile. Nous surmontons cette difficulté en ajoutant un ingrédient local supplémentaire exprimé en termes d'action du groupe des unités sur des arbres de Bruhat–Tits. On ne peut pas prouver que l'algorithme que nous présentons (Algorithmes 4.2.1.14 et 4.2.1.19) est sous-exponentiel en l'absence de progrès sur l'algorithme de Buchmann. Nous formulons cependant des heuristiques sur son comportement, et nous montrons que l'algorithme est sous-exponentiel si ces heuristiques sont correctes. L'algorithme est rapide en pratique, et est l'objet d'un article [**Pag14**] accepté pour publication à ANTS-XI.

Les algorithmes que nous présentons dans cette thèse fournissent les ingrédients suffisants pour permettre des calculs explicites sur certaines formes automorphes en utilisant la formule de Matshushima et la correspondance de Jacquet–Langlands. Certains calculs de ce type ont été réalisés durant la thèse, mais seront publiés ultérieurement.

Introduction

Algebraic number theory. Algebraic number theory as it exists today was developed to solve arithmetic problems such as the following:

(i) Pell–Fermat equation: what are the solutions in integers x, y of the equation $x^2 - dy^2 = \pm 1$ when d is not a square?

(ii) Fermat's conjecture: does the equation $x^n + y^n = z^n$ have solutions in positive integers x, y, z when $n \geq 3$ is an integer?

(iii) Solvability by radicals: when is it possible to express the solutions of a polynomial equation $P(x) = 0$ only with the four arithmetic operations and extraction of roots?

(iv) For a positive integer n, which prime numbers can be written in the form $x^2 + ny^2$ with x, y integers?

The study of these problems has progressively led to the notion of an *algebraic number field* F, that is the set of numbers constructed by addition and multiplication from the rational numbers $\mathbb{Q}$ together with a root of a polynomial with integer coefficients. For instance, the problems above lead to the study of (i) $F = \mathbb{Q}(\sqrt{d})$, (ii) $F = \mathbb{Q}(\zeta)$ where ζ is a nontrivial n-th root of unity: $\zeta^n = 1$, (iii) $F = \mathbb{Q}(\alpha)$, where α is a root of the polynomial $P(x)$, and (iv) $F = \mathbb{Q}(\sqrt{-n})$. These problems are formulated in terms of integers, not in terms of rational numbers, so we need an analogue in number fields of what are the integers $\mathbb{Z}$ inside the rationals $\mathbb{Q}$: this is the *ring of algebraic integers* $\mathbb{Z}_F$ of F.

The problems we have just presented lead to the study of important arithmetic objects attached to number fields. The Pell–Fermat equation (i) reduces to the study of a first important invariant of the number field F: the *unit group* $\mathbb{Z}_F^\times$, that is the elements of $\mathbb{Z}_F$ whose inverses are also in $\mathbb{Z}_F$:

$$\frac{1}{x + \sqrt{d}y} = \frac{x - \sqrt{d}y}{(x + \sqrt{d}y)(x - \sqrt{d}y)} = \frac{x + \sqrt{d}y}{x^2 - dy^2} = \pm(x + \sqrt{d}y).$$

One of the first attempts to prove Fermat's conjecture consisted of factorizing the equation into

$$x^n = z^n - y^n = (z - y)(z - \zeta y)(z - \zeta^2 y) \cdots (z - \zeta^{n-1} y),$$

and factoring each side as products of "prime" numbers. Unfortunately, in rings such as $\mathbb{Z}_F = \mathbb{Z}[\zeta]$ the unique factorization property into a product of prime numbers no longer holds. We need to replace this property with a sophisticated substitute. For instance, two integers always have a greatest common divisor or GCD, and similarly we would like to find the GCD of two elements a and b in $\mathbb{Z}_F$. Such a GCD does not

always exist in $\mathbb{Z}_F$, but we can imagine an "ideal number" α that would be the GCD of a and b. This "ideal number" does not make sense, but we can make sense of the set of its multiples: this is what we call the ideal $\mathfrak{a} = (a, b)$ generated by a and b. The question of whether a and b actually have a GCD reduces to asking whether the ideal $\mathfrak{a}$ is principal, that is whether it is the set of multiples $\mathfrak{a} = (d)$ of a single element d that would then be a GCD of a and b. If we group together in a class the ideals that can be obtained one from another by multiplying with a principal ideal, we obtain a second important invariant, the *class group* $\mathrm{Cl}(F)$, which measures how much the unique factorization property fails in F.

The problem of solvability by radicals can be reduced to the study of the *Galois group* $\mathrm{Gal}(F/\mathbb{Q})$ that encodes the symetries of the equation $P(x) = 0$. The simplest groups of symetries are called abelian, and certain groups built from abelian groups in a simple way are called solvable, refering to the problem of solvability by radicals.

The problem of deciding whether a prime number p is of the form $x^2 + ny^2$ reduces to the problem of deciding whether the ideals dividing p in $F = \mathbb{Q}(\sqrt{-n})$ are principal. This property can be analysed with *class field theory*, which describes a deep link between two kinds of objects: on one hand the extensions of F, that is the number fields containing F, whose Galois group is abelian; and on the other hand the ray class groups, which are generalizations of the class group $\mathrm{Cl}(F)$. In particular, there exists an extension H of F called the *Hilbert class field*, satisfying $\mathrm{Gal}(H/F) \cong \mathrm{Cl}(F)$, and that controls the set of primes p that are solutions of (iv).

Our goal is to study non-commutative generalizations of algebraic number theory.

Noncommutative generalizations and arithmetic groups.

Central simple algebras. A first way to generalize algebraic number theory is to allow the multiplication to no longer be commutative: in a number field, we always have $ab = ba$. This generalization leads us to replace number fields with central simple algebras. Formally, if F is a number field, an algebra A over F is a F-vector space, equipped with an associative multiplication and a neutral element; the multiplication is required to be compatible with the vector space structure. We will assume that every algebra we consider is finite-dimensional. A *central simple algebra* is an algebra whose center equals $F \cdot 1_A$ and that does not have any nontrivial two-sided ideal. Central simple algebras arise naturally:

- The algebra $\mathcal{M}_n(F)$ of $n \times n$ matrices is central simple.
- If G is a finite group, the group algebra $F[G]$, which appears in the representation theory of G, is central simple.
- The endomorphism ring of an abelian variety is a direct sum of central simple algebras.
- Every division algebra over $\mathbb{Q}$, which means such that every nonzero element has a multiplicative inverse, is simple and its center is a number field.

A central simple algebra A has an analogue of the ring of integers $\mathbb{Z}_F$: a *maximal order* $\mathcal{O}$. An order in A is an "integral version" of A: formally, a finitely generated sub-$\mathbb{Z}$-module $\mathcal{O}$ that contains 1, that is stable under multiplication, and such

that $F\mathcal{O} = A$. An order is called maximal if it is not contained in a strictly larger order. However, because of non-commutativity, maximal orders are not unique: there are several maximal orders in A (if $A \neq F$), there are even infinitely many of them! We can obtain other orders $x^{-1}\mathcal{O}x$ by conjugating any given one. However, there are only finitely many conjugacy classes of maximal orders.

The classical invariants of algebraic number theory have an analogue in this context. We may consider the group of units $\mathcal{O}^\times$. There is a notion of a right ideal I of $\mathcal{O}$ (or left ideal, in general not the same because of non-commutativity), and of a principal right ideal $I = x\mathcal{O}$. We can then study the set $\mathrm{Cl}(\mathcal{O})$ of right ideal classes. However, because of non-commutativity, $\mathrm{Cl}(\mathcal{O})$ is not a group!

Automorphic forms and arithmetic groups. I will not give precise definitions in this section, since we do not directly use automorphic forms in this thesis. Another way to generalize algebraic number theory is to consider class field theory, which provides a description of abelian extensions of a number field F. We would like to have an analogue that would describe the extensions of F whose Galois group is not necessarily commutative. As expected, this is extremely difficult and an area of active research. Here is a way to attack this problem. One perspective on class field theory is that it describes the characters of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$, i.e. continuous homomorphisms

$$\mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathbb{C}^\times = \mathrm{GL}_1(\mathbb{C}),$$

in terms of characters of ray class groups. We can generalize this by studying higher dimensional Galois representations: continuous homomorphisms

$$\mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_n(\mathbb{C}).$$

This is the point of view of a vast set of conjectures known as the Langlands programme, where we replace the characters of ray class groups with *automorphic forms*, which are analytic functions that transform in a prescribed manner under the action of *arithmetic groups*. Loosely speaking, arithmetic groups are the sets of integral points of algebraic groups defined over $\mathbb{Q}$. More precisely, let $\mathbb{G} \subset \mathrm{GL}_n$ be an algebraic group over $\mathbb{Q}$, that is a subgroup defined by polynomial equations with rational coefficients. We can then define $\mathbb{G}(\mathbb{Z}) = \mathbb{G}(\mathbb{Q}) \cap \mathrm{GL}_n(\mathbb{Z})$. A subgroup $\Gamma \subset \mathbb{G}(\mathbb{Q})$ is said to be *arithmetic* if it is commensurable with $\mathbb{G}(\mathbb{Z})$, that is the intersection $\Gamma \cap \mathbb{G}(\mathbb{Z})$ has finite index in both groups. The most classical example of an arithmetic group is $\mathrm{SL}_2(\mathbb{Z})$, which plays a central role in the theory of modular forms. Another important example of arithmetic group of interest to us in this thesis is the group of units $\mathcal{O}^\times$ of an order in a central simple algebra.

The link between Galois representations and automorphic forms can be expressed in terms of *L-functions*. These are functions of a complex variable generalizing the Riemann zeta function. We construct them from a certain type of generating series adapted to arithmetic questions. Given a Galois representation or an automorphic eigenform, we can attach an L-function, and we conjecture that the L-functions

coming from Galois constructions and automorphic constructions are actually the same.

Our goal is to describe algorithms to study central simple algebras, and the arithmetic groups and automorphic forms that are attached to them.

Explicit methods.

Approach. In all the problems that we consider in this thesis, we present two kinds of algorithms:

- algorithms of which we prove the complexity but that are not efficient in practice;
- deterministic or probabilistic algorithms that are efficient in practice but whose correctness or complexity is heuristic, in interesting special cases.

This dichotomy reflects the fact that the problems we consider are difficult: at the moment we cannot describe fast algorithms and prove that they are. Note that for these problems, complexity proofs are rare in the literature. In this these, the algorithmic complexity is the *binary complexity*: we count the number of elementary binary operations as a function of the binary size of the input. On top of that, we have implemented all the efficient algorithms in Magma, and we compared them to existing algorithms and implementations when it was possible. Our algorithms are both faster and more general than existing ones.

Generators of S-units. Let S be a finite set of places of a number field F. The first problem we consider asks whether the group of S-units $\mathcal{O}_S^\times$ of a maximal order $\mathcal{O}$ in a central simple algebra A over F can be generated by elements of small height, where "small" means logarithmic in the discriminant of A. The classical example of real quadratic fields shows that height of the fundamental units can be of order a power of the discriminant, which prevents us from manipulating these units directly as linear combinations of the vectors of an integral basis: we need to use a compact representation as products of S-units. This problem was considered by Lenstra [**Len92**] in the case of number fields. By using techniques of geometry of numbers, he proves the following theorem.

Theorem (Lenstra). *Let F be a number field with r_2 complex places and discriminant Δ_F. Let $\mathbb{Z}_F$ be the ring of integers of F, and let S be a finite set of places of F containing every infinite place and every finite place $\mathfrak{p}$ such that*

$$N(\mathfrak{p}) \leq (2/\pi)^{r_2}|\Delta_F|^{1/2}.$$

Let m_S be the maximum of the norms of primes in S or $m_S = 1$ if S contains no finite place. Then the group of S-units $\mathbb{Z}_{F,S}^\times$ is generated by its elements with logarithmic height less than or equal to

$$\frac{1}{2}\log|\Delta_F| + \log m_S + r_2 \log\Big(\frac{2}{\pi}\Big).$$

In a recent article [**CS12**], Chinburg and Stover define a notion of height on a division algebra, and by using the same technique they prove a generalization to division algebras over $\mathbb{Q}$. In the following two theorems, we let F be a number field of

degree n and A be a central division algebra over F with absolute discriminant Δ_A, such that r real places of F ramify in A, and $\mathcal{O}$ is a maximal order in A. For a finite set S of places of F we let m_S be the maximum of the norms of primes in S and $m_S = 1$ if there is none. The explicit constants mentionned at the beginning of the theorems depend only on n and d.

THEOREM (Chinburg–Stover). *There exist explicit constants $f_1(n,d)$ and $f_2(n,d)$ such that the following holds. Define*

$$e = \frac{n}{d(2n-r)}.$$

We have $1/(2d) \leq e \leq 1/d$. Let $\mathcal{O}$ be a maximal order in A, and S a finite set of places of F containing every infinite place and every prime $\mathfrak{p}$ such that

$$N(\mathfrak{p}) \leq f_1(n,d)\Delta_A^e.$$

Then the group $\mathcal{O}_S^\times$ is generated by its elements of logarithmic height less than or equal to

$$e\log(\Delta_A) + \log m_S + f_2(n,d).$$

By using properties of representation theory, we prove new bounds on the size of generators of the group $\mathcal{O}_S^1$ of S-units of reduced norm 1 for arbitrary sets of places S and for the group $\mathcal{O}_S^\times$ of S-units with bounds on S depending only on F. In Chapter 2, we prove the following theorem (Theorem 2.4.2.4 and Theorem 2.4.3.4). For the sake of simplicity we state a weaker version.

THEOREM A. *There exist explicit constants $g_1(n,d)$, $g_2(n,d)$, $g_3(n,d)$ and $g_4(n,d)$ such that the following holds. Let S a finite set of places of F containing every infinite place. Then the group $\mathcal{O}_S^1$ is generated by its elements of logarithmic height less than or equal to*

$$g_1(n,d)\log(\Delta_A) + \log m_S + g_2(n,d),$$

and we have $2/d \leq g_1(n,d) \leq 803/d$. Assume in addition that S contains every finite place $\mathfrak{p}$ such that

$$N(\mathfrak{p}) \leq (2/\pi)^{r_2}|\Delta_F|^{1/2}.$$

Then the group $\mathcal{O}_S^\times$ is generated by its elements of logarithmic height less than or equal to

$$g_3(n,d)\log(\Delta_A) + (r+1)\log m_S + g_4(n,d).$$

Computation of unit groups. We then consider the problem of computing a unit group $\Gamma = \mathcal{O}^1$, where "compute" means computing a finite presentation of Γ with a computable isomorphism. In particular this contains the problem of computing a finite set of generators. Note that in some cases, the group considered is finite: this is the case for the group units of reduced norm 1 in a totally definite quaternion algebra. Regarding theoretical algorithms, Grunewald and Segal described an algorithm that can compute an arbitrary arithmetic group [**GS80**], but it is not practical and its complexity is unknown. We know only two results that prove the complexity of an algorithm for computing some unit groups. The first one is due to Swan [**Swa71**] who

describes an algorithm that computes the group $\mathrm{SL}_2(\mathbb{Z}_F)$ where $\mathbb{Z}_F$ is a quadratic imaginary field, and he proves that the running time is of order $\Delta_F^{O(1)}$, which is optimal up to the exponent. The second one is attributed to Chalk in a paper of Jahangiri [**Jah10**]: he considers some specific unit groups in quaternion algebras over $\mathbb{Q}$, and the complexity is of the form $\exp(O(\Delta_A))$. In Chapter 3, we use our bounds from the previous chapter to present an algorithm (Algorithm 3.1.2.8) and we prove the following theorem (Theorem 3.1.2.9).

THEOREM B. *Let A be a central division algebra of degree d over a number field F. Assume that A is not a totally definite quaternion algebra. Given a maximal order $\mathcal{O}$ in A, Algorithm 3.1.2.8 returns a finitely presented group Γ, and two computable group isomorphisms $\phi : \Gamma \to \mathcal{O}^1$ and $\psi : \mathcal{O}^1 \to \Gamma$, inverse of each other. The algorithm terminates in time at most*

$$\exp\Big(O(d \log \Delta_A) + O_N(\log\log \Delta_A)\Big).$$

Regarding efficient algorithms, there is an abundant literature, most of which only consider cases where the algebraic group is isotropic; in our case this means that A is not a division algebra. Considering division algebras, Voight [**Voi09**] describes an efficient algorithm in the Fuchsian case, that is when $A \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathcal{M}_2(\mathbb{R}) \times \mathbb{H}^r$. It appears that the only algorithm in the general case is due to Coulangeon and Nebe [**CN13**]. We describe an efficient algorithm (Algorithm 3.2.6.1) for the Kleinian case, that is when $A \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathcal{M}_2(\mathbb{C}) \times \mathbb{H}^r$, which generalizes Voight's algorithm, and we present an improvement using a probabilistic algorithm. Experimental data suggest that our algorithm has time complexity

$$(\Delta_A/\Delta_F)^{2+o(1)}$$

when the degree of the base field is fixed. This algorithm was published in a paper [**Pag13**] to appear in Mathematics of Computation. This work has already been used by several authors:

- Luzzi, Othman and Belfiore have used it to construct an efficient reduction procedure for some space-time codes [**LOB12**].
- Rivin was interested in some randomness aspects of the algorithm [**Riv13, Riv12**].
- Rahm, Berkove and Şengün have used it to complement some of their computations in [**RŞ13, Rah13, BR13**].
- Calegari and Venkatesh have used it to compute some examples in [**CV12**].
- Guitart, Masdeu and Şengün have used it to compute Darmon points in [**GMcS14**].

Principal ideal problem. Given a right ideal I of an order $\mathcal{O}$ in a central simple algebra A over a number field F, the problem of deciding whether I is principal and finding a generator in that case is called the *principal ideal problem*. We consider this in Chapter 4. When $A = F$ is a number field, this problem already has many applications in algorithmic number theory: computation of Selmer groups and explicit descent [**CFO$^+$11**], effective class field theory [**Coh00**] and solving Thue

equations [**BH96**]. In quaternion algebras, solving the principal ideal problem allows computing Hecke operators acting on spaces of Hilbert modular forms [**DV13**], or computing CM points on Shimura curves [**Voi06**].

In an imaginary quadratic field, Hafner and McCurley's algorithm [**HM89**] solves the principal ideal problem in subexponential time, under the Generalized Riemann Hypothesis. The generalization of this algorithm to arbitrary number fields, due to Buchmann [**Buc90**], is heuristically also subexponential. In a matrix algebra $\mathcal{M}_d(F)$, the principal ideal problem reduces to that in the base field via the theory of Steinitz classes and pseudomatrices [**Coh93**]. In general, the problem naturally splits into two cases: definite and indefinite algebras. In the definite case, Dembélé and Donnelly described an algorithm, and Voight and Kirschmer [**KV10**] proved that this algorithm was polynomial when the base field is fixed. In the indefinite case, the decision problem reduces to that in the base field, but finding a generator is hard. Kirschmer and Voight describe an algorithm for quaternion algebras, but they do not analyse its complexity. We describe a general algorithm (Algorithm 4.1.0.2) that solves the principal ideal problem in a division algebra, and we prove the following theorem (Theorem 4.1.0.4).

THEOREM C. *Given a right $\mathcal{O}$-ideal I for some maximal order $\mathcal{O}$ of a division algebra over $\mathbb{Q}$, and a generator λ of* $\mathrm{nrd}(I)$ *that is positive at every ramified real place, Algorithm 4.1.0.2 returns a generator x of I. It terminates in time at most*

$$\exp(O(d \log \Delta_A) + O_N(\log \log \Delta_A))$$

times a polynomial in the size of the input.

It is a natural idea to try and adapt Buchmann's algorithm to non-commutative algebras. However, the fact that the set of right ideals of an order is not a group makes this task difficult. We overcome this difficulty by adding a local algorithm expressed in terms of the action of the unit group on Bruhat–Tits trees. We cannot prove that the algorithm we present (Algorithms 4.2.1.14 and 4.2.1.19) is subexponential without significant progress on understanding Buchmann's algorithm. However we are able to formulate heuristics on its behaviour, and we show that the algorithm is subexponential if these heuristics are correct. The algorithm is fast in practice, and it is published in a paper [**Pag14**] accepted for publication at ANTS-XI.

The algorithms presented in this thesis allow explicit computations of certain automorphic forms using Matsushima's formula and the Jacquet–Langlands correspondence. We have carried out such computations during our PhD, but we will publish them in a later work.

Contents

CHAPTER 1

Background

1. Central simple algebras over number fields

1.1. Number fields.

General references for this section are [**Coh93**], [**Bel05**] and [**Ser62**].

Local fields. In this section we fix some notations and recall standard definitions for local fields. Let F be a characteristic zero local field, that is, a non-discrete, locally compact Hausdorff topological field. Such a field is always a finite extension of $\mathbb{Q}_p$ for some prime p or $p = \infty$ with the convention that $\mathbb{Q}_\infty = \mathbb{R}$. Every local field that we will consider in this thesis will have characteristic zero, so from now on we will simply write "local field" for "characteristic zero local field". We normalize the absolute value on F so it agrees with the standard absolute value on $\mathbb{Q}_p$: $|p| = p^{-1}$ if $p \neq \infty$ and $|2| = 2$ otherwise. When F is nonarchimedean, we let $\mathbb{Z}_F$ be its ring of integers, π a uniformizer, v the valuation such that $v(\pi) = 1$, q the cardinality of the residue field $\mathbb{F} = \mathbb{Z}_F/\pi\mathbb{Z}_F$. With this normalization we have $|\pi| = q^{-1/[F:\mathbb{Q}_p]}$ and $|x| = q^{-v(x)/[F:\mathbb{Q}_p]}$ for all $x \in F$.

To make the discussion of heights in central simple algebras simpler, we define a height on local fields as follows: the *height* of an element $x \in F$ is

$$\mathrm{H}_F(x) = \max\Big(1, |x|\Big)^{[F:\mathbb{Q}_p]},$$

and its *logarithmic height* is $\mathrm{h}_F(x) = \log \mathrm{H}_F(x)$.

Let L/F be an extension of nonarchimedean local fields of degree n. We say that the extension L/F is *unramified* if π is a uniformizer in $\mathbb{Z}_L$. In this case, the corresponding extension of residue fields $\mathbb{L}/\mathbb{F}$ is also of degree n, and we have an isomorphism $\mathrm{Gal}(L/F) \cong \mathrm{Gal}(\mathbb{L}/\mathbb{F})$ induced by reduction modulo π. We call the preimage of the Frobenius automorphism $x \mapsto x^q$ in $\mathrm{Gal}(L/F)$ the Frobenius automorphism and we denot it Frob.

Number fields. We fix some notations and recall standard definitions for number fields. Let now F be a number field of degree n over $\mathbb{Q}$, let $\mathbb{Z}_F$ be its ring of integers, and let Δ_F be its discriminant. Let $\mathcal{V}_F$ be the set of *places* of F, that is the set of equivalence classes of absolute values on F. This set is partitioned into the set $\mathcal{V}_f$ of *finite* places, which is in bijection with the set of prime ideals of $\mathbb{Z}_F$, and the set $\mathcal{V}_\infty$ of *infinite* places, which is in bijection with the set of embeddings of F into $\mathbb{C}$ up to conjugation. An infinite place is *real* or *complex* depending on whether the image of the corresponding embedding is contained in $\mathbb{R}$ or not. We write r_1 for the number of real embeddings and r_2 for the number of complex embeddings, so that $n = r_1 + 2r_2$.

Let v be a place of F. Let F_v be the completion of F with respect to an absolute value corresponding to v. We write every object attached to F_v as a local field with a subscript v: $|\cdot|_v$, $\mathbb{Z}_{F,v}$, $\mathbb{F}_v$, etc. Note that with our convention for absolute values, the product formula takes the following form: for all $x \in F^\times$, we have

$$\prod_{v \in \mathcal{V}_F} |x|_v^{[F_v:\mathbb{Q}_p]} = 1.$$

Let S be a finite set of places of F containing $\mathcal{V}_\infty$. The ring $\mathbb{Z}_{F,S}$ of *S-integers* of F is the set of $x \in F$ such that $|x|_v \leq 1$ for all $v \notin S$. The condition $|x|_v \leq 1$ is equivalent to $x \in \mathbb{Z}_{F,v}$. The group $\mathbb{Z}_{F,S}^\times$ of *S-units* in F is the unit group of $\mathbb{Z}_{F,S}$; it is a finitely generated group of rank $\#S - 1$.

The *height* of an element $x \in F$ is

$$\mathrm{H}_F(x) = \prod_{v \in \mathcal{V}_F} \mathrm{H}_{F_v}(x) = \prod_{v \in \mathcal{V}_F} \max\bigl(1, |x|_v\bigr)^{[F_v:\mathbb{Q}_p]},$$

and its *logarithmic height* is $\mathrm{h}_F(x) = \log \mathrm{H}_F(x)$. The height has the following properties:

Proposition 1.1.1.1. *Let F be a number field of degree n over $\mathbb{Q}$.*

(i) For all $B > 0$, the set $\{x \in F \mid \mathrm{H}_F(x) \leq B\}$ is finite.

(ii) For all $x, y \in F$,

$$\mathrm{H}_F(xy) \leq \mathrm{H}_F(x)\mathrm{H}_F(y).$$

(iii) If L/F is a finite extension and $x \in F$, then

$$\mathrm{H}_L(x) = \mathrm{H}_F(x)^{[L:F]}.$$

(iv) If $x \in F^\times$ satisfies $\mathrm{H}_F(x) = 1$, then x is a root of unity.

Proof. [**HS00**, Theorem B.2.3, Lemma B.2.1 and Corollary B.2.3.1] □

Let L/F be a finite extension of number fields. Let v be a place of F and w be a place of L. We say that w *divides* v and we write $w \mid v$ if $|\cdot|_w$ agrees with $|\cdot|_v$ on F. For any place v of F, we have the relation $\sum_{w|v}[L_w : F_v] = [L : F]$.

Class groups. Let F be a number field. A *fractional ideal* of F is a submodule $\mathfrak{a}$ of F such that there exists a nonzero integer d such that $d\mathfrak{a}$ is a nonzero ideal of $\mathbb{Z}_F$. Given two fractional ideals $\mathfrak{a}, \mathfrak{b}$ of F, their *product* $\mathfrak{ab}$ is the $\mathbb{Z}$-module generated by all the products ab where $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. Given a fractional ideal $\mathfrak{a}$ of F, its *inverse* is the set $\mathfrak{a}^{-1} = \{x \in F \mid x\mathfrak{a} \subset F\}$. It is again a fractional ideal of F, and we have $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a} = \mathbb{Z}_F$. The set of fractional ideals forms a group under multiplication, the neutral element being $\mathbb{Z}_F$. An ideal $\mathfrak{a}$ of F is *principal* if there exists $x \in F$ such that $\mathfrak{a} = x\mathbb{Z}_F$. The set of principal ideals is a subgroup of the group of fractional ideals of F, and the quotient is finite: this quotient is called the *class group* $\mathrm{Cl}(F)$ of F. More generally, a *modulus* is a pair $\mathfrak{M} = (\mathfrak{M}_f, \mathfrak{M}_\infty)$ where $\mathfrak{M}_f$ is an integral ideal of $\mathbb{Z}_F$ and $\mathfrak{M}_\infty$ is a set of real embeddings of F. If $\mathfrak{a}$ is a fractional ideal of F, we say that $\mathfrak{a}$ is *coprime to* $\mathfrak{M}$ if $\mathfrak{a}$ is coprime to $\mathfrak{M}_f$, i.e. if $v_\mathfrak{p}(\mathfrak{a}) = 0$ for all primes $\mathfrak{p}$ dividing $\mathfrak{M}_f$. An element $x \in F$ is *congruent to* 1 *modulo* $\mathfrak{M}$ if $v_\mathfrak{p}(x - 1) \geq v_\mathfrak{p}(\mathfrak{M}_f)$ for all primes $\mathfrak{p}$ dividing $\mathfrak{M}_f$ and $\sigma(x) > 0$ for

all embeddings $\sigma \in \mathfrak{M}_\infty$. Let $I_{\mathfrak{M}}(F)$ be the set of fractional ideals of F that are coprime to $\mathfrak{M}$; it is a subgroup of the group of ideals of $\mathfrak{M}$. Let $P_{\mathfrak{M}}(F)$ be the set of fractional ideals of F that are principal and generated by an element $x \in F$ that is congruent to 1 modulo $\mathfrak{M}$; it is a subgroup of $I_{\mathfrak{M}}(F)$. The *ray class group* of modulus $\mathfrak{M}$ is the quotient $\mathrm{Cl}_{\mathfrak{M}}(F) = I_{\mathfrak{M}}(F)/P_{\mathfrak{M}}(F)$; it is a finite group.

Adèles. In this section, we present the notion of adèles and idèles of a number field.

Let $(G_i)_{i\in I}$ be a family of locally compact Hausdorff topological groups and let $(H_i)_{i\in J}$ a family of compact open subgroups of G_i, where J is a cofinite subset of I. The *restricted product* of the G_i with respect of the H_i is the subgroup G of the direct product $\prod_{i\in I} G_i$ defined by

$$G = \{g = (g_i) \in \prod_{i\in I} G_i \mid g_i \in H_i \text{ for almost all } i \in I\}.$$

The restricted product topology on G is defined by taking as a system of neighborhoods of the identity the sets $\prod_{i\in I} U_i$, where for all $i \in I$ the set U_i is an open neighborhood of the identity in G_i, and for almost all $i \in I$ we have $U_i = H_i$. The group G defined in this way is locally compact.

Let F be a number field. The *ring of adèles* $\mathbb{A}_F$ of F is the restricted product of the additive groups $(F_v)_{v\in\mathcal{V}_F}$ with respect to the compact open subgroups $(\mathbb{Z}_{F,v})_{v\in\mathcal{V}_f}$, equipped with the componentwise multiplication. It is a topological ring. The field F embeds into $\mathbb{A}_F$ diagonally, and unless stated otherwise we will always use the diagonal embedding. The subgroup $F \subset \mathbb{A}_F$ is discrete, and the quotient $F\backslash\mathbb{A}_F$ is compact.

The *group of idèles* $\mathbb{A}_F^\times$ of F is the restricted product of the multiplicative groups $(F_v^\times)_{v\in\mathcal{V}_F}$ with respect to the compact open subgroups $(\mathbb{Z}_{F,v}^\times)_{v\in\mathcal{V}_f}$. It is the group of invertible elements in the ring $\mathbb{A}_F$, but the topology on $\mathbb{A}_F^\times$ is not the topology induced by the inclusion $\mathbb{A}_F^\times \subset \mathbb{A}_F$: it is the topology induced from the embedding $\mathbb{A}_F^\times \hookrightarrow \mathbb{A}_F \times \mathbb{A}_F$ given by $x \mapsto (x, x^{-1})$. The group $F^\times$ embeds into $\mathbb{A}_F^\times$ diagonally as a discrete subgroup, but the quotient $F^\times\backslash\mathbb{A}_F^\times$ is not compact. The reason is the existence of the continuous surjective homomorphism

$$\begin{array}{rccc} \nu: & \mathbb{A}_F^\times & \longrightarrow & \mathbb{R}_{>0} \\ & x & \longmapsto & \prod_{v\in\mathcal{V}_F} |x|_v^{[F_v:\mathbb{Q}_p]} \end{array}$$

that factors through the quotient $F^\times\backslash\mathbb{A}_F^\times$ by the product formula. However, the quotient $F^\times\backslash \ker\nu$ is compact.

The main interest of adèles is that integrality becomes an open condition. For instance, let S be a finite set of places containing $\mathcal{V}_\infty$. Let U be the set

$$U = \prod_{v\in S} F_v \times \prod_{v\notin S} \mathbb{Z}_{F,v} \subset \mathbb{A}_F.$$

Then U is open in $\mathbb{A}_F$, and $U \cap F = \mathbb{Z}_{F,S}$ is the ring of S-integral elements. Similarly, let W be the set

$$W = \prod_{v \in S} F_v^\times \times \prod_{v \notin S} \mathbb{Z}_{F,v}^\times \subset \mathbb{A}_F^\times.$$

Then W is open in $\mathbb{A}_F^\times$, and $W \cap F^\times = \mathbb{Z}_{F,S}^\times$ is the group of S-units.

As a consequence, topological properties capture arithmetic information. For instance, let $\mathfrak{M}$ be a modulus and consider the group $I_{\mathfrak{M}}(F)$ of fractional ideals of F that are coprime to $\mathfrak{M}$. Let H, K be the open subgroups

$$H = \prod_{v \in \mathfrak{M}_\infty} \mathbb{R}_{>0} \times \prod_{v | \mathfrak{M}_f} (1 + \pi_v^{v(\mathfrak{M}_f)} \mathbb{Z}_{F,v}) \times \prod_{v \nmid \mathfrak{M}} F_v^\times \subset \mathbb{A}_F^\times,$$

and

$$K = \prod_{v \in \mathcal{V}_\infty} F_v^\times \times \prod_{v \in \mathcal{V}_f} \mathbb{Z}_{F,v}^\times \subset \mathbb{A}_F^\times,$$

and let R be the open subring

$$R = \prod_{v \in \mathcal{V}_\infty} F_v \times \prod_{v \in \mathcal{V}_f} \mathbb{Z}_{F,v} \subset \mathbb{A}_F.$$

Since the restriction of ν to $F_v^\times$ is surjective for any $v \in \mathcal{V}_\infty$, the quotient $F^\times K \backslash \mathbb{A}_F^\times$ is compact. Since K is opent, the quotient is also discrete, so it is finite. Since H is open in $\mathbb{A}_F^\times$ the quotient $(H \cap F^\times K) \backslash H$ is also finite. But we have a group isomorphism

$$\begin{array}{rccc} j: & (H \cap K)\backslash H & \longrightarrow & I_{\mathfrak{M}}(F) \\ & x & \longmapsto & F \cap Rx \end{array}$$

satisfying $j(F^\times) = P_{\mathfrak{M}}(F)$, so that the quotient $(H \cap F^\times K)\backslash H$ is isomorphic to the ray class group $\mathrm{Cl}_{\mathfrak{M}}(F)$: the fact that the quotient $F^\times \backslash \ker \nu$ is compact implies that the ray class groups are finite.

1.2. Central simple algebras. The main references for this section are [**Rei03**] and [**PR94**, Sections 1.4 and 1.5]. Let F be a field. Let A be a finite dimensional associative unital algebra over F. We say that A is *central* if the center of A is F. We say that A is *simple* if it has no nontrivial two-sided ideals. We say that A is a *division algebra* if every nonzero elements admits an inverse; a division algebra is always simple.

Every (finite-dimensional) central simple algebra A is isomorphic to $\mathcal{M}_n(D)$ for an integer n and a central division algebra D that are uniquely determined by the isomorphism class of A. The matrix algebra $\mathcal{M}_n(F)$ is central simple over F. Over an algebraically closed field, we always have $D = F$: every central simple algebra is isomorphic to a matrix algebra over F. If A is a central simple algebra over F and L/F is a field extension, then $A \otimes_F L$ is a central simple algebra over L. The dimension of a central simple algebra is always a square d^2 and the integer d is called the *degree* of the algebra. Let $x \in A$ and let $\phi : A \otimes_F F^{\mathrm{al}} \to \mathcal{M}_d(F^{\mathrm{al}})$ be an isomorphism. Then the trace (resp. norm, characteristic polynomial) of $\phi(x)$ actually lie in F (resp. F, $F[X]$) and depend only on x, not on the choice of ϕ. We call them the *reduced trace* $\mathrm{trd}(x)$ (resp. *reduced norm* $\mathrm{nrd}(x)$, *reduced characteristic*

polynomial) of x. The reduced trace is a linear form on A. The reduced norm is multiplicative and x is invertible if and only if $\mathrm{nrd}(x)$ is nonzero. The reduced characteristic polynomial P of x satisfies $P(x) = 0$. When $\mathcal{R}$ is a subring of a central simple algebra, we write $\mathcal{R}^1$ the group of elements of reduced norm 1. We say that an extension L of F is a *splitting field* of A if $A \otimes_F L \cong \mathcal{M}_d(L)$. Let L be a subfield of A containing F. Then the degree $[L : F]$ divides d. If there is equality, then L is a splitting field of A.

As an example, suppose in this paragraph that the characteristic of F is not 2. Let $a, b \in F^\times$ and let A be the algebra $F + Fi + Fj + Fij$ with multiplication given by $i^2 = a$, $j^2 = b$ and $ij = -ji$. Then A is a central simple algebra of degree 2 over F, called the *quaternion algebra* $\left(\frac{a,b}{F}\right)$.

More generally, let L/F be an cyclic extension of degree d with Galois group generated by an element σ, and let $b \in F^\times$. Let A be the algebra $\oplus_{i=0}^{n-1} u^i L$ with multiplication given by $u^n = b$ and $\lambda u = u\sigma(\lambda)$ for all $\lambda \in L$. Then A is a central simple algebra over F, called the *cyclic algebra* $(L/F, \sigma, b)$.

Orders and ideals. Let R be a Dedekind ring and let $F = \mathrm{Frac}\, R$. An *R-lattice* (or simply *lattice* if the ring is clear from the context) in a finite-dimensional F-vector space V is a finitely generated R-submodule L such that $FL = V$. An *R-order* $\mathcal{O}$ (or simply *order*) in a central simple algebra A over F is a lattice in A that is also a subring with unit. If I is a lattice in A, we define its *right order* (resp. *left order*) to be $\mathcal{O}_r(I) = \{x \in A \mid Ix \subset I\}$ (resp. $\mathcal{O}_l(I) = \{x \in A \mid xI \subset I\}$). A *right $\mathcal{O}$-ideal* (resp. *left $\mathcal{O}$-ideal*) is a lattice I in A such that $\mathcal{O}_r(I) = \mathcal{O}$ (resp. $\mathcal{O}_l(I) = \mathcal{O}$). A right or left $\mathcal{O}$-ideal I is *integral* if $I \subset \mathcal{O}$. It is *two-sided* if $\mathcal{O}_r(I) = \mathcal{O}_l(I)$. The inverse I^{-1} of I is $\{x \in A \mid IxI \subset I\}$. If I, J are lattices, the product IJ is the lattice generated by the set $\{xy : x \in I, y \in J\}$. This notion is only well-behaved when $\mathcal{O}_r(I) = \mathcal{O}_l(J)$, so we call the product *compatible* in this case. The *reduced norm* $\mathrm{nrd}(I)$ of a right or left $\mathcal{O}$-ideal I is the R-submodule of F generated by the reduced norms of elements in I: it is a fractional ideal. The reduced norm of ideals is multiplicative for compatible products. When F is a number field, the *absolute norm* $N_{A/\mathbb{Q}}(L) \in \mathbb{Q}_{>0}$ of a lattice $L \subset A$ is the positive generator of the $\mathbb{Z}$-module generated by the absolute norms of elements in L. The absolute norm is multiplicative for compatible products.

The Brauer group. The tensor product of two central simple algebras is again central simple. Let A be a central simple algebra of degree d. Then its *opposite algebra* A^{opp} is the algebra with the same underlying vector space as A but with multiplication reversed. We have $A \otimes_F A^{\mathrm{opp}} \cong \mathcal{M}_{d^2}(F)$. Two central simple algebras A, B over F are called *similar* if there exist integers m, n such that $\mathcal{M}_m(A) \cong \mathcal{M}_n(B)$. The set of similarity classes of central simple algebras over F forms a group with multiplication induced by the tensor product, called the *Brauer group* $\mathrm{Br}(F)$ of F. As we have seen, any element of the Brauer group is always represented by a unique central division algebra.

We now define Hasse invariants at the infinite places. As we have seen, the Brauer group of an algebraically closed field is trivial. In particular, $\mathrm{Br}(\mathbb{C}) = 0$. We

define the *Hasse invariant* of a central simple algebra over $\mathbb{C}$ to be $0 \in \mathbb{Q}/\mathbb{Z}$. Over $\mathbb{R}$, there is a nontrivial division algebra $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$, called the algebra of Hamiltonian quaternions. The Brauer group of $\mathbb{R}$ has exactly 2 elements, the nontrivial one being represented by $\mathbb{H}$. We define the *Hasse invariant* $h(A)$ of a central simple algebra A over $\mathbb{R}$ to be 0 if it is isomorphic to a matrix algebra and $\frac{1}{2}$ otherwise. This defines an isomorphism

$$h : \mathrm{Br}(\mathbb{R}) \to \tfrac{1}{2}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}.$$

Central simple algebras over local fields. Let F be a nonarchimedean local field and let A be a central simple algebra of degree d over F. Let L be the unique unramified extension of F of degree d. Then A is isomorphic to the cyclic algebra $(L/F, \mathrm{Frob}, \pi^k)$ for some $k \in \mathbb{Z}$. We define the *Hasse invariant* of A to be $h(A) = \frac{k}{d} \in \mathbb{Q}/\mathbb{Z}$. This defines an isomorphism

$$h : \mathrm{Br}(F) \to \mathbb{Q}/\mathbb{Z}.$$

Now let D be a central division algebra of degree e over F. For all $x \in D$, define $w(x) = v(\mathrm{nrd}(x))$: this defines a discrete valuation w on D. The set $\Lambda = \{x \in D \mid w(x) \geq 0\}$ is the unique maximal order of D. There exists elements $\Pi \in \Lambda$ such that $w(\Pi) = 1$. We call such an element a *uniformizer*, and we fix one. Then every Λ-ideal is two-sided, of the form $\Pi^k\Lambda = \Lambda\Pi^k$ for some $k \in \mathbb{Z}$. The ideal $\Pi\Lambda = \{x \in D \mid w(x) > 0\}$ is the unique maximal ideal of Λ and we have $\Lambda^\times = \Lambda \smallsetminus \Pi\Lambda = \{x \in D \mid w(x) = 0\}$. The residue field $\Lambda/\Pi\Lambda$ is the unique extension of degree e of the residue field $\mathbb{F}$. We also define an absolute value on D that extends the one on F: for all $x \in D$ we set $|x| = |\mathrm{nrd}(x)|^{1/e}$. Finally, the group $D^1 = \Lambda^1$ is compact.

Let $A = \mathcal{M}_d(D)$ and $\mathcal{O} = \mathcal{M}_d(\Lambda)$. On one hand, we have the groups A^1 and $\mathcal{O}^1$ that are the kernel of the reduced norm on $A^\times$ and $\mathcal{O}^\times$ respectively. On the other hand, we have the groups $\mathrm{E}_d(D)$ and $\mathrm{E}_d(\Lambda)$ generated by the elementary matrices, that is the matrices with diagonal $(1, \ldots, 1)$ and exactly one non-zero off-diagonal coefficient. It is clear that $\mathrm{E}_d(D) \subset A^1$ and $\mathrm{E}_d(\Lambda) \subset \mathcal{O}^1$, but there is in fact equality. We will write these groups $\mathrm{SL}_d(D)$ and $\mathrm{SL}_d(\Lambda)$, respectively.

Central simple algebras over number fields. Let F be a number field and let A be a central simple algebra over F. For every place v of F, let $A_v = A \otimes_F F_v$; we define the local Hasse invariant at v to be $h_v(A) = h(A_v)$. The Hasse invariant of A is trivial for almost all places. Every central simple algebra over a number field is isomorphic to a cyclic algebra, and we have an exact sequence

$$0 \longrightarrow \mathrm{Br}(F) \longrightarrow \bigoplus_v \mathrm{Br}(F_v) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0,$$

where the first map is given by the localization at the places v and the second map is given by the sum of the Hasse invariants. In other words, the isomorphism classes of central simple algebras over F are completely determined by the degree and the collection of all the Hasse invariants, with the only constraint that the Hasse invariants must sum to 0 in $\mathbb{Q}/\mathbb{Z}$. For every place v, we have $A_v \cong \mathcal{M}_{d_v}(D_v)$ for some central division algebra D_v of degree e_v over F_v and some integer d_v such

that $d_v e_v = d$. For almost all v we have $d_v = d$. We say that v *is split* or *splits in* A if $e_v = 1$, and that v *is ramified* or *ramifies in* A otherwise. We say that v is *totally ramified* if $e_v = d$, so that $d_v = 1$. We usually write r the number of real places of F that ramify in A and s the number of real places that split in A, so that $r + s = r_1$. When v is a finite place and $\mathcal{O}$ an order in A, we write $\mathcal{O}_v = \mathbb{Z}_{F,v}\mathcal{O} \subset A_v$, and we write every object attached to D_v with a subscript v: Λ_v, Π_v, etc.

Let $\mathcal{O}$ be a $\mathbb{Z}_F$-order in A, which we usually abbreviate by simply saying that $\mathcal{O}$ is an order in A. The *different* $\mathfrak{D}(\mathcal{O})$ of $\mathcal{O}$ is a two-sided $\mathcal{O}$-ideal defined as the inverse of the two-sided ideal $\{x \in A \mid \mathrm{trd}(x\mathcal{O}) \in \mathbb{Z}_F\}$. The *reduced discriminant* of $\mathcal{O}$ is $\delta_{\mathcal{O}} = \mathrm{nrd}(\mathfrak{D}(\mathcal{O}))$. The *absolute discriminant* of $\mathcal{O}$ is defined to be $\Delta_{\mathcal{O}} = |\det(T(w_i w_j))|$, where $T = \mathrm{Tr}_{F/\mathbb{Q}} \circ \mathrm{trd}$ and (w_i) is a $\mathbb{Z}$-basis of $\mathcal{O}$. We have $\Delta_{\mathcal{O}} = |\Delta_F|^{d^2} N(\delta_{\mathcal{O}})^d$. When $\mathcal{O}$ is a maximal order, the reduced discriminant of $\mathcal{O}$ is called the *reduced discriminant of* A and we have $\delta_A = \delta_{\mathcal{O}} = \prod_{\mathfrak{p}} \mathfrak{p}^{d_{\mathfrak{p}}(e_{\mathfrak{p}}-1)} = \prod_{\mathfrak{p}} \mathfrak{p}^{d-d_{\mathfrak{p}}}$. The absolute discriminant of $\mathcal{O}$ is called the *absolute discriminant* Δ_A *of* A.

Let $\mathcal{O}$ be an order in A. The set of right $\mathcal{O}$-ideals is equipped with an action of the group $A^\times$ by multiplication on the left. Two right $\mathcal{O}$-ideals I, J are *equivalent* if there exists $x \in A^\times$ such that $xI = J$, that is if they lie in the same orbit modulo $A^\times$. The set $\mathrm{Cl}(\mathcal{O})$ of equivalence classes of right $\mathcal{O}$-ideals is finite. A right $\mathcal{O}$-ideal is *principal* if it is equivalent to the unit ideal $\mathcal{O}$.

Assume that $\mathcal{O}$ is maximal. When I is a right $\mathcal{O}$-ideal, we have $II^{-1} = \mathcal{O}_l(I)$ and $I^{-1}I = \mathcal{O}_r(I) = \mathcal{O}$. The set of two-sided $\mathcal{O}$-ideals forms a group under multiplication, and the set of right $\mathcal{O}$-ideals is equipped with an action of the group of two-sided $\mathcal{O}$-ideals by multiplication on the right. Let $\mathfrak{p}$ be a prime of $\mathbb{Z}_F$. Then there exists a unique two-sided $\mathcal{O}$-ideal $\mathfrak{P}$ such that every two-sided $\mathcal{O}$-ideal having reduced norm a power of $\mathfrak{p}$ is itself a power of $\mathfrak{P}$. We have $\mathfrak{P}^{e_{\mathfrak{p}}} = \mathfrak{p}\mathcal{O}$: such an ideal is called a prime of $\mathcal{O}$, and every two-sided $\mathcal{O}$-ideal is a product of primes of $\mathcal{O}$.

Let S be a finite set of places of F containing $\mathcal{V}_\infty$ and let $\mathcal{O}$ be an order in A. The ring of *S-integral elements* of $\mathcal{O}$ is $\mathcal{O}_S = \mathbb{Z}_{F,S}\mathcal{O}$, or equivalently the ring of elements $x \in A$ such that $x_v \in \mathcal{O}_v$ for all $v \notin S$. The group $\mathcal{O}_S^\times$ of *S-units* of $\mathcal{O}$ is the unit group of $\mathcal{O}_S$, or equivalently the group of elements $x \in A^\times$ such that $x_v \in \mathcal{O}_v^\times$ for all $v \notin S$. It contains the subgroup $\mathcal{O}_S^1$ of S-units of reduced norm 1. Let $G_S = \prod_{v \in S} A_v^1$. Then G_S is a locally compact group that is compact if and only if every place of S is totally ramified in A. Under the diagonal embedding, the group $\mathcal{O}_S^1$ is a discrete subgroup of G_S. The quotient $\mathcal{O}_S^1 \backslash G_S$ has finite Haar measure, and it is compact if and only if A is a division algebra.

Adèles. Let A be a central simple algebra over a number field F, and let $\mathcal{O} \subset A$ be an order. The *ring of adèles* $\mathbb{A}_A$ of A is the restricted product of the additive groups $(A_v)_{v \in \mathcal{V}_F}$ with respect to the compact open subgroups $(\mathcal{O}_v)_{v \in \mathcal{V}_f}$, equipped with the componentwise multiplication. Then $\mathbb{A}_A$ is a locally compact topological ring. The algebra A embeds into $\mathbb{A}_A$ diagonally, and unless stated otherwise we will always use the diagonal embedding. The subgroup $A \subset \mathbb{A}_A$ is discrete, and the quotient $A \backslash \mathbb{A}_A$ is compact.

We also define the idélic multiplicative group $\mathbb{A}_A^\times$ of A to be the restricted product of the multiplicative groups $(A_v^\times)_{v\in\mathcal{V}_F}$ with respect to the compact open subgroups $(\mathcal{O}_v^\times)_{v\in\mathcal{V}_f}$, and the group of idèles $\mathbb{A}_A^1$ of reduced norm 1 to be the subgroup of elements $x \in \mathbb{A}_A^\times$ such that $\mathrm{nrd}(x_v) = 1$ for all $v \in \mathcal{V}_F$. Again, the corresponding topology is induced by the embedding $\mathbb{A}_A^\times \to \mathbb{A}_A \times \mathbb{A}_A$ but it is not the subspace topology inside $\mathbb{A}_A$. The subgroup $A^1 \subset \mathbb{A}_A^1$ is discrete, the quotient $A^1\backslash\mathbb{A}_A^1$ has finite Haar measure and is compact if and only if A is a division algebra.

The Eichler condition. In this section we present the properties of some central simple algebras, or more precisely of certain sets of places relatively to some central simple algebra, subject to a condition called the Eichler condition. The theorems presented here can be considered as versions of the local-global principle: for the properties considered, if there is no local obstruction due to compactness, then there is no global obstruction either.

THEOREM 1.1.2.1 (Strong approximation). *Let A be a central simple algebra over a number field F and $\mathcal{O}$ an order in A. Let v be a place of F such that A_v^1 is not compact. Then the subgroup*

$$A^1 \cdot A_v^1 \subset \mathbb{A}_A^1$$

is dense.

We say that the set S *satisfies the Eichler condition* if it contains a place v such that A_v^1 is not compact. We say that A satisfies the Eichler condition or that A is *indefinite* if the set $\mathcal{V}_\infty$ satisfies the Eichler condition.

THEOREM 1.1.2.2 (Consequence of strong approximation). *Let A be a central simple algebra over a number field F, $\mathcal{O}$ an order in A. Let S be a finite set of places of F satisfying the Eichler condition. Let T be a finite set of places disjoint from S and such that $S \cup T$ contains the infinite places. Then the image of the diagonal embedding*

$$\mathcal{O}_{S\cup T}^1 \longrightarrow \prod_{v\in T} A_v^1 \prod_{v\notin S\cup T} \mathcal{O}_v^1$$

is dense.

Since the reduced norm on the Hamiltonian quaternions is positive definite, the reduced norm of an element in a central simple algebra is positive at every ramified real place. Eichler proved the following converse.

THEOREM 1.1.2.3 (Integral version of Eichler's norm theorem). *Let A be a central simple algebra over a number field F, $\mathcal{O}$ a maximal order in A. Let S be a finite set of places containing the infinite places and satisfying the Eichler condition. Let $\mathbb{Z}_{F,S,A}$ be the group of S-units that are positive at every real place of F that ramifies in A. Then the reduced norm*

$$\mathrm{nrd} : \mathcal{O}_S^\times \longrightarrow \mathbb{Z}_{F,S,A}^\times$$

is surjective.

THEOREM 1.1.2.4 (Eichler). *Let A be a central simple algebra over a number field F, satisfying the Eichler condition. Let $\mathcal{O}$ be a maximal order in A. Let $\mathrm{Cl}_A(F)$ be the ray class group with modulus the set of real places of F that ramify in A. Then the reduced norm induces a bijection*

$$\mathrm{Cl}(\mathcal{O}) \xrightarrow{\sim} \mathrm{Cl}_A(F).$$

In other words, two right $\mathcal{O}$-ideals are equivalent if and only if the classes of their norm in $\mathrm{Cl}_A(F)$ are equal when A is indefinite.

2. Geometry

To obtain information about the various groups that we are going to study, a classical tool is make to them act on various spaces and use geometry.

2.1. Euclidean lattices. We start with the simplest type of geometry: Euclidean geometry, which takes place in $\mathbb{R}^N$. We study the discrete subgroups of $\mathbb{R}^N$, called lattices, but we give an alternative definition that is more useful in an algorithmic context.

Note that this notion is not compatible with the previous notion of a lattice since $\mathbb{R}$ is not the field of fractions of $\mathbb{Z}$. This should cause no confusion, since the previous notion of lattice was used only to define ideals and orders, and subsequent apparitions of the word lattice refer to the following definition.

DEFINITION 1.2.1.1. A *lattice* is a free $\mathbb{Z}$-module of finite rank Λ equipped with a positive definite quadratic form $q : \Lambda \to \mathbb{R}_{\geq 0}$.

Such a quadratic form has an associated symmetric bilinear form $b : \Lambda \times \Lambda \to \mathbb{R}$ such that $q(x) = b(x, x)$. We will represent a lattice with basis $(w_i)_{1 \leq i \leq N}$ by the Gram matrix of its bilinear form, that is to say the matrix $\Big(b(w_i, w_j)\Big)_{i,j}$. We can consider Λ as embedded discretely in the real vector space $E = \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$, and the bilinear and the quadratic form extend uniquely to E. In this space, the *Gram–Schmidt orthogonalization procedure* is defined by induction for $1 \leq i \leq N$: we put $w_1^* = w_1$, and for $i > 1$ we define

$$w_i^* = w_i - \sum_{j=1}^{i-1} \mu_{i,j} w_j^*,$$

where

$$\mu_{i,j} = b(w_i, w_j^*)/q(w_j^*).$$

The $(w_j^*)_{j=1}^i$ form an orthogonal basis of $\langle w_1, \ldots, w_i \rangle_{\mathbb{R}} \subset E$.

One important invariant of a lattice is its covolume, which we denote $\mathrm{covol}(\Lambda)$: the covolume of Λ is the volume of the quotient $\Lambda \backslash E$ with respect to the Lebesgue measure on E that gives volume 1 to a cube based on an orthonormal basis with respect to q. Equivalently, we have

$$\mathrm{covol}(\Lambda)^2 = \prod_{i=1}^{N} q(w_i^*) = \det\Big(b(w_i, w_j)\Big)_{1 \leq i,j \leq N}.$$

The basis of a lattice can be of various qualities, depending on how much it is distorted with respect to the volume. The *LLL*-reduced bases achieve a good compromise as they can be computed in polynomial time. Using the notation of the Gram–Schmidt orthogonalization procedure above, a basis w_i of a lattice is called *LLL-reduced* if the following conditions hold:

- $|\mu_{i,j}| \leq \frac{1}{2}$ for all $1 \leq j < i \leq N$ (*size-reduction*), and
- $q(w_i^* + \mu_{i,i-1} w_{i-1}^*) \geq \frac{3}{4} q(w_{i-1}^*)$ (*Lovász condition*).

The celebrated *LLL*-algorithm (named after its inventors, Lenstra, Lenstra and Lovász) computes, given an arbitrary basis of a lattice as an input, an *LLL*-reduced basis of the same lattice in polynomial time [**Coh93**, Section 2.6.1]. An *LLL*-reduced basis has the following properties:

PROPOSITION 1.2.1.2. *Let $(w_i)_{1 \leq i \leq N}$ be a basis of a lattice (Λ, q) of rank N that is LLL-reduced. Let w_i^* be the corresponding orthogonalized Gram-Schmidt basis, and let $(b_i)_{1 \leq i \leq N}$ be linearly independent vectors in Λ. Then*

(i) $q(w_{i+1}^*) \geq \dfrac{q(w_i^*)}{2}$ *for all* $1 \leq i \leq N$;
(ii) $\operatorname{covol}(\Lambda)^2 \leq \prod_{i=1}^{N} q(w_i) \leq 2^{N(N-1)/2} \operatorname{covol}(\Lambda)^2$;
(iii) $q(w_j) \leq 2^{i-1} q(w_i^*)$ *for all* $1 \leq j \leq i \leq N$;
(iv) $q(w_j) \leq 2^{(N+j-2)/2} \Big(\dfrac{\operatorname{covol}(\Lambda)}{\prod_{i<j} q(w_i^*)} \Big)^{2/(N-j+1)}$ *for all* $1 \leq j \leq N$;
(v) $q(w_i) \leq 2^{N-1} \max_{1 \leq j \leq i} q(b_j)$.

PROOF. This is Theorem 2.6.2 in [**Coh93**]. □

For some algorithms, we will need something stronger than an *LLL*-reduced basis, we will need to compute short vectors in a lattice. This is computationally harder, but there are good algorithms for this task too.

THEOREM 1.2.1.3 (Kannan, Fincke–Pohst). *There is an explicit algorithm that, given a basis of a lattice (Λ, q) of rank N and a bound $A > 0$, computes the set of vectors x in Λ such that $q(x) \leq A$, and that runs in time at most*

$$O_N\left(1 + \left(\frac{A}{q(x_0)}\right)^{\frac{N}{2}}\right),$$

times a polynomial in the size of the input and in $\log A$, where x_0 is a shortest vector in Λ and the implicit constant depends only on N.

PROOF. [**HS07**, Theorem 2 and Sections 4.1 and 4.2] □

Note that we will use this algorithm with quadratic forms that are not known exactly but instead up to any given precision. In order to enumerate the vectors, one has to use integral approximations of the quadratic forms, see for instance [**Bel04**, Section 4].

2.2. Fundamental sets and domains. In this section we give some basic results on discontinuous group actions.

DEFINITION 1.2.2.1. Let X be a locally compact Hausdorff space and Γ a discrete group acting on X by homeomorphisms. We say that Γ acts *properly discontinuously* on X if for every compact subset $C \subset X$, there are only finitely many $\gamma \in \Gamma$ such that $\gamma C \cap C \neq \emptyset$. Let $D \subset X$. Then D is a *fundamental set* for Γ if $\Gamma \cdot D = X$. An open set D is a *fundamental domain* if $\overline{D}$ is a fundamental set and if in addition $\gamma \cdot D \cap D = \emptyset$ for all $1 \neq \gamma \in \Gamma$.

The following two results will be useful to construct sets of generators and presentations of groups.

LEMMA 1.2.2.2. *Let Γ be a group acting properly discontinuously on a pathwise connected space X. Let D be an open fundamental set for Γ. Then the set Σ of elements $\gamma \in \Gamma$ such that $\gamma D \cap D \neq \emptyset$ is a generating set for Γ.*

PROOF. This is part of [**Swa71**, Theorem 1.1]. □

LEMMA 1.2.2.3. *Let Γ be a group acting properly discontinuously on a pathwise connected, simply connected space X. Let D be an open, pathwise connected fundamental set for Γ. Let Σ be the set of elements $\gamma \in \Gamma$ such that $\gamma D \cap D \neq \emptyset$. Let R be the set of relations of the form $f = gh$ with $f, g, h \in \Sigma$, that hold in Γ. Let $\mathsf{\Gamma}$ be the finitely presented group $\langle \Sigma \mid \mathsf{R} \rangle$. Then the natural homomorphism*

$$\mathsf{\Gamma} \to \Gamma$$

is an isomorphism.

PROOF. This is [**Swa71**, Theorem 1.1]. □

2.3. Symmetric spaces. The main reference for this section is [**Ebe96**]. Our main source of spaces to have groups act on will be symmetric spaces. We do not give a general definition and theory of symmetric spaces, but instead we focus on the special example that we need. In what follows, G will be a group of the form $\prod_i \mathrm{GL}_{d_i}(D_i)$ or $\prod_i \mathrm{SL}_{d_i}(D_i)$ where d_i are integers and D_i division algebras over $\mathbb{R}$ with center F_i, and we will simply write d, D, F when there is only one factor.

Lie algebras. We can see G as a closed subgroup of $\mathrm{GL}_m(\mathbb{R})$ for some integer m. Then we have an exponential map

$$\exp : \mathcal{M}_m(\mathbb{R}) \to \mathrm{GL}_m(\mathbb{R}),$$

and a Lie bracket operation

$$[X, Y] = XY - YX$$

for all $X, Y \in \mathcal{M}_m(\mathbb{R})$. A subspace of $\mathcal{M}_m(\mathbb{R})$ is called a *Lie algebra* if it is stable under the Lie bracket operation. The Lie algebra $\mathrm{Lie}(G)$ is defined by

$$\mathrm{Lie}(G) = \{X \in \mathcal{M}_m(\mathbb{R}) \mid \exp(tX) \in G \text{ for all } t \in \mathbb{R}\}.$$

We have

- $\mathrm{Lie}(\mathrm{GL}_d(\mathbb{R})) = \mathfrak{gl}_d(\mathbb{R}) = \mathcal{M}_d(\mathbb{R})$;
- $\mathrm{Lie}(\mathrm{SL}_d(\mathbb{R})) = \mathfrak{sl}_d(\mathbb{R}) \subset \mathfrak{gl}_d(\mathbb{R})$ is the space of trace zero matrices;
- $\mathrm{Lie}(\mathrm{GL}_d(\mathbb{C})) = \mathfrak{gl}_d(\mathbb{C}) = \mathcal{M}_d(\mathbb{C})$;
- $\mathrm{Lie}(\mathrm{SL}_d(\mathbb{C})) = \mathfrak{sl}_d(\mathbb{C}) \subset \mathfrak{gl}_d(\mathbb{C})$ is the space of trace zero matrices;
- $\mathrm{Lie}(\mathrm{GL}_d(\mathbb{H})) = \mathfrak{gl}_d(\mathbb{H}) = \mathcal{M}_d(\mathbb{H})$;
- $\mathrm{Lie}(\mathrm{SL}_d(\mathbb{H})) = \mathfrak{sl}_d(\mathbb{H}) \subset \mathfrak{gl}_d(\mathbb{H})$ is the space of matrices with reduced trace zero.

Let $\mathfrak{g}$ be a Lie algebra. For all $X \in \mathfrak{g}$, the *adjoint endomorphism* $\mathrm{ad}(X) \in \mathrm{End}(\mathfrak{g})$ is defined by

$$\mathrm{ad}(X)(Y) = [X, Y] \text{ for all } Y \in \mathfrak{g}.$$

The *Killing form* $\mathcal{K}$ is the symmetric bilinear form defined by

$$\mathcal{K}(X, Y) = \mathrm{Tr}(\mathrm{ad}(x)\mathrm{ad}(y))$$

for all $X, Y \in \mathfrak{g}$.

In the Lie algebra $\mathfrak{gl}_d(D)$, we have

$$\mathcal{K}(X, Y) = 2[F : \mathbb{R}] \left(d \cdot \mathrm{trd}(XY) - \mathrm{trd}(X)\mathrm{trd}(Y)\right),$$

and the Killing form on $\mathfrak{sl}_d(D)$ is the restriction of the Killing form on $\mathfrak{gl}_d(D)$.

A Lie algebra is *semisimple* if the Killing form is nondegenerate. The Lie algebra $\mathfrak{sl}_d(D)$ is semisimple, but $\mathfrak{gl}_d(D)$ is not. The group G is *semisimple* if its Lie algebra is.

A *Cartan involution* is an involutive Lie algebra homomorphism $\theta : \mathfrak{g} \to \mathfrak{g}$ such that the bilinear form $(X, Y) \mapsto -\mathcal{K}(X, \theta Y)$ is positive definite. We have a decomposition $\mathfrak{g} = \mathfrak{K} \oplus \mathfrak{P}$ where $\mathfrak{K}$ is the $+1$-eigenspace of θ and $\mathfrak{P}$ is the -1-eigenspace of θ. This decomposition is orthogonal with respect to the Killing form, the restriction of the Killing form is negative definite on $\mathfrak{K}$, positive definite on $\mathfrak{P}$ and $\mathfrak{K}$ is a Lie subalgebra of $\mathfrak{g}$. The group $K = \exp(\mathfrak{K})$ is a compact subgroup of $\mathfrak{g}$.

The map $\theta : X \mapsto -\overline{X}^t$ is the *standard* Cartan involution on $\mathfrak{gl}_d(D)$. The Lie algebra $\mathfrak{K} = \mathfrak{u}_d(D)$ is the space of skew-Hermitian matrices, and the space $\mathfrak{P}$ is the space of Hermitian matrices. The group $K = \mathrm{U}_d(D)$ is the group of unitary matrices g such that

$$g\overline{g}^t = 1.$$

We will write $K = \prod_i \mathrm{U}_{d_i}(D_i) \subset \prod_i \mathrm{GL}_{d_i}(D_i)$ or $\prod_i \mathrm{SU}_{d_i}(D_i) \subset \prod_i \mathrm{SL}_{d_i}(D_i)$, respectively. The *symmetric space* attached to G is the quotient $X = G/K$. We summarize the dimensions of the groups and spaces we are considering in the following table.

G	K	$\dim G$	$\dim K$	$\dim G/K$
$\mathrm{SL}_d(\mathbb{R})$	$\mathrm{SO}_d(\mathbb{R})$	d^2-1	$\frac{d(d-1)}{2}$	$\frac{(d-1)(d+2)}{2}$
$\mathrm{SL}_d(\mathbb{C})$	$\mathrm{SU}_d(\mathbb{C})$	$2(d^2-1)$	d^2-1	d^2-1
$\mathrm{SL}_{\frac{d}{2}}(\mathbb{H})$	$\mathrm{SU}_{\frac{d}{2}}(\mathbb{H})$	d^2-1	$\frac{d(d+1)}{2}$	$\frac{(d-2)(d+1)}{2}$

Group decompositions. We will need several useful group decompositions.

Let $\mathfrak{g} = \mathfrak{P} + \mathfrak{K}$ be the decomposition associated with a Cartan involution, and $K = \exp(\mathfrak{K})$. Then we have the *polar decomposition*

$$G = \exp(\mathfrak{P})K.$$

Let $G = \mathrm{GL}_d(D)$ and $K = \mathrm{U}_d(D)$. Let A be the subgroup of diagonal matrices with positive real coefficients. Let $A^+ \subset A$ be the subset of matrices with weakly decreasing diagonal coefficients. Then we have the *Cartan decomposition*

$$G = KA^+K.$$

This is also known as the singular value decomposition (in the invertible case).

We will need a nonarchimedean analogue of the previous decomposition. It takes the following form. Let F be a nonarchimedean local field, D a central division algebra over F, Λ the maximal order of D with uniformizer Π. Let $G = \mathrm{GL}_d(D)$ and $K = \mathrm{GL}_d(\Lambda)$. Let A be the subgroup of matrices with diagonal coefficients that are powers of Π, and let A^+ be the subset of matrices where the powers are weakly decreasing. Then we have the *Cartan decomposition*

$$G = KA^+K.$$

Riemannian geometry. A *Riemannian metric* g on a smooth real manifold M is a positive definite inner product $g_p : T_pM \times T_pM \to \mathbb{R}$ that varies smoothly with the point p. The *Riemannian distance* between two points $p, q \in M$ is then the infimum over every $\mathcal{C}^1$ path $c : [0,1] \to M$ such that $c(0) = p$ and $c(1) = q$ of the quantity

$$\int_0^1 g(c'(t), c'(t))^{1/2} dt.$$

For this paragraph, the section 2 of [**Wan69**] is a good reference. Let G be the semisimple group $\prod_i \mathrm{SL}_{d_i}(D_i)$ and let θ be the standard Cartan involution. Identifying $\mathfrak{g}$ with the tangent space at the identity we can define a G-invariant Riemannian metric by taking $\langle X, Y\rangle_{\mathcal{K}} = -\mathcal{K}(X, \theta Y)$ for all $X, Y \in \mathfrak{g}$. This induces a G-invariant metric $d(\cdot,\cdot)$ on G. Similarly, the tangent space at $1 \cdot K$ on G/K can be identified with $\mathfrak{P}$ which we can equip with the Riemannian metric $\mathcal{K}(X, Y)$. This induces a G-invariant metric $\bar{d}(\cdot,\cdot)$ on $X = G/K$, which is also the quotient metric induced by the projection $G \to X$: for all $x, y \in G$ we have

$$\bar{d}(xK, yK) = \inf_{k,k' \in K} d(xk, yk').$$

Let $V \subset \mathbb{R}^d$ be the subspace of elements whose coordinates sum to zero. Then the image of the map

$$\begin{array}{rccl} f: & V & \longrightarrow & X \\ & v = (v_i) & \longmapsto & \exp\begin{pmatrix} v_1 & & 0 \\ & \ddots & \\ 0 & & v_d \end{pmatrix} K \end{array}$$

is *flat*, in the sense that it is isometric to a Euclidean space $\mathbb{R}^{d-1}$.

Finally, the quotient G/K is simply connected.

2.4. Hyperbolic geometry. In this section we recall basic definitions and properties of hyperbolic geometry and Kleinian groups. General references for this section are [**MR03**] and [**Rat06**].

The *upper half-space* is the Riemannian manifold $\mathcal{H}^3 = \mathbb{C}\times\mathbb{R}_{>0}$ with Riemannian metric given by

$$ds^2 = \frac{dx^2 + dy^2 + dt^2}{t^2}$$

where $(z,t) \in \mathcal{H}^3$, $z = x + iy$ and $t > 0$. For $w, w' \in \mathcal{H}^3$, we write $d(w,w')$ the distance between w and w'. The set $\mathbb{P}^1(\mathbb{C})$ is called the *sphere at infinity*. The upper half-space is a model of hyperbolic 3-space: it is the unique connected, simply connected Riemannian manifold with constant sectional curvature -1 up to isomorphism. In this space, the volume of the hyperbolic ball of radius r is $\pi(\sinh(2r)-2r)$.

The group $\mathrm{PSL}_2(\mathbb{C})$ acts on $\mathcal{H}^3$ in the following way. Consider the ring of Hamiltonians $\mathbb{H} = \mathbb{C}+\mathbb{C}j$ with multiplication given by $j^2 = -1$ and $jz = \bar{z}j$ for $z \in \mathbb{C}$, and identify $\mathcal{H}^3$ with the subset $\mathbb{C}+\mathbb{R}_{>0}j \subset \mathbb{H}$. Then for an element $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{C})$ and $w \in \mathcal{H}^3$, the formula

$$g \cdot w = (aw + b)(cw + d)^{-1} = (wc + d)^{-1}(wa + b)$$

defines an action of $\mathrm{PSL}_2(\mathbb{C})$ on $\mathcal{H}^3$ by orientation-preserving isometries. This action is transitive and the stabilizer of the point $j \in \mathcal{H}^3$ in $\mathrm{PSL}_2(\mathbb{C})$ is the subgroup $\mathrm{PSU}_2(\mathbb{C})$.

We can relate the hyperbolic metric to the canonical metric on the symmetric space $\mathrm{SL}_2(\mathbb{C})/\mathrm{SU}_2(\mathbb{C})$ defined in the previous section as follows. It suffices to compare the Riemannian metrics on the tangent space at j. We have

$$\begin{pmatrix} 1 + \frac{dt}{2} & \frac{dx+idy}{2} \\ \frac{dx-idy}{2} & 1 + \frac{dt}{2} \end{pmatrix} \cdot j = j + dx + idy + jdt,$$

so we get

$$\left\| \begin{pmatrix} \frac{dt}{2} & \frac{dx+idy}{2} \\ \frac{dx-idy}{2} & \frac{dt}{2} \end{pmatrix} \right\|^2_{\mathcal{K}} = 4(dx^2 + dy^2 + dz^2) = 4ds^2.$$

The canonical metric is 2 times the hyperbolic metric, and accordingly the volume induced by the canonical metric is 8 times the hyperbolic volume.

The trace of an element of $\mathrm{PSL}_2(\mathbb{C})$ is defined up to sign, and we have the following classification of conjugacy classes of elements $1 \neq g \in \mathrm{PSL}_2(\mathbb{C})$:

- If $\mathrm{Tr}(g) \in \mathbb{C} \smallsetminus [-2,2]$, then g has two distinct fixed points in $\mathbb{P}^1(\mathbb{C})$, no fixed point in $\mathcal{H}^3$ and stabilizes the geodesic between its fixed points, called its *axis*. The element g is conjugate to $\pm\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$ with $|\lambda| > 1$; it is called *loxodromic*.
- If $\mathrm{Tr}(g) \in (-2,2)$, then g has two distinct fixed points in $\mathbb{P}^1(\mathbb{C})$, and fixes every point in the geodesic between these two fixed points. The element g is conjugate to $\pm\left(\begin{smallmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{smallmatrix}\right)$ with $\theta \in \mathbb{R} \smallsetminus (\pi + 2\pi\mathbb{Z})$; it is called *elliptic*.

- If $\mathrm{Tr}(g) = \pm 2$, then g has one fixed point in $\mathbb{P}^1(\mathbb{C})$ and no fixed point in $\mathcal{H}^3$. It is conjugate to $\pm \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$; it is called *parabolic*.

The unit ball model. In actual computations we are going to work with another model of hyperbolic 3-space. The *unit ball* $\mathcal{B}$ is the open ball of center 0 and radius 1 in $\mathbb{R}^3 \cong \mathbb{C} + \mathbb{R}j \subset \mathbb{H}$, equipped with the Riemannian metric

$$ds^2 = \frac{4(dx^2 + dy^2 + dt^2)}{(1 - |w|^2)^2}$$

where $w = (z, t) \in \mathcal{B}$, $z = x + iy$ and $|w|^2 = x^2 + y^2 + t^2 < 1$. The *sphere at infinity* $\partial\mathcal{B}$ is the Euclidean sphere of center 0 and radius 1. The distance between two points $w, w' \in \mathcal{B}$ is given by the explicit formula

$$d(w, w') = \cosh^{-1}\left(1 + 2\frac{|w - w'|^2}{(1 - |w|^2)(1 - |w'|^2)}\right).$$

The upper half-space and the unit ball are isometric, the isometry being given by

$$\eta\colon \begin{cases} \mathcal{H}^3 \longrightarrow \mathcal{B} \\ \quad w \longmapsto (w - j)(1 - jw)^{-1} = (1 - wj)^{-1}(w - j), \end{cases}$$

and the action of an element $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{C})$ on a point $w \in \mathcal{B}$ is given by

$$g \cdot w = (Aw + B)(Cw + D)^{-1} \tag{1}$$

where

$$A = a + \bar{d} + (b - \bar{c})j,\ B = b + \bar{c} + (a - \bar{d})j,$$
$$C = c + \bar{b} + (d - \bar{a})j,\ D = d + \bar{a} + (c - \bar{b})j.$$

In the unit ball model, the geodesic planes are the intersections with $\mathcal{B}$ of Euclidean spheres and Euclidean planes orthogonal to the sphere at infinity, and the geodesics are the intersections with $\mathcal{B}$ of Euclidean circles and Euclidean straight lines orthogonal to the sphere at infinity. A *half-space* is an open connected subset of $\mathcal{B}$ with boundary consisting of a geodesic plane. A *convex polyhedron* is the intersection of a set of half-spaces, such that the corresponding set of geodesic planes is locally finite.

The Lobachevsky function and volumes of tetrahedra. We are going to compute hyperbolic volumes, and for this the main tool is going to be the Lobachevsky function, which we define here. The integral

$$-\int_0^\theta \ln|2\sin u| du$$

converges for $\theta \in \mathbb{R} \smallsetminus \pi\mathbb{Z}$ and admits a continuous extension to $\mathbb{R}$ that is odd and periodic with period π. This extension is called the *Lobachevsky function* $\mathcal{L}(\theta)$. The Lobachevsky function admits a power series expansion, converging for $\theta \in [-\pi, \pi]$:

$$\mathcal{L}(\theta) = \theta\left(1 - \ln(2|\theta|) + \sum_{n=1}^{\infty} \frac{\zeta(2n)}{n(2n+1)}\left(\frac{\theta}{\pi}\right)^{2n}\right).$$

With this function we can derive a formula for the volume of a certain standard tetrahedron, which we will use to compute the volume of convex polyhedra.

PROPOSITION 1.2.4.1. *Let T be the tetrahedron in $\mathcal{H}^3$ with one vertex at ∞ and the other vertices A, B, C on the unit hemisphere projecting vertically onto A', B', C' in $\mathbb{C}$ with $A' = 0$ to form a Euclidean triangle, with angles $\frac{\pi}{2}$ at B' and α at A', and such that the angle along BC is γ. Then the volume of T is finite and given by*

$$\mathrm{vol}(T) = \frac{1}{4}\left[\mathcal{L}(\alpha+\gamma) + \mathcal{L}(\alpha-\gamma) + 2\mathcal{L}\left(\frac{\pi}{2}-\alpha\right)\right].$$

PROOF. This formula can be found in [**MR03**, paragraph 1.7]. □

Kleinian groups and Dirichlet domains. A subgroup Γ of $\mathrm{PSL}_2(\mathbb{C})$ is a *Kleinian group* if it acts discontinuously on $\mathcal{H}^3$, or equivalently if it is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{C})$. To compute a fundamental domain for a Kleinian group Γ, we are going to use the standard construction of Dirichlet domains. The idea is to choose one distinguished point in the space, and then in each orbit choose "the closest point to the distinguished one": in this way, we pick generically one element in each orbit. More precisely, Let $p \in \mathcal{B}$ be a point with trivial stabilizer in Γ. Then the *Dirichlet domain* centered at p

$$D_p(\Gamma) = \{x \in \mathcal{B} \mid \text{for all } \gamma \in \Gamma \smallsetminus \{1\},\ d(x,p) < d(\gamma x, p)\}$$

is a convex fundamental polyhedron for Γ. If Γ has finite covolume, then the closure of $D_p(\Gamma)$ has finitely many faces. A Kleinian group Γ is *geometrically finite* if the closure of one (equivalently, every) Dirichlet domain for Γ has finitely many faces. This does not imply having finite covolume.

Note that since Γ acts properly discontinuously on $\mathcal{B}$, every point outside a zero measure, closed subset of $\mathcal{B}$ has a trivial stabilizer in Γ. In the unit ball model, the Dirichlet domain centered at 0 has a simple description. Consider an element $g \in \mathrm{SL}_2(\mathbb{C})$ not fixing $0 \in \mathcal{B}$. Let

- $\mathrm{I}(g) = \{w \in \mathcal{B} \mid d(w,0) = d(gw,0)\}$;
- $\mathrm{Ext}(g) = \{w \in \mathcal{B} \mid d(w,0) < d(gw,0)\}$;
- $\mathrm{Int}(g) = \{w \in \mathcal{B} \mid d(w,0) > d(gw,0)\}$.

We call $\mathrm{I}(g)$ the *isometric sphere* of g. For a subset $S \subset \mathrm{SL}_2(\mathbb{C})$ such that no element of S fixes 0, the *exterior domain* of S is $\mathrm{Ext}(S) = \bigcap_{g\in S} \mathrm{Ext}(g)$. The set S is a *defining set* for $\mathrm{Ext}(S)$. A *minimal defining set* for $\mathrm{Ext}(S)$ is a subset $S' \subset S$ such that $\mathrm{Ext}(S') = \mathrm{Ext}(S)$ and for all $g \in S'$, the geodesic plane $\mathrm{I}(g)$ contains a face of $\overline{\mathrm{Ext}(S)}$.

With these definitions it is clear that $D_0(\Gamma) = \mathrm{Ext}(\Gamma \smallsetminus \{1\})$. Note that for all $p \in \mathcal{B}$ with trivial stabilizer in Γ, $D_p(\Gamma) = uD_0(u^{-1}\Gamma u)$ where $u \in \mathrm{PSL}_2(\mathbb{C})$ is such that $p = u \cdot 0$, so there is no harm in restricting to the Dirichlet domain centered at 0. Consider an element $g \in \mathrm{SL}_2(\mathbb{C})$ and A, B, C, D as in formula (1). Then $g \cdot 0 = 0$ if and only if $C = 0$ and, if g does not fix 0, then a simple but lengthy

computation reveals that $\mathrm{I}(g)$ is the intersection of $\mathcal{B}$ and the Euclidean sphere of center w and radius r, where

$$w = -C^{-1}D \text{ and } r = 2/|C|, \tag{2}$$

and that $\mathrm{Int}(g)$ is the interior of this sphere. The reader can find the details in [**Pag10**, Proposition 3.1.6].

Another property of Dirichlet domains is their rich structure: they give a presentation for the group, and also necessary and sufficient conditions for an exterior domain to be a fundamental fomain. Suppose Γ is a Kleinian group in which 0 has trivial stabilizer, and let $g, h \in \Gamma$. Then we have $\mathrm{I}(g) = \mathrm{I}(h)$ if and only if $g = h$. We also have $g\mathrm{I}(g) = \mathrm{I}(g^{-1})$, and a point $x \in \mathrm{I}(g)$ is in the defining set of $D_0(\Gamma)$ if and only if $gx \in \mathrm{I}(g^{-1})$ is, too.

From this, we can group the faces of $\overline{D_0(\Gamma)}$ in pairs, one contained in some $\mathrm{I}(g)$ and the other contained in $\mathrm{I}(g^{-1})$, and g, g^{-1} send the faces to each other. This is the *face pairing* structure, and the elements g such that $\mathrm{I}(g)$ contains a face of $\overline{D_0(\Gamma)}$ are called the *face pairing transformations*. They generate the group Γ.

Now we are going to look for relations. The first type comes from edge cycles: consider an edge e_1 of $\overline{D_0(\Gamma)}$ contained in some $\mathrm{I}(g) \cap \mathrm{I}(h)$, and let $g_1 = g$. We define inductively a sequence of edges and elements in Γ in the following way. We let $e_{n+1} = g_n e_n$. Then e_{n+1} is contained in $\mathrm{I}(g_n^{-1}) \cap \mathrm{I}(g_{n+1})$ for a unique $\mathrm{I}(g_{n+1})$ (see Figure 1). If $\overline{D_0(\Gamma)}$ has finitely many faces, then the sequence $(e_n, g_n)_n$ is periodic, let m be its period. The sequence of edges $C = (e_1, \dots, e_m)$ is a *cycle* of edges, and m is its *length*. The *cycle transformation* at e_1 is $h = g_m g_{m-1} \dots g_1$, and has the following property:

(i) The cycle transformation at e_1 fixes e_1 pointwise.

This implies that h satisfies the *cycle relation* $h^\nu = 1$ for some integer ν. If $\nu \neq 1$, the cycle is called *elliptic*. At every edge e_i, the geodesic planes $\mathrm{I}(g_i^{-1})$ and $\mathrm{I}(g_{i+1})$ make an angle $\alpha(e_i)$ inside $D_0(\Gamma)$. The *cycle angle* of C is $\alpha(C) = \sum_{i=1}^m \alpha(e_i)$. Since the translates of $D_0(\Gamma)$ cover a neighborhood of e_1, we have the following property:

(ii) The cycle angle is $\frac{2\pi}{\nu}$, where ν is the order of the cycle transformation h.

The second type of relations comes from elements of order 2: it can happen that $\mathrm{I}(g) = \mathrm{I}(g^{-1})$, then the element g satisfies the *reflection relation* $g^2 = 1$.

THEOREM 1.2.4.2 (Poincaré). *Let $D = D_0(\Gamma)$ be the Dirichlet domain centrered at 0 of a geometrically finite Kleinian group Γ. Then the face pairing transformation generate the group Γ, and the reflection relations together with the cycle relations form a complete set of relations for Γ.*

PROOF. It is a special case of the second Theorem in [**Mas71**]. □

REMARK 1.2.4.3. In the presentation given by the theorem we consider only one element for each pair of face-pairing transformations g, g^{-1}. If we consider both g and g^{-1} to be in the set of generators, we have to add the "inverse" relation $g \cdot g^{-1} = 1$.

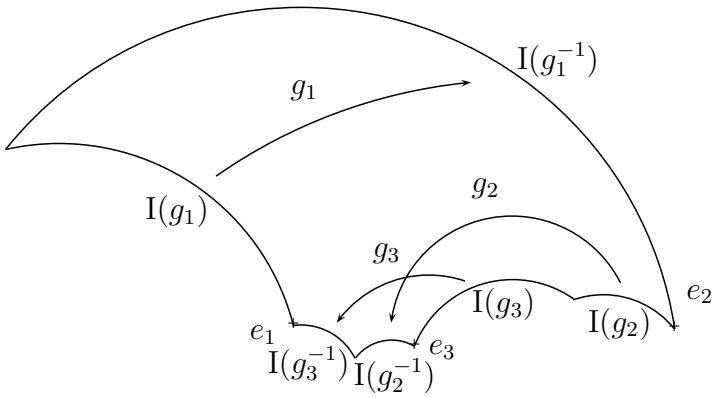

FIGURE 1. A length three cycle in a planar cut

We are now looking for sufficient conditions for an exterior domain to be a fundamental domain. There is another necessary condition, coming from cycles of some special points at infinity. A point $z \in \partial\mathcal{B}$ is a *tangency vertex* if it is a point of tangency $z = f \cap f'$ of two faces $f \subset \mathrm{I}(g)$, $f' \subset \mathrm{I}(g')$ of $D_0(\Gamma)$. If $z_1 = \mathrm{I}(g_0) \cap \mathrm{I}(g_1)$ is a tangency vertex, then we define a sequence by letting $z_{i+1} = g_i \cdot z_i = \mathrm{I}(g_i^{-1}) \cap \mathrm{I}(g_{i+1})$ while z_{i+1} is a tangency vertex (otherwise the sequence ends at z_i). If such a sequence (z_i) is infinite and $D_0(\Gamma)$ has finitely many faces, then it is periodic. Let m be its period; then $(z_1, \dots, z_m)$ is a *tangency vertex cycle* and the *tangency vertex transformation* is $h = g_m g_{m-1} \dots g_1$. The fact that $\mathcal{B}/\Gamma$ is complete implies the following property:

(iii) The tangency vertex transformation is parabolic.

Actually all these definitions make sense for any exterior domain. Suppose $\mathrm{Ext}(S)$ is an exterior domain with $S \subset \Gamma$ a finite minimal defining set. We say that it has a face pairing if $S = S^{-1}$ and for every $g \in S$ the image by g of the face contained in $\mathrm{I}(g)$ is the face contained in $\mathrm{I}(g^{-1})$ – equivalently, the image of every edge of $\overline{\mathrm{Ext}(S)}$ by the pairing transformation of an adjacent face is an edge of $\overline{\mathrm{Ext}(S)}$. This implies that every cycle is well-defined. We say that it satisfies the *cycle condition* if every cycle satisfies the properties (i) and (ii), and that it is *complete* if every tangency vertex cycle satisfies the property (iii).

THEOREM 1.2.4.4 (Poincaré). *Let $D = \mathrm{Ext}(S)$ be an exterior domain with finite S. Suppose D has a face pairing, satisfies the cycle condition, and is complete. Let Γ' be the group generated by the face pairing transformations. Then D is a fundamental polyhedron for Γ'.*

PROOF. It is a special case of the second Theorem in [**Mas71**]. □

Quaternion algebras and arithmetic Kleinian groups. We can construct Kleinian groups as follows. Let F be a number field with exactly one complex place and r_1 real places, and let A be a quaternion algebra over F that is ramified at every real place. Let $G = \mathrm{SL}_2(\mathbb{C}) \times (\mathbb{H}^1)^{r_1}$. Let $\mathcal{O}$ be an order in A. Then $\mathcal{O}^1 \subset G$ is discrete

and $\mathcal{O}^1\backslash G$ has finite invariant measure, and this quotient is compact if and only if A is a division algebra. Let $\iota : A \hookrightarrow \mathcal{M}_2(\mathbb{C})$ be an embedding of algebras extending the complex place of F. Then $\Gamma(\mathcal{O}) = \iota(\mathcal{O}^1)/\{\pm 1\} \subset \mathrm{PSL}_2(\mathbb{C})$ is a Kleinian group. It has finite covolume, and it is cocompact if and only if A is a division algebra. An *arithmetic Kleinian group* is a Kleinian group that is commensurable with a group $\Gamma(\mathcal{O})$, that is to say a subgroup $\Gamma \subset \mathrm{PSL}_2(\mathbb{C})$ such that $\Gamma \cap \Gamma(\mathcal{O})$ has finite index in both groups or a conjugate of such a group. The object of Chapter 3 is to describe an algorithm that, given such a group, computes a fundamental domain for $\Gamma(\mathcal{O})$, and a presentation with a computable isomorphism.

2.5. The Bruhat-Tits tree. The standard reference for this section is [**Ser80**]. Let F be a field with a discrete valuation v. Let R be its valuation ring, π a uniformizer and $\mathbb{F} = R/\pi R$ the residue field. We define the *Bruhat-Tits tree* $\mathcal{T}$, which we write $\mathcal{T}_\mathfrak{p}$ when F is the $\mathfrak{p}$-adic completion of a number field. The set of vertices of $\mathcal{T}$ is the set of homothety classes of R-lattices in F^2. Let L, L' be two such R-lattices. There exists an ordered R-basis (e_1, e_2) of L and integers a, b such that $(\pi^a e_1, \pi^b e_2)$ is an R-basis of L'. The integer $|a - b|$ depends only on the homothety classes of L, L' and is called their *distance*. By definition, there is an edge in the tree $\mathcal{T}$ between every pair of vertices at distance 1. The graph $\mathcal{T}$ is an infinite tree. If P, Q are two vertices, the unique path of minimum length between P and Q is called the *segment* PQ and the distance $d(P, Q)$ equals the length of the segment PQ. The set of vertices at distance 1 from a given vertex is in natural bijection with $\mathbb{P}^1(\mathbb{F})$.

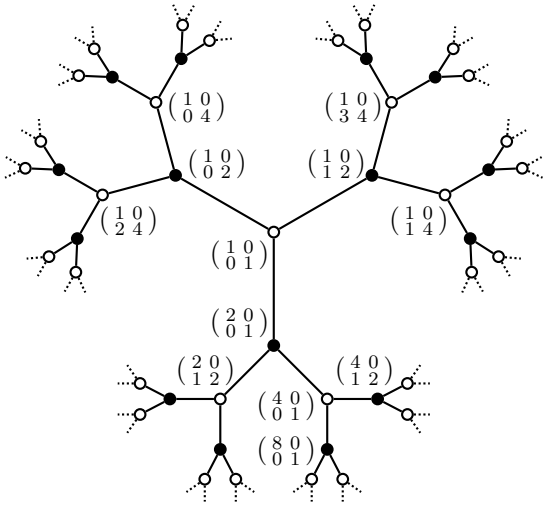

FIGURE 2. The Bruhat-Tits tree for $F = \mathbb{Q}_2$

The group $\mathrm{GL}_2(F)$ acts on the tree and preserves the distance, and this action factors through $\mathrm{PGL}_2(F)$ and is transitive on the set of vertices. The stabilizer of the vertex P_0 corresponding to the R-lattice R^2 is $F^\times \mathrm{GL}_2(R)$ and the stabilizer of any vertex is a conjugate of this group. The group $\mathrm{SL}_2(R)$ acts transitively on the

set of vertices at a fixed distance from P_0. For every $g \in \mathcal{M}_2(R) \smallsetminus \pi\mathcal{M}_2(R)$, the Smith normal form shows that $d(g \cdot P_0, P_0) = v(\det(g))$. The tree is illustrated in Figure 2 where we label some vertices P with a matrix g such that $P = g \cdot P_0$.

THEOREM 1.2.5.1. *Let P, Q be two vertices of the tree $\mathcal{T}$ with $d(P, Q) = 1$. Then the action of the group $G = \mathrm{SL}_2(F)$ on the vertices of $\mathcal{T}$ has exactly two orbits $G \cdot P$ and $G \cdot Q$.*

3. Representation theory

In this section we introduce unitary representations. We will use some properties of these representations, namely properties (T) and (τ), to estimate the size of fundamental domains of certain cocompact lattices. A good reference for the properties presented here is [**BdlHV08**].

Hilbert spaces and unitary representations. Let V be a Hilbert space, that is, a complex vector space with a Hermitian inner product that is complete with respect to the norm $\|v\| = \langle v, v\rangle^{1/2}$. The *unitary group* $\mathcal{U}(V)$ of V is the group of all invertible bounded linear operators $f : V \to V$ that are unitary, namely such that for all $v, v' \in V$,

$$\langle fv, fv'\rangle = \langle v, v'\rangle.$$

Let G be a topological group. A *unitary representation* of G on V is a homomorphism $\pi : G \to \mathcal{U}(V)$ such that for all $v \in V$, the map $g \mapsto \pi(g)(v)$ is continuous. If (V, π) and (V', π') are unitary representations of G, an *intertwining operator* is a continuous (equivalently, bounded) linear operator $V \to V'$ such that

$$f \circ \pi(g) = \pi'(g) \circ f \text{ for all } g \in G.$$

The representations V, V' are *equivalent* if there is an intertwining operator $f : V \to V'$ that is invertible. When two representations are equivalent, we can always choose the operator f so that it is an isometry.

A *subrepresentation* of V is the restriction of π to a closed invariant subspace. The representation (V, π) is *irreducible* if there is no nontrivial closed invariant subspace $0 \subsetneq U \subsetneq V$. The *unitary dual* $\widehat{G}$ of G is the set of irreducible unitary representations of G.

Let $(V_i)_{i\in I}$ be a family of Hilbert spaces. The *Hilbert direct sum* of the V_i is the Hilbert space

$$\hat{\bigoplus}_{i\in I} V_i = \left\{(v_i) \in \prod_{i\in I} V_i : \sum_{i\in I} \|v_i\|^2 \text{ converges}\right\},$$

with inner product given by the sum of the componentwise inner product. If (V_i, π_i) are unitary representations of G, then their *direct sum* is $\hat{\bigoplus}_{i\in I} V_i$ with the componentwise action.

Locally compact groups. Assume that G is locally compact, so that it has a left Haar measure μ. In this case, the space $L^2(G) = L^2(G, \mu)$ is a Hilbert space, and the action of G by left translations induces a unitary representation λ_G on $L^2(G, \mu)$, called the *left regular representation*.

For compact groups, the unitary dual is described by the Peter–Weyl theorem. Let G be a compact group. Then the Peter–Weyl theorem says that

(i) Every unitary representation of G is the direct sum of its irreducible subrepresentations.
(ii) Every irreducible representation of G is finite dimensional.
(iii) Every irreducible unitary representation of G is contained in the regular representation λ_G of G. More precisely, λ_G is the direct sum

$$\hat{\bigoplus}_{\pi \in \widehat{G}} (\dim \pi)\pi.$$

Properties (T) *and* (τ). The following property will play an important role in Chapter 2. When π is a unitary representation of G, a function of the form $g \mapsto \langle \pi(g)u, v \rangle$ is called a *matrix coefficient*. A representation π' is *weakly contained* in π if the matrix coefficients of π' can be approximated uniformly on compact sets by matrix coefficients of π. Kazhdan pairs express the fact that the trivial representation is not weakly contained in certain representations.

Definition 1.3.0.2. Let G be a topological group and (π, V) be a unitary representation of G. A *Kazhdan pair* for (π, V) is a pair (Q, ε) where $Q \subset G$ is a compact subset and $\varepsilon \in \mathbb{R}_{>0}$, with the property that for every $x \in V$ there exists $g \in Q$ such that

$$\|gx - x\|^2 \geq \varepsilon \|x\|^2.$$

Let $\mathcal{F}$ be a family of unitary representations of G. A Kazhdan pair for $\mathcal{F}$ is a pair (Q, ε) that is a Kazhdan pair for every $\pi \in \mathcal{F}$. We say that the group G has *Property* (T) or is a *Kazhdan group* if G admits a Kazhdan pair for the family of all unitary representations (π, V) such that the subspace of fixed vectors V^G is zero. The set Q is then called a *Kazhdan set* for G.

If $\mathcal{G}$ is a family of lattices in G, we say that G has *Property* (τ) with respect to $\mathcal{G}$ if it admits a Kazhdan pair for the family of unitary representations $(L^2_0(\Gamma\backslash G))_{\Gamma \in \mathcal{G}}$, where $L^2_0(\Gamma\backslash G)$ is the space of L^2 functions on G, left invariant by Γ, with zero mean.

The group $\mathrm{SL}_d(D)$ where $d \geq 2$ and D is a division algebra over $\mathbb{R}$ has Property (T). More generally, every Lie group of rank strictly larger than 1 has Property (T). Some groups of rank 1, such as $\mathrm{SL}_2(D)$, do not have Property (T). However, it was conjectured by Lubotzky and Zimmer that such groups have Property (τ) with respect to the family of congruence subgroups. This conjecture was proved by Burger and Sarnak [**BS91**] and Clozel [**Clo03**].

CHAPTER 2

Generators of S-unit groups in division algebras

Units in number fields play a significant role in algebraic number theory and diophantine geometry. Because of that, the problem of computing the unit group of the ring of integers $\mathbb{Z}_F$ of a number field F is an important task of algorithmic number theory and has received a lot of attention ([**Len92**], [**Coh93**]). The fact that this group conjecturally does not admit small generators makes this task difficult: as the classical example of real quadratic fields shows, the number of bits required to write down generators as linear combinations of an (LLL-reduced) integral basis seems to be at least $|\Delta_F|^{1/2-\varepsilon}$ for a positive proportion of number fields F, where Δ_F denotes the discriminant of F. The classical way of circumventing this problem is to write units as products of S-units where S is a well-chosen set of places of F; this is one of the reasons for being interested in S-units as well as units. More generally, we would like to compute the unit group of an order $\mathcal{O}$ in a central simple algebra A over a number field F: these groups provide important examples of arithmetic groups, and are related to the theory of finite groups [**Seh90**] or space-time codes [**LOB12**]. To study this task, it is natural to ask for which sets of places S the S-unit group $\mathcal{O}_S^\times$ admits small generators. We cannot expect such an S-unit group to have much smaller generators than the corresponding S-unit group in the base field F since the reduced norm $\mathcal{O}_S^\times \to \mathbb{Z}_{F,S}^\times$ is almost surjective. On the other hand, we can be optimistic and ask the following questions:

- Is the group $\mathcal{O}_S^\times$ generated by elements that are small with respect to the discriminant of the algebra A, when the base field is fixed?
- If we restrict our attention to the kernel $\mathcal{O}_S^1$ of the reduced norm, is this group generated by small elements?

Let us mention previous work on this topic. In [**Len92**], Lenstra treats the case of number fields and proves the following theorem.

THEOREM 2.0.0.3 (Lenstra, [**Len92**]). *Let F be a number field with r_2 complex places and discriminant Δ_F. Let $\mathbb{Z}_F$ be the ring of integers of F, and let S be a finite set of places of F containing every infinite place and every finite place with norm less than or equal to $(2/\pi)^{r_2}|\Delta_F|^{1/2}$, and let m_S be the maximum of the norms of primes in S or $m_S = 1$ if S contains no finite place. Then the group of S-units $\mathbb{Z}_{F,S}^\times$ is generated by its elements with logarithmic height less than or equal to*

$$\frac{1}{2}\log|\Delta_F| + \log m_S + r_2 \log\Big(\frac{2}{\pi}\Big)\cdot$$

The proof of this result is based on Minkowski's theorem on lattice points, and can be seen as the case of algebras of degree 1 in our context. More recently in [**CS12**], Chinburg and Stover define a notion of height in a division algebra over $\mathbb{Q}$ and use the same method to prove the following generalization.

THEOREM 2.0.0.4 (Chinburg–Stover, [**CS12**]). *There exist explicit functions of integer variables $f_1(n,d)$ and $f_2(n,d)$ such that the following holds. Let F be a number field of degree n and A a degree d central division algebra over F with absolute discriminant Δ_A, such that r real places of F ramify in A. Define*

$$e = \frac{n}{d(2n-r)}.$$

We have $1/(2d) \leq e \leq 1/d$. Let $\mathcal{O}$ be a maximal order in A, and S a finite set of places of F containing every infinite place and every prime $\mathfrak{p}$ such that

$$N(\mathfrak{p}) \leq f_1(n,d)\Delta_A^e.$$

Let m_S be the maximum of the norms of primes in S and $m_S = 1$ if S contains no such place. Then the group $\mathcal{O}_S^\times$ is generated by its elements of logarithmic height less than or equal to

$$e \log|\Delta_A| + \log m_S + f_2(n,d).$$

The height will be defined later, but one important fact is that the height depends on the choice of the order $\mathcal{O}$ (see definition in Section 3). This may seem artificial, but it is the correct notion as this height is related to the size of the coefficients required to write the elements in terms of a basis of the order $\mathcal{O}$ (Proposition 2.3.0.37).

Using properties (T) and (τ), we give new estimates for the size of generators for the group $\mathcal{O}_S^1$ of S-units of reduced norm 1 for arbitrary sets of places S and for the group $\mathcal{O}_S^\times$ of S-units with bounds on S depending only on F.

THEOREM 2.0.0.5. *There exist explicit functions of integer variables $g_1(n,d)$, $g_2(n,d)$, $g_3(n,d)$ and $g_4(n,d)$ such that the following holds. Let F be a number field of degree n and A a central division algebra of degree $d \geq 2$ over F with absolute discriminant Δ_A. Let $\mathcal{O}$ be a maximal order in A, and S a finite set of places of F containing every infinite place. Let m_S be the maximum of $N(\mathfrak{p})$ for primes $\mathfrak{p}$ in S that are not totally ramified in A, or $m_S = 1$ if S contains no such prime. Let q_S be the minimum norm of a split prime in S if A is a totally definite quaternion algebra and such a prime exists, and $q_S = 1$ otherwise. Then the group $\mathcal{O}_S^1$ is generated by its elements of logarithmic height less than or equal to*

$$g_1(n,d)\log(\Delta_A) + \log m_S + \tfrac{5}{2}\log q_S + g_2(n,d),$$

and we have $2/d \leq g_1(n,d) \leq 803/d$. Assume in addition that S contains every finite place of norm less than or equal to $(2/\pi)^{r_2}|\Delta_F|^{1/2}$. Let r be the number of real places of F that ramify in A. Then the group $\mathcal{O}_S^\times$ is generated by its elements of logarithmic height less than or equal to

$$g_3(n,d)\log(\Delta_A) + (r+1)\log m_S + \tfrac{5}{2}\log q_S + g_4(n,d).$$

Note that this result is expressed with Chinburg and Stover's notion of height. We use a slightly different notion in the following, so the formulation of the theorems in this chapter is slightly different. The second part of this theorem is interesting only when the base field is fixed: in that case we can choose a fixed set S independently of the algebra A, and still obtain small generators for the S-unit group of $\mathcal{O}$.

In [**CS12**, p. 3], Chinburg and Stover state that *"it appears [to them] that it is a deep problem to extend such height results to generators for the S-integral points of more general linear algebraic groups over number fields"*. Our method extends to many such instances, and we give a general bound in the following cases:

- a lattice in a Kazhdan group (Corollary 2.2.0.10);
- a cocompact lattice in a locally compact group with a spectral gap (Proposition 2.2.0.14);
- a congruence lattice in a connected semisimple Lie group (Corollary 2.2.0.16).

Our method shows that a lot of the difficulty is actually contained in the properties (T) and (τ).

Our estimates provide an algorithm with proved complexity that, given a maximal order $\mathcal{O}$ in a division algebra over $\mathbb{Q}$, computes a set of generators of the group $\mathcal{O}^1$ (Chapter 3). To our knowledge, this is the first algorithm *with proved complexity* for computing a set of generators of an infinite, noncommutative arithmetic group in a family of *anisotropic* algebraic groups over $\mathbb{Q}$.

In [**GS85**], Grunewald and Segal provide a completely general algorithm for computing a set of generators of an S-arithmetic group in a reductive algebraic group over a number field, which includes S-unit groups in division algebras. However, they do not analyse its complexity and the algorithm is not even primitive-recursive. As in [**CS12**], our algorithm is primitive recursive, and we even have a bound on the complexity.

This chapter is organised as follows. We first explain our method in the case of totally definite quaternion algebras in Section 1. In this case, it reduces to a classical construction of expander graphs. Then, we present the general case in Section 2, where we give estimates for the size of generators of lattices in Kazhdan groups, cocompact lattices in presence of a spectral gap, and congruence lattices in semisimple Lie groups. We then specialize to unit groups in division algebras in Section 4, where we make our bounds completely explicit.

1. Warm-up: totally definite quaternion algebras

As an introduction to our method, we study the case of S-units of reduced norm 1 for small sets of places S in definite quaternion algebras. A quaternion algebra over a totally real number field is *totally definite* if every real place is ramified. Throughout this section, F is a totally real number field of degree n, A is a quaternion algebra over F that is totally definite, $\mathcal{O}$ is a maximal order in A and S is a set of places of F, containing the infinite places. The case where S only contains ramified places is straightforward since the group $\mathcal{O}_S^1$ is finite.

LEMMA 2.1.0.6. *Assume that S contanins only ramified places. Then the group $\mathcal{O}_S^1$ is finite and for all $x \in \mathcal{O}_S^1$, we have*

$$x \in \mathcal{O}^1 \text{ and } \mathrm{Tr}_{F/\mathbb{Q}}(\mathrm{nrd}(x)) = n.$$

PROOF. Let $x \in \mathcal{O}_S^1$. Let $\mathfrak{p} \in S$ be a prime. Then $A_\mathfrak{p}$ is a division algebra with maximal order $\Lambda_\mathfrak{p}$ and valuation $w_\mathfrak{p}$. We have $w_\mathfrak{p}(x) = v_\mathfrak{p}(\mathrm{nrd}(x)) = v_\mathfrak{p}(1) = 0$, so $x \in \Lambda_\mathfrak{p}$. We get that $x \in \mathcal{O}^1_{S\smallsetminus\{\mathfrak{p}\}}$. Since this holds for every prime in S, we get $\mathcal{O}_S^1 = \mathcal{O}^1$. In addition, we have $\mathrm{Tr}_{F/\mathbb{Q}}(\mathrm{nrd}(x)) = \mathrm{Tr}_{F/\mathbb{Q}}(1) = n$. Since $\mathrm{Tr}_{F/\mathbb{Q}} \circ \mathrm{nrd}$ is a positive definite quadratic form turning $\mathcal{O}$ into a lattice, the set $\mathcal{O}^1$ is finite. □

Since $\mathrm{Tr}_{F/\mathbb{Q}} \circ \mathrm{nrd}$ is a positive definite quadratic form, this lemma gives a bound on the size of the elements of $\mathcal{O}_S^1$. Anticipating on Section 3, the elements of $\mathcal{O}_S^1$ have logarithmic height 0.

The first interesting case is when $S = T \cup \{\mathfrak{p}\}$, where every place in T is ramified and $\mathfrak{p}$ is split. As before, we have $\mathcal{O}_S^1 = \mathcal{O}^1_{\mathcal{V}_\infty \cup \{\mathfrak{p}\}}$ so we may assume that $S = \mathcal{V}_\infty \cup \{\mathfrak{p}\}$. The group $\mathcal{O}_S^1$ acts cocompactly on the Bruhat-Tits tree $\mathcal{T}_\mathfrak{p}$ of $\mathrm{SL}_2(F_\mathfrak{p})$. If the group $\mathcal{O}_S^1$ was torsion-free, our method would reduce to the classical fact that the quotient $\mathcal{O}_S^1 \backslash \mathcal{T}_\mathfrak{p}$ is a Ramanujan graph [**LPS88**].Because of torsion, we need a variant of their method, which we present in the next section.

1.1. Quotients of trees. In this section, let $k \geq 2$ be an integer and $\mathcal{T}$ the k-regular tree with set of vertices $V(\mathcal{T})$. We also write $q = k - 1$. A tree is always bipartite, so we fix a function $s : V(\mathcal{T}) \to \{\pm 1\}$ such that for all vertices x, the value $s(x)$ equals $-s(y)$ for every neighbor y of x. Let Γ be a group acting faithfully on $\mathcal{T}$ by automorphisms (i.e. preserving the edges), with finite vertex stabilizers, and such that $\Gamma \backslash V(\mathcal{T})$ is finite. We want to study $\Gamma \backslash \mathcal{T}$ by spectral methods, but the problem is that this quotient graph might not be k-regular. Instead we will work Γ-equivariantly.

Stabilizers and neighbors. Let ω be an orbit of vertices. The vertex stabilizers Γ_x, where $x \in \omega$, are conjugate, so we may define $\#\Gamma_\omega$ to be $\#\Gamma_x$ for every $x \in \omega$.

Neighbors. Let $x, y \in V(\mathcal{T})$. We will write $x \sim y$ when x and y are neighbors in $\mathcal{T}$. We need to study how neighbors of x are grouped under the action of Γ. Let $x, y \in V(\mathcal{T})$ and define

$$A(x, y) = \{y' \in V(\mathcal{T}) \mid y' \sim x \text{ and } \Gamma y' = \Gamma y\} = \{y' \in \Gamma y \mid y' \sim x\}.$$

The following lemma expresses the number of elements of $A(x, y)$ in a nicer way. Define

$$C(x, y) = \{\gamma \in \Gamma \mid \gamma y \sim x\},\ c(x, y) = \#C(x, y)$$

and

$$\mu(y) = \frac{1}{\#\Gamma_y}.$$

LEMMA 2.1.1.1. *For all $x, y \in V(\mathcal{T})$, we have*

$$\#A(x, y) = \mu(y)c(x, y)$$

and

$$c(x,y) = c(y,x).$$

PROOF. Define a map $\phi : C(x,y) \to A(x,y)$ by $\gamma \mapsto \gamma y$. Then the map ϕ is surjective, and its fibers are in bijection with Γ_y. Since $A(x,y)$ is a subset of the neighbors of x, it is finite, so $C(x,y)$ is also finite and we have the relation $\#\Gamma_y \cdot \#A(x,y) = \#C(x,y)$. This proves that $c(x,y)$ is well-defined and satisfies $\#A(x,y) = \mu(y)c(x,y)$. Since for all $\gamma \in \Gamma$, $\gamma x \sim y$ if and only if $x \sim \gamma^{-1}y$, inversion in Γ defines a bijection $C(x,y) \to C(y,x)$. This proves that $c(\cdot,\cdot)$ is symmetric. □

Since $c(x,y)$ only depends on the respecive orbits ω, ω' of x and y, we may define $c(\omega,\omega') = c(x,y)$, and similarly $\mu(\omega) = \mu(x)$.

Laplace operator. Let $L^2(\Gamma\backslash\mathcal{T})$ be the finite-dimensional real vector space of functions $f : V(\mathcal{T}) \to \mathbb{R}$ such that $f(\gamma x) = f(x)$ for all $x \in V(\mathcal{T})$ and $\gamma \in \Gamma$. For such a function f and an orbit ω, we define $f(\omega)$ to be $f(x)$ for some $x \in \omega$. On this space we define the positive definite inner product

$$\langle f, g\rangle = \sum_{\omega \in \Gamma\backslash V(\mathcal{T})} \mu(\omega) f(\omega) g(\omega).$$

On the space $L^2(\Gamma\backslash\mathcal{T})$ we define the *Laplace operator* $\mathcal{L}$ by

$$(\mathcal{L}f)(x) = \sum_{y \sim x} f(y).$$

Lemma 2.1.1.1 has the following consequence.

LEMMA 2.1.1.2. *The Laplace operator $\mathcal{L}$ is self-adjoint.*

PROOF. For every orbit $\omega \in \Gamma\backslash V(\mathcal{T})$, let $r(\omega) \in V(\mathcal{T})$ be a representative of ω. For all $f \in L^2(\Gamma\backslash\mathcal{T})$ we have

$$\begin{aligned}
(\mathcal{L}f)(\omega) &= (\mathcal{L}f)(r(\omega)) \\
&= \sum_{y \sim r(\omega)} f(y) \\
&= \sum_{\omega' \in \Gamma\backslash V(\mathcal{T})} \sum_{y \sim r(\omega),\, y \in \omega'} f(\omega') \\
&= \sum_{\omega' \in \Gamma\backslash V(\mathcal{T})} \#A(r(\omega), r(\omega')) f(\omega') \\
&= \sum_{\omega' \in \Gamma\backslash V(\mathcal{T})} \mu(\omega') c(\omega,\omega') f(\omega').
\end{aligned}$$

This gives, for all $f, g \in L^2(\Gamma\backslash\mathcal{T})$,

$$\begin{aligned}
\langle \mathcal{L}f, g\rangle &= \sum_{\omega \in \Gamma\backslash V(\mathcal{T})} \mu(\omega) \sum_{\omega' \in \Gamma\backslash V(\mathcal{T})} \mu(\omega') c(\omega,\omega') f(\omega') g(\omega) \\
&= \sum_{\omega,\omega' \in \Gamma\backslash V(\mathcal{T})} \mu(\omega)\mu(\omega') \cdot c(\omega,\omega') \cdot g(\omega) f(\omega').
\end{aligned}$$

This last expression is symmetric in f and g by Lemma 2.1.1.1: this proves the claim. □

Extremal eigenvalues. Recall that s is a function $V(\mathcal{T}) \to \{\pm 1\}$ such that for all vertices x, the value $s(x)$ equals $-s(y)$ for every neighbor y of x. We say that Γ is *type-preserving* if $s(\gamma x) = s(x)$ for all $\gamma \in \Gamma$ and $x \in V(\mathcal{T})$. Note that the constant function $\mathbf{1}$ is an eigenvector of $\mathcal{L}$ with eigenvalue k and that if Γ is type-preserving, the function s is an eigenvector of $\mathcal{L}$ with eigenvalue $-k$. More precisely we have the following lemma.

LEMMA 2.1.1.3. *For every eigenvalue λ of $\mathcal{L}$, we have $|\lambda| \leq k$. The eigenvalue k has multiplicity* 1. *The value $-k$ is an eigenvalue of $\mathcal{L}$ if and only if Γ is type-preserving, and in that case it has multiplicity* 1.

PROOF. Let $f \in L^2(\Gamma\backslash\mathcal{T})$ be nonzero and $\lambda \in \mathbb{R}$ be such that $\mathcal{L}f = \lambda f$. Let $x \in V(\mathcal{T})$ be such that $|f(x)|$ is maximal: we have

$$|\lambda f(x)| = |\mathcal{L}f| \leq \sum_{y \sim x} |f(y)| \leq k \cdot |f(x)|,$$

proving the claim by dividing by $|f(x)| \neq 0$.

Now let $f \in L^2(\Gamma\backslash\mathcal{T})$ be an eigenvector of $\mathcal{L}$ with eigenvalue k. Let $x \in V(\mathcal{T})$ be such that $f(x)$ is maximal. We have

$$kf(x) = \mathcal{L}f(x) = \sum_{y \sim x} f(y) \leq kf(x),$$

so the inequality is an equality : we have $f(y) = f(x)$ for evey neighbor of x. Since this is valid for every vertex such that $f(x)$ is maximal and $\mathcal{T}$ is connected, f is constant. This proves that k has multiplicity 1.

Finally let $f \in L^2(\Gamma\backslash\mathcal{T})$ be an eigenvector of $\mathcal{L}$ with eigenvalue $-k$. By the same argument as previously, using $x \in V(\mathcal{T})$ such that $|f(x)|$ is maximal, we get that the function $|f|$ is constant. By dividing by this constant, we may assume that f takes values in $\{\pm 1\}$. But then it must satisfy $f(y) = -f(x)$ for all $y \sim x$, so that $f = \pm s$. This implies that s is Γ-invariant, so Γ is type-preserving as claimed, and $-k$ has multiplicity 1. □

Eigenvalues and diameter bounds. From now on, we assume that Γ is type-preserving. Let $\lambda(\Gamma\backslash\mathcal{T})$ be the maximum of $|\lambda|$ where λ is an eigenvalue of $\mathcal{L}$ distinct from $\pm k$. We say that $\Gamma\backslash\mathcal{T}$ is *Ramanujan* if $\lambda(\Gamma\backslash\mathcal{T}) \leq 2\sqrt{q}$, and from now on we assume that this is satisfied. Let $\mu(\Gamma\backslash\mathcal{T}) = \sum_{\omega \in \Gamma\backslash V(\mathcal{T})} \mu(\omega)$. Our goal is to obtain a bound on the diameter of $\Gamma\backslash\mathcal{T}$ in terms of $\mu(\Gamma\backslash\mathcal{T})$.

We let $r = \#(\Gamma\backslash V(\mathcal{T}))$, and let $\lambda_1 = -k, \lambda_2 = k, \ldots, \lambda_r$ be the eigenvalues of $\mathcal{L}$. Let $\theta_1, \ldots, \theta_r \in \mathbb{C}$ be such that for all i we have $\lambda_i = 2\sqrt{q}\cos(\theta_i)$. We have $\theta_i \in \mathbb{R}$ for all $i \geq 2$ since we are assuming $|\lambda_i| \leq 2\sqrt{q}$.

For $n \geq 0$ let T_n be the usual Tchebychev polynomial satisfying $T_n(\cos\theta) = \cos(n\theta)$ for all $\theta \in \mathbb{C}$. Define $H_n(x) = q^{n/2}T_n(\frac{x}{2\sqrt{q}})$, satisfying the relations

$$H_0(x) = 1,\ H_1(x) = \tfrac{x}{2} \text{ and } H_{n+1} = xH_n(x) - qH_{n-1}(x),$$

and so that we have

$$H_n(2\sqrt{q}\cos\theta) = q^{n/2}\cos(n\theta) \text{ for all } \theta \in \mathbb{C}$$

and

$$H_n(k) = \frac{q^n+1}{2} = (-1)^n H_n(-k).$$

For $\omega \in \Gamma\backslash V(\mathcal{T})$, let $e_\omega = \mathbf{1}_\omega \mu(\omega)^{-1/2}$. They form an orthonormal basis of $L^2(\Gamma\backslash\mathcal{T})$. Let $u_1, \ldots, u_r$ be an orthonormal basis of $L^2(\Gamma\backslash\mathcal{T})$ such that $\mathcal{L}u_i = \lambda_i u_i$ for all i. We are now ready to prove the following proposition.

PROPOSITION 2.1.1.4. *Let $k \geq 2$, let $\mathcal{T}$ be a k-regular tree and $q = k-1$. Let Γ be a group acting on $\mathcal{T}$ with finite stabilizer with $\Gamma\backslash V(\mathcal{T})$ finite. Assume that Γ is type-preserving and that $\Gamma\backslash\mathcal{T}$ is Ramanujan. Then for every $\omega, \omega' \in \Gamma\backslash V(\mathcal{T})$ we have*

$$d(\omega,\omega') \leq \log_q\Big(\frac{\mu(\Gamma\backslash\mathcal{T})^2}{\mu(\omega)\mu(\omega')}\Big) + \delta,$$

where $\delta = 2$ if $d(\omega,\omega')$ is even and $\delta = 1$ otherwise.

PROOF. Let n be even and such that $d(\omega,\omega') > n$. Then we have

$$\begin{aligned} 0 &= \langle H_n(\mathcal{L})e_\omega, e_{\omega'}\rangle \\ &= \sum_{i=1}^{r} H_n(\lambda_i)u_i(\omega)u_i(\omega')\sqrt{\mu(\omega)\mu(\omega')}. \end{aligned}$$

For the terms corresponding to $i = 1$ and $i = 2$, we have $H_n(\lambda_1) = H_n(\lambda_2) = \frac{q^n+1}{2}$. We get

$$\begin{aligned} (q^n+1)\Big(\frac{\mu(\Gamma\backslash\mathcal{T})^2}{\mu(\omega)\mu(\omega')}\Big)^{-1/2} &\leq \sum_{i=3}^{r} |H_n(2\sqrt{q}\cos\theta_i)u_i(\omega)u_i(\omega')|\sqrt{\mu(\omega)\mu(\omega')} \\ &= \sum_{i=3}^{r} q^{n/2}|\cos(n\theta_i)u_i(\omega)u_i(\omega')|\sqrt{\mu(\omega)\mu(\omega')} \\ &\leq \sum_{i=3}^{r} q^{n/2}(u_i(\omega)^2\mu(\omega) + u_i(\omega')^2\mu(\omega'))/2 \\ &\leq q^{n/2}, \end{aligned}$$

where the last inequality comes from $1 = \langle e_\omega, e_\omega\rangle = \sum_{i=1}^r \langle e_\omega, u_i\rangle^2 = \sum_{i=1}^r u_i(\omega)^2\mu(\omega)$.

This gives $q^{n/2} < \Big(\frac{\mu(\Gamma\backslash\mathcal{T})^2}{\mu(\omega)\mu(\omega')}\Big)^{1/2}$, which is the same as

$$n < \log_q\Big(\frac{\mu(\Gamma\backslash\mathcal{T})^2}{\mu(\omega)\mu(\omega')}\Big),$$

proving the result. □

1.2. Bounds in the totally definite case. We return to the estimation of the size of generators for $\mathcal{O}_S^1$.

We need the following simple estimate on values of the Dedekind zeta function.

LEMMA 2.1.2.1. *Let F be a number field of degree n, and let $s > 1$. Then*

$$\zeta_F(s) \leq \zeta(s)^n.$$

PROOF. Since the Euler product converges, it suffices to prove the bound for each Euler factor at a prime p. Let $\mathfrak{p}$ be a prime of F of degree f above the rational prime p. We have $1-N(\mathfrak{p})^{-s} = 1-p^{-fs} \geq 1-p^{-s}$ since $0 \leq p^{-s} \leq 1$ and $f \geq 1$. This gives $\prod_{\mathfrak{p}|p}(1-N(\mathfrak{p})^{-s})^{-1} \leq \prod_{\mathfrak{p}|p}(1-p^{-s})^{-1} \leq (1-p^{-s})^{-n}$, proving the result. □

We also need a bound for the number of roots of unity in a number field.

LEMMA 2.1.2.2. *Let $N \geq 2$ be an integer. Then*

$$\phi(N) \geq \frac{N^{\frac{\log 2}{\log 3}}}{2}.$$

A number field of degree m contains at most $(2m)^{\frac{\log 3}{\log 2}}$ roots of unity.

PROOF. For the first statement, separate the prime 2 and other prime factors of N. If a number field L of degree m contains N roots of unity, then the cyclotomic field $\mathbb{Q}(\zeta_N)$ is contained in L so $\phi(N) \leq m$. □

Note that there exist better inequalities, but this elementary one is enough for our purpose. The proof of the next result uses the notion of *graph Laplacian* $\mathcal{L}$ that sends a function f on the vertices of a graph to the function $\mathcal{L}f$ whose value at a vertex v is the sum of the values of f over the neighbors of v.

PROPOSITION 2.1.2.3. *Let F be a totally real number field of degree n, A a totally definite quaternion algebra over F, $\mathcal{O}$ a maximal order in A, $\mathfrak{p}$ a prime of F that splits in A and $S = \mathcal{V}_\infty \cup \{\mathfrak{p}\}$. Let $\mathcal{T}_\mathfrak{p}$ be the Bruhat-Tits tree of $\mathrm{SL}_2(F_\mathfrak{p})$ and P_0 be the vertex fixed by $\mathcal{O}_\mathfrak{p}^1$. Then the group $\mathcal{O}_S^1$ is generated by the subset of its elements γ satisfying*

$$\begin{aligned} d(\gamma P_0, P_0) \cdot \log N(\mathfrak{p}) \quad &\leq \quad 2\log\left(\frac{\Delta_A}{\Delta_F}\right) + 4\log(6) - 4\log(24)n \\ &\quad +4\log\max(20, 3n^{\frac{\log 3}{\log 2}}) + 5\log N(\mathfrak{p}). \end{aligned}$$

PROOF. We will apply the results of the previous section to $\Gamma = \mathcal{O}_S^1/\{\pm 1\}$ and the tree $\mathcal{T}_\mathfrak{p}$. It is indeed k-regular for $k = q+1$ with $q = N(\mathfrak{p})$. Since $\mathcal{O}_S^1 \backslash \mathrm{SL}_2(F_\mathfrak{p})$ is compact, the quotient $\Gamma \backslash V(\mathcal{T})$ is finite. The group Γ acts by type-preserving automorphisms, and stabilizers of vertices are quotients of finite groups $\mathcal{O}_2^1$ for other maximal orders $\mathcal{O}_2 \subset A$, so we only need to check the Ramanujan condition. By the Jacquet–Langlands correspondence [**JL70**], eigenvalues λ of the Laplace operator $\mathcal{L}$ on $L^2(\Gamma \backslash \mathcal{T}_\mathfrak{p})$ can be of two types:

(i) λ comes from a character (one-dimensional automorphic representation) in the sense that $\lambda = \chi(\mathfrak{p})(q+1)$ for some character χ of a class group, or

(ii) λ is the eigenvalue of the $T_{\mathfrak{p}}$ Hecke operator on a parallel weight 2 Hilbert cusp form over F.

In case (i), the value $\chi(\mathfrak{p})$ is a root of unity, but λ is real so $\lambda = \pm k$. By Lemma 2.1.1.3, these eigenvalue both appear with multiplicity 1.

In case (ii), by the proof of the Ramanujan-Petersson conjecture for Hilbert modular forms by Don Blasius [**Bla06**], we have $|\lambda| \leq 2\sqrt{q}$. This precisely says that the quotient $\Gamma\backslash\mathcal{T}_{\mathfrak{p}}$ is Ramanujan. By Proposition 2.1.1.4, we have

$$d(\omega, \omega') \leq 2\log_q V + 2,$$

where $V = \mu(\Gamma\backslash\mathcal{T}_{\mathfrak{p}}) \cdot B$ and B is an upper bound on the size of finite subgroups G of Γ. Finite subgroups of quaternion algebras are classified [**Vig80**, Théorème 3.7]: either $\#G \leq 60$, or $\#G \leq m$ and G contains an element of order m. Since an element of order m in G is contained in a subfield of A having degree over $\mathbb{Q}$ at most $2n$, we have $m \leq (4n)^{\frac{\log 3}{\log 2}} = 9n^{\frac{\log 3}{\log 2}}$ by Lemma 2.1.2.2.

To estimate the mass μ of the quotient, we use Prasad's formula [**Pra89**]:

$$\mu_{\mathrm{Pras}}(\mathcal{O}_S^1\backslash \mathrm{SL}_2(F_{\mathfrak{p}})) = (q+1)\Delta_F^{3/2}\frac{\zeta_F(2)}{(2\pi)^{2n}}\prod_{\mathfrak{q}|\delta_A}\Big(N(\mathfrak{q})-1\Big),$$

where μ_{Pras} is the Haar measure on $\mathrm{SL}_2(F_{\mathfrak{p}})$ that gives measure 1 to the subgroup $\mathrm{I}_{\mathfrak{p}}$ of matrices in $\mathrm{SL}_2(\mathbb{Z}_{F_{\mathfrak{p}}})$ that are upper triangular modulo $\mathfrak{p}$. Since this group has index $q+1$ inside the stabilizer $\mathrm{SL}_2(\mathbb{Z}_{F_{\mathfrak{p}}})$ of a vertex, we obtain

$$\mu(\Gamma\backslash\mathcal{T}_{\mathfrak{p}}) = 2\Delta_F^{3/2}\frac{\zeta_F(2)}{(2\pi)^{2n}}\prod_{\mathfrak{q}|\delta_A}\Big(N(\mathfrak{q})-1\Big).$$

We estimate the last quantity with Lemma 2.1.2.1: we have $\zeta_F(2) \leq \zeta(2)^n = \pi^{2n}6^{-n}$, and we use the bound $\prod_{\mathfrak{q}|\delta_A}\Big(N(\mathfrak{q})-1\Big) \leq N(\delta_A)$. With the equality $\Delta_A = \Delta_F^4 N(\delta_A)^2$ we obtain

$$\log(V) \leq \frac{1}{2}\log\left(\frac{\Delta_A}{\Delta_F}\right) + \log(6) - \log(24)n + \log\max(20, 3n^{\frac{\log 3}{\log 2}}).$$

Let D be a ball in $V(\mathcal{T}_{\mathfrak{p}})$ containing a representative of every vertex orbit. In the realization of $\mathcal{T}_{\mathfrak{p}}$, let U be the open subset of points at distance less than $3/4$ from D. Then U is an open fundamental set for Γ, so by Lemma 1.2.2.2 the set Σ of elements $\gamma \in \Gamma$ such that $\gamma U \cap U \neq \emptyset$ is a generating set for Γ. It is the same as the set of elements $\gamma \in \Gamma$ such that there is an edge joining D and γD or such that $\gamma P_0 = P_0$, so every element $\gamma \in \Sigma$ satisfies $d(\gamma P_0, P_0) \leq 2\mathrm{Diam}(M) + 1$, and we get

$$\begin{aligned} d(\gamma P_0, P_0)\cdot \log N(\mathfrak{p}) \quad &\leq \quad 2\log\left(\frac{\Delta_A}{\Delta_F}\right) + 4\log(6) - 4\log(24)n \\ &\quad +4\log\max(20, 3n^{\frac{\log 3}{\log 2}}) + 5\log N(\mathfrak{p}) \end{aligned}$$

as claimed. □

REMARK 2.1.2.4. We can compare the mass formula obtained from Prasad's formula to the Eichler mass formula:

$$\sum_{[J]\in \mathrm{Cl}(\mathcal{O})} \frac{1}{[\mathcal{O}_l(J)^\times : \mathbb{Z}_F^\times]} = h_F \cdot 2\Delta_F^{3/2} \frac{\zeta_F(2)}{(2\pi)^{2n}} \prod_{\mathfrak{q}|\delta_A} \Big(N(\mathfrak{q}) - 1\Big),$$

where h_F is the class number of F.

As we will see in Section 4, Proposition 2.1.2.3 is actually a bound on the size of the generators. Our goal is to generalize these arguments to other unit groups. Since the symmetric space replacing the Bruhat-Tits tree is no longer discrete, the technique has to be adapted. We could use the Laplace operator on the Riemannian symmetric space (cf [**CGY97**], [**Bro92**]), but we found it technically simpler and more general to rely on representation theory.

2. Small generators of lattices

In this section we provide the generic version of our method for obtaining bounds on the size of generators of lattices. We prove some lemmas that are basic tools for the various bounds, and we prove general bounds in the setting of lattices in Kazhdan groups, relying on the work of Shalom [**Sha00**], and congruence lattices in semisimple Lie groups, relying on the work of Gelander [**Gel11**]. The main ingredient is an expansion property similar to the one of *expander graphs* [**Lub10**], which is described in Lemma 2.2.0.6. Given this, we can produce bounds for sets of generators for Γ, provided explicit estimates for

(1) Kazhdan pairs for $L^2_0(\Gamma\backslash G)$,
(2) the volume of small balls in $\Gamma\backslash G$,
(3) the volume of the quotient $\Gamma\backslash G$.

For congruence groups, those are respectively given by (1) the Selberg property proved by Burger, Sarnak [**BS91**] and Clozel [**Clo03**], (2) the Margulis lemma (Theorem 2.4.1.4) and bounds towards Lehmer's conjecture [**Smy08**], (3) Prasad's covolume formula [**Pra89**].

We first define an operation on subsets of a set, that is analogous to the graph boundary, to measure the expansion of subsets under the action of a group.

DEFINITION 2.2.0.5. Let G be a group, let $Q \subset G$ be a subset and M be a G-set. We define the map

$$\begin{array}{rccc} D: & \mathcal{P}(M) & \longrightarrow & \mathcal{P}(M) \\ & X & \longmapsto & \bigcup_{g\in Q} gX \smallsetminus X, \end{array}$$

where $\mathcal{P}$ denotes the power set.

Recall the definitions of a Kazhdan group, set, constant and pair from Definition 1.3.0.2. The Cayley graph of the quotient of a discrete Kazhdan group by a finite index subgroup is an expander. We prove an analogous expansion property for locally compact groups and their lattices.

LEMMA 2.2.0.6. *Let G be a second-countable locally compact, unimodular group. Let Γ be a lattice in G. Let μ be a left G-invariant measure on the quotient $M = \Gamma\backslash G$ and let $\pi = L^2_0(M)$. Let (Q, ε) be a Kazhdan pair for the G-representation π with $Q^{-1} = Q$. Then for every measurable set $X \subset M$ we have*

$$\mu(DX) \geq \frac{\varepsilon}{2}\mu(X)\left(1 - \frac{\mu(X)}{\mu(M)}\right).$$

PROOF. Let $Y = M \smallsetminus X$. Let $u = \mu(Y)\mathbf{1}_X$, $v = \mu(X)\mathbf{1}_Y$ and $f = u - v$. Since M has finite volume, we have $u, v \in L^2(M)$, u and v are orthogonal and $f \in L^2_0(M)$. Since (Q, ε) is a Kazhdan pair for π, there exists $g \in Q$ such that $\|g \cdot f - f\|^2 \geq \varepsilon\|f\|^2$.

We have

$$\begin{aligned} \|f\|^2 &= \|u\|^2 + \|v\|^2 \\ &= \mu(Y)^2\mu(X) + \mu(X)^2\mu(Y) \\ &= \mu(X)\mu(Y)\mu(M). \end{aligned}$$

On the other hand, we have $\frac{1}{2}\|g \cdot f - f\|^2 = \|f\|^2 - \langle g \cdot f, f\rangle$. We compute

$$\begin{aligned} \langle g \cdot f, f\rangle &= \langle g \cdot u - g \cdot v, u - v\rangle \\ &= \langle g \cdot u, u\rangle - \langle g \cdot u, v\rangle - \langle g \cdot v, u\rangle + \langle g \cdot v, v\rangle. \end{aligned}$$

We have $\langle g \cdot u, u\rangle = \mu(Y)^2\mu(gX \cap X) = \mu(Y)^2\mu(X) - \mu(Y)^2\mu(gX \cap Y)$ and similarly for v, so we get

$$\begin{aligned} \|f\|^2 - \langle g \cdot u, u\rangle - \langle g \cdot u, u\rangle &= \mu(Y)^2\mu(gX \cap Y) + \mu(X)^2\mu(gY \cap X) \\ &= \mu(Y)^2\mu(gX \cap Y) + \mu(X)^2\mu(g^{-1}X \cap Y) \\ &\leq (\mu(X)^2 + \mu(Y)^2)\mu(DX). \end{aligned}$$

We also have $\langle g \cdot u, v\rangle = \mu(X)\mu(Y)\mu(gX \cap Y) \leq \mu(X)\mu(Y)\mu(DX)$ and similarly for the symmetric expression. Altogether we obtain

$$\begin{aligned} \|g \cdot f - f\|^2 &\leq 2(\mu(X)^2 + \mu(Y)^2 + 2\mu(X)\mu(Y))\mu(DX) \\ &= 2\mu(M)^2\mu(DX). \end{aligned}$$

The Kazhdan inequality now reads

$$2\mu(DX)\mu(M)^2 \geq \varepsilon\mu(X)(\mu(M) - \mu(X))\mu(M)$$

as claimed. □

The sequence $u_{n+1} - u_n = \frac{\varepsilon}{2}u_n(1 - u_n)$ appears naturally from Lemma 2.2.0.6 when considering volumes of sequences of sets of the form $(Q^nX)_n$. We prove simple estimates for its speed of convergence. The first one is better when u_n is close to the repulsive fixed point 0, the second one is better when u_n is closer to the attractive fixed point 1.

LEMMA 2.2.0.7. *Let $c \in (0, 1)$. Consider the sequence u defined by $u_0 \in (0, 1)$ and for all $n \in \mathbb{Z}_{\geq 0}$,*

$$u_{n+1} - u_n = cu_n(1 - u_n).$$

Then u is increasing, $u_n \in (0,1)$ for all $n \geq 0$ and u_n converges to 1. For all $\delta > 0$, the smallest $k \geq 0$ such that $u_k > 1 - \delta$ satisfies

$$\begin{aligned} k &\leq \left\lceil \frac{1}{\log(1+c\delta)} \log\left(\frac{1-\delta}{u_0}\right) \right\rceil, \text{ and} \\ k &\leq \left\lceil \frac{1}{-\log(1-cu_0)} \log\left(\frac{1-u_0}{\delta}\right) \right\rceil. \end{aligned}$$

PROOF. Let f be the real function defined by $f(x) = x + cx(1-x)$ for all $x \in \mathbb{R}$. Then f maps $(0,1)$ into $(0,1)$: it is clearly positive on $(0,1)$, and since $f'(x) = (c+1) - 2cx = 1 - cx + c(1-x)$, the function f is increasing on $(0,1)$ and attains its maximum only at 1 where its value is 1. Since $cx(1-x) > 0$ for all $x \in (0,1)$, the sequence is increasing. Being increasing and bounded, u converges and its limit is a fixed point of f: it cannot be 0 since u is increasing, so it is 1.

For all $n < k$ we have $u_n \leq 1 - \delta$ so $u_{n+1} \geq u_n + cu_n\delta = (1 + c\delta)u_n$. This gives $1 - \delta \geq u_n \geq (1 + c\delta)^n u_0$, hence the first inequality.

Let $v_n = 1 - u_n$, then $v_{n+1} = v_n - cv_n(1 - v_n)$. For all $n < k$, since v is decreasing, we have $v_n \leq 1 - u_0$, so $1 - v_n \geq u_0$ and $v_{n+1} \leq (1 - cu_0)v_n$. This gives the bound $\delta \leq v_n \leq (1 - cu_0)^n(1 - u_0)$, hence the second inequality. □

In [**Sha00**], Shalom proves an explicit version of the classical result that any lattice in a Kazhdan group is again a Kazhdan group. Since a Kazhdan set in a discrete group is always a generating set, it suffices for our purpose to estimate the size of the elements in a Kazhdan set.

DEFINITION 2.2.0.8. Let G be a group and $\rho : G \to \mathbb{R}_{\geq 0}$ a map. We say that ρ is

- *symmetric* if $\rho(g^{-1}) = \rho(g)$ for all $g \in G$;
- *subadditive* if $\rho(gh) \leq \rho(g) + \rho(h)$ for all $g, h \in G$.

Let $d : G \times G \to \mathbb{R}$. We say that d is

- *symmetric* if $d(g,h) = d(h,g)$ for all $g, h \in G$;
- *subadditive* if $d(g,h) \leq d(g,k) + d(k,h)$ for all $g, h, k \in G$
- *left G-invariant* if $d(gh, gk) = d(h,k)$ for all $g, h, k \in G$.

The two notions are related by setting $d(g,h) = \rho(h^{-1}g)$ given ρ or $\rho(g) = d(g,1)$ given d. We will define one and implicily define the other using these formulas. For every $r > 0$ and $x \in G$, we write $B_r(x) = \{g \in G \mid d(g,x) \leq r\}$ and $B_r = B_r(1) = \{g \in G \mid \rho(g) \leq r\}$, which depend on the choice of ρ or d.

THEOREM 2.2.0.9 (Shalom). *Let G be as in Lemma 2.2.0.6, let $\rho : G \to \mathbb{R}_{\geq 0}$ be symmetric subadditive, and let (Q, ε) be a Kazhdan pair for G. Let Γ be a lattice in G, let μ be a left G-invariant measure on $\Gamma\backslash G$, and let $\pi : G \to \Gamma\backslash G$ be the canonical projection. Fix some $0 \leq \delta < \frac{\varepsilon}{8}$ and choose $R_0 < \infty$ satisfying $\mu(\pi(B_{R_0})) \geq (1-\delta)\mu(\Gamma\backslash G)$. Denote $R = 2R_0 + \max\{\rho(g) : g \in Q\}$, and let Σ be the finite set $\Sigma = \Gamma \cap B_R$. Then $(\Sigma, \frac{\varepsilon - 8\delta}{1-2\delta})$ is a Kazhdan pair for Γ.*

Shalom's theorem is completely explicit, except for the constant R_0 measuring the size of the elements in Σ: it is defined implicitly with a volume condition. In [**Oh02**], Oh raises the question of making this dependence more explicit: *"obtaining Kazhdan constants for a lattice Γ of G using this method involves understanding the size of a fundamental domain of Γ in G, which seems highly non-trivial in general."* Using the expansion property, we prove a bound on R_0 in terms of two natural invariants of the group Γ: the covolume $\mu(\Gamma\backslash G)$ and the volume of the projection of a small ball in the quotient $\Gamma\backslash G$. The covolume is something that we cannot avoid, and the volume of balls in the quotient is not a difficult quantity to estimate: for instance in many cases we can use the Margulis Lemma to get a lower bound.

COROLLARY 2.2.0.10. *Let G be a group as in Lemma 2.2.0.6, let $\rho : G \to \mathbb{R}_{\geq 0}$ be symmetric subadditive, and let (Q, ε) be a Kazhdan pair for G with $Q = Q^{-1}$. Let Γ be a lattice in G, let $M = \Gamma\backslash G$ with left G-invariant measure μ, and let $\pi : G \to M$ be the canonical projection. Let $r = \max_{g\in Q} \rho(g)$. Assume that $v = \mu(\pi(B_r)) > 0$. Let $0 < \delta < \frac{\varepsilon}{8}$ and let*

$$R = \frac{r}{\log(1 + \frac{\varepsilon}{4})} \log\left(\frac{\mu(M)}{4v\delta}\right) + 3r$$

and $\Sigma = \Gamma \cap B_R$. Then $(\Sigma, \frac{\varepsilon - 8\delta}{1-2\delta})$ is a Kazhdan pair for Γ. In particular, the set Σ generates Γ.

PROOF. Let $X_n = \pi(Q^{n+1}) \subset \pi(B_{(n+1)r})$ and $u_n = \mu(X_n)/\mu(M)$. By Lemma 2.2.0.6 we have $u_{n+1} - u_n \geq \frac{\varepsilon}{2} u_n(1 - u_n)$. We use the first inequality from Lemma 2.2.0.7 with $c = \varepsilon/2$, $u_0 = v/\mu(M)$ and $\delta = 1/2$: for any $n_0 \geq \frac{1}{\log(1+\varepsilon/4)} \log(\frac{\mu(M)}{2v}) + 1$ we have $u_{n_0} \geq 1/2$. Then we apply the second inequality to the sequence u_{n-n_0} with $c = \varepsilon/2$, $u_0 = 1/2$ and $\delta = \delta$: for all $n \geq n_0 + \frac{1}{-\log(1-\varepsilon/4)} \log(\frac{1}{2\delta}) + 1$ we have $u_n \geq 1 - \delta$. In the end, we get $u_n \geq 1 - \delta$ for all $n \geq \frac{1}{\log(1+\varepsilon/4)} \log(\frac{\mu(M)}{2v}) + \frac{1}{-\log(1-\varepsilon/4)} \log(\frac{1}{2\delta}) + 2$. Taking $R_0 = (n-1)r$ in Shalom's Theorem 2.2.0.9 and using $1/(1 - \varepsilon/4) \geq 1 + \varepsilon/4$ gives the result. □

Corollary 2.2.0.10 gives good bounds, but it fails for lattices in groups that do not have property (T), for instance $\mathrm{SL}_2(\mathbb{R})$. For those groups, we use the expansion property to estimate the diameter of a fundamental set for the action of Γ on a suitable space. The elementary distance bound is expressed in the following lemma.

LEMMA 2.2.0.11. *Use the same notations as in Lemma 2.2.0.6. Let $\rho : G \to \mathbb{R}_{\geq 0}$ be symmetric subadditive and let $r = \max_{g\in Q} \rho(g)$. Let $X_1, X_2 \subset M$ be measurable, for $i = 1, 2$ let $v_i = \mu(X_i)$ and assume that $v_i > 0$. Then*

$$d(X_1, X_2) \leq \frac{r}{\log(1 + \frac{\varepsilon}{4})} \log\left(\frac{V^2}{4v_1v_2}\right) + 2r\cdot$$

PROOF. First fix i and let $Y_n = Q^n X_i$ and $u_n = \mu(Y_n)/V$, so that $d(y, X_i) \leq nr$ for all $y \in Y_n$. By Lemma 2.2.0.6, we have $u_{n+1} - u_n \geq \frac{\varepsilon}{2} u_n(1 - u_n)$. By the first inequality of Lemma 2.2.0.7 with $c = \varepsilon/2$ and $\delta = 1/2$, for all $n_i \geq \frac{1}{\log(1+\varepsilon/4)} \log(\frac{V}{2v_i}) +$

1 we have $u_{n_i} > 1/2$. Applying this to X_1 and X_2 we find that $\mu(Q^{n_i}X_i) > V/2$, so $Q^{n_1}X_1$ and $Q^{n_2}X_2$ must intersect at a point $y \in M$. Then

$$d(X_1, X_2) \leq d(y, X_1) + d(y, X_2) \leq n_1 r + n_2 r,$$

proving the lemma. □

The simplest case where we can use this lemma is when the lattice Γ is actually cocompact. In this case we can simply bound the diameter of a fundamental domain for Γ.

Definition 2.2.0.12. Let G be a group with $\rho : G \to \mathbb{R}_{\geq 0}$ symmetric subadditive. The *Dirichlet domain* of Γ is the set

$$D = \{g \in G \mid \rho(g) \leq \rho(\gamma g) \text{ for all } \gamma \in \Gamma\}.$$

Remark 2.2.0.13. This is not the same as the Dirichlet domain that we defined in Chapter 1, but when ρ comes from the canonical metric on a symmetric space attached to a simple Lie group, the Dirichlet domain in the symmetric space is the image of the Dirichlet domain in G from Definition 2.2.0.12. However, we will need more general functions in Section 4.

Proposition 2.2.0.14. *Let G be a second-countable locally compact, unimodular group. Let $\Gamma \leq G$ be a lattice. Let μ be a left G-invariant measure on the quotient $M = \Gamma\backslash G$, let $V = \mu(M)$ and let $\pi = L^2_0(M)$. Let (Q, ε) be a Kazhdan pair for the G-representation π with $Q^{-1} = Q$. Let $\rho : G \to \mathbb{R}_{\geq 0}$ be symmetric subadditive and let $r = \max_{g \in Q} \rho(g)$. Assume that Γ is cocompact in G. Choose $\eta > 0$ and let $v > 0$ be a common lower bound for the volume of every closed ball of radius η in $M = \Gamma\backslash G$. Then the Dirichlet domain D satisfies*

$$\max_{g \in D} \rho(g) \leq R,$$

where we define

$$R = \frac{2r}{\log(1 + \frac{\varepsilon}{4})} \log\left(\frac{V}{2v}\right) + 2r + 2\eta.$$

The group Γ is generated by the set of elements $\gamma \in \Gamma$ such that

$$\rho(\gamma) \leq 2R.$$

Proof. Let $x, y \in M$. Applying Lemma 2.2.0.11 to $X_1 = B_\eta(x)$ and $X_2 = B_\eta(y)$ and noting that $d(x, y) \leq d(X_1, X_2) + 2\eta$ gives $d(x, y) \leq R$. By definition, for all $g \in D$ we have $\rho(g) = d(\pi(g), \pi(1))$ where π denotes the canonical projection $G \to \Gamma\backslash G$. This gives $\max_{g \in D} \rho(g) \leq R$. Let Σ be the set of $\gamma \in \Gamma$ such that $\gamma D \cap D \neq \emptyset$. Since D is compact, by Lemma 1.2.2.2 the set Σ generates Γ and for all $\gamma \in \Sigma$ we have $\rho(\gamma) \leq 2R$. □

When the lattice is not cocompact, it is not always finitely generated: for instance $\mathrm{SL}_2(\mathbb{F}_p[1/t]) \subset \mathrm{SL}_2(\mathbb{F}_p(\!(t)\!))$ is a lattice that is not finitely generated. In many such cases it is nontrivial to prove finite generation. In [**Gel11**], Gelander proves a general bound for the *number* of generators of lattices in semisimple Lie groups.

THEOREM 2.2.0.15 (Gelander). *Let G be a connected semisimple Lie group without compact factors. Then there is an effectively computable constant $A = A(G)$ such that every irreducible lattice $\Gamma \leq G$ admits a generating set Σ with*

$$\#\Sigma \leq A \cdot V,$$

where $V = \mu(\Gamma\backslash G)$.

In the words of Gelander, the method of proof consists in *"deform(ing) the symmetric space $X = G/K$ to a nice connected Γ-invariant subset $Y \subset X$ where the displacement of every $\gamma \in \Gamma \smallsetminus \{1\}$ is bounded below by a uniform constant"*. For algorithmic purposes, the *size* of the generators is mostly relevant. However, it is probably too much to expect small generators for arbitrary lattices. Instead, we restrict to a *congruence* lattice Γ. In this case, the Selberg property allows us to apply Lemma 2.2.0.11 and to construct a short fundamental set for the action of Γ on Gelander's set Y, providing the desired bound.

COROLLARY 2.2.0.16. *Let G be as in Theorem 2.2.0.15, K a maximal compact subgroup and let $\rho(g) = d(g, 1)$, where d is the canonical metric on G. If at least one simple factor of G has property (T), let $\mathcal{G}$ be the family of all irreducible lattices $\Gamma \leq G$; otherwise let $\mathcal{G}$ be the family of all irreducible congruence lattices $\Gamma \leq G$. Then there are effectively computable constants $B = B(G)$ and $C = C(G)$ such that for all $\Gamma \in \mathcal{G}$, there exists $g \in G$ such that there is a generating set Σ satisfying*

$$\max_{\gamma \in \Sigma} \rho(g^{-1}\gamma g) \leq B \cdot \log V + C.$$

where $V = \mu(\Gamma\backslash G)$.

PROOF. In [**Gel11**], Gelander defines a constant $\alpha = \alpha(G)$ and constructs a nonempty Γ-invariant connected set $Y \subset G/K$ that is α-thick with respect to Γ, that is to say $\bar{d}(\gamma y, y) \geq \alpha$ for all $y \in Y$ and $\gamma \in \Gamma$. Let $Y' \subset G$ be the inverse image of Y; it is also α-thick with respect to Γ.

If a simple factor $H \leq G$ has property (T), let (Q, ε) be a Kazhdan pair for H. It is also a Kazhdan pair for the G-representations $L^2_0(\Gamma\backslash G)$ for $\Gamma \in \mathcal{G}$. Otherwise, by the solution of Conjecture (τ) by Burger and Sarnak [**BS91**] and Clozel [**Clo03**], there exists a Kazhdan pair (Q, ε) for the G-representations $L^2_0(\Gamma\backslash G)$ for $\Gamma \in \mathcal{G}$. With the same notations as in Lemma 2.2.0.11, let $a = \frac{2r}{\log(1+\varepsilon/4)}$ and $b = 2\alpha + 2r - \frac{2r}{\log(1+\varepsilon/4)} \log(2\mu(B_\alpha))$. By Lemma 2.2.0.11, the diameter of $\Gamma\backslash Y'$ is bounded by $R = a \log V(\Gamma) + b$ and the diameter of $\Gamma\backslash Y$ is bounded by the same quantity.

Let $U = B_R \cap Y$, so that U is open in Y and $Y = \Gamma \cdot U$. Let Σ be the set of $\gamma \in \Gamma$ such that $\gamma U \cap U \neq \emptyset$. By Lemma 1.2.2.2, Σ is a generating set for Γ. Let $g \in G$ such that $x = gK \in U$. Then for all $\gamma \in \Sigma$, we have

$$\rho(g^{-1}\gamma g) \leq 2R \leq 2a \log V(\Gamma) + 2b = B \log V(\Gamma) + C$$

with $B = 2a$ and $C = 2b$. □

Note that such an estimate cannot hold uniformly for *every* $g \in G$ if the lattice Γ is not cocompact: for instance, if $G = \mathrm{SL}_2(\mathbb{R})$, B is a constant and $g \cdot x$ tends to

infinity in a cusp of $\Gamma\backslash\mathcal{H}^2$, then the group generated by the set of $\gamma \in \Gamma$ such that $\rho(g^{-1}\gamma g) \leq B$ will eventually be only the stabilizer of the cusp.

3. Heights in division algebras

Following Chinburg and Stover, we define a notion of height to measure the size of elements in A. We start with the local case. Since there is no nonzero absolute value on a central simple algebra that is not a division algebra, we replace the absolute values with norms.

Definition 2.3.0.17. Let F be a local field, d a positive integer and D a central division algebra of degree e over F. Let V be the right D-vector space D^d, so that $\mathrm{End}_D(V) \cong \mathcal{M}_d(D)$ by multiplication on the left. For all $v \in V$ we define the *norm* $\|v\|$ by

- if F is nonarchimedean, $\|v\| = \max_i |v_i|$;
- if F is archimedean, $\|v\|^2 = \sum_i v_i\overline{v_i}$.

Let $A = \mathcal{M}_d(D)$. For all $M \in A$ we define the *norm* $\|M\|$ by

$$\|M\| = \sup_{v \in V \smallsetminus \{0\}} \frac{\|Mv\|}{\|v\|}.$$

We give a more concrete description of these norms as follows.

Lemma 2.3.0.18. *Use the same notations as in Definition 2.3.0.17.*

(i) If F is nonarchimedean, then for all $M \in A$ we have

$$\|M\| = \max_{i,j} |M_{i,j}|,$$

where $M_{i,j}$ denotes the (i,j)-th matrix entry of M.

(ii) If F is archimedean, let $M \in A$ and let $M = k_1 a k_2$ be the Cartan decomposition of M, with the matrix a being diagonal with positive real coefficients (a_i) and $k_1, k_2 \in K = \mathrm{U}_d(D)$. Then

$$\|M\| = \max_i a_i.$$

Proof.

(i) By the ultrametric inequality we have $\|M\| \leq \max_{i,j} |M_{i,j}|$. Both sides of the equality are invariant by $K = \mathrm{GL}_d(\Lambda)$ where Λ is the unique maximal order of D, so by Cartan decomposition it suffices to prove the other inequality when M is a diagonal matrix with coefficients (Π^{m_i}), where Π is a uniformizer of Λ and $m_i \in \mathbb{Z}$. In this case, let i be such that m_i is minimal and let $v \in V$ have all coordinates 0 except the i-th being 1. Then $\|v\| = 1$ and $\|Mv\| = \max_{i,j} |M_{i,j}|$, proving the result.

(ii) Since $\|\cdot\|$ is bi-invariant by $K = \mathrm{U}_d(D)$, it suffices to prove the result when $M = a$ is a diagonal matrix with positive real coefficients a_i. In this case, for all $v \in V$ we have $\|Mv\|^2 = \sum_i a_i^2 v_i\overline{v_i} \leq (\max_i a_i)^2\|v\|^2$. Taking v with all coordinates 0 except a 1 corresponding to the maximum a_i gives the equality.

□

In order to prove important properties of our notion of height, we need to prove a bound on the eigenvalues of elements of A in terms of their norm, which is done in Corollary 2.3.0.22. The proof uses the following two technical lemmas.

LEMMA 2.3.0.19. *Let L be a nonarchimedean local field and $(V, \|\cdot\|)$ a finite dimensional normed L-vector space such that the set of possible values of the norm satisfies $\|V\| \subset \{|\lambda| \ : \ \lambda \in L\}$, which we will write $|L|$. Then there exists a basis (b_i) of V such that for all $v = \sum_i v_i b_i \in V$ with $v_i \in L$, we have $\|v\| = \max_i |v_i|$.*

PROOF. We first prove that there exists an element in V having norm 1: let $x \in V \smallsetminus \{0\}$ and let $\lambda \in L$ such that $\|x\| = |\lambda|$. Then x/λ has norm 1. We proceed by induction on the dimension of V. The result is clear in dimension 1, take an element of norm 1 as the basis. Assume V has dimension $n \geq 2$. Let b_1 be an element of V of norm 1. Let W be V/Lb_1 with canonical projection $p : V \to W$, equipped with the induced norm $\|\cdot\|$ such that for all $v \in V$, $\|p(v)\| = \inf_{w \in v + Lb_1} \|w\|$. By induction, let $c_2, \ldots, c_n$ be a basis of W satisfying the required property, so that $\|c_i\| = 1$ for all i. Let $b_2, \ldots, b_n$ be lifts of $c_2, \ldots, c_n$ such that $\|b_i\| = 1$ for all i. Now let $v = \sum_i v_i b_i \in V$ with $v_i \in L$. Since $\|b_i\| = 1$ for all i, we have $\|v\| \leq \max_i |v_i|$. If the maximum is attained only for $i = 1$, then $\|v\| = |v_1| = \max_i |v_i|$. Otherwise, the maximum is attained for at least an $i \geq 2$ and we have $\|v\| \geq \|p(v)\| = \|\sum_{i \geq 2} v_i c_i\| = \max_{i \geq 2} |v_i| = \max_i |v_i|$. □

LEMMA 2.3.0.20. *Use the same notations as in Definition 2.3.0.17. Let L be a finite extension of F containing a totally ramified splitting field of D of degree e. Then there exists an embedding $s : A \hookrightarrow \mathcal{M}_{ed}(L)$ such that for all $x \in A$, $\|s(x)\| = \|x\|$.*

PROOF. It suffices to prove the result when L is a totally ramified splitting field of L of degree e. Since L embeds into D, we can use the embedding induced by the left action of A on $V = D^d$, to which we give the structure of an L-vector space of dimension ed by multiplication on the right. It suffices to find an L-basis (b_i) of V such that the norms given by the D-vector space structure $V = D^d$ and by the L-vector space structure $V = \oplus_i b_i L$ agree. It suffices to prove the result when $d = 1$.

- In the archimedean case, $(1, j)$ is such a basis: $\mathbb{H} = \mathbb{C} + j\mathbb{C}$ and for all $w = z_1 + jz_2 \in \mathbb{H}$, $\|w\|^2 = \mathrm{nrd}(w) = |z_1|^2 + |z_2|^2$.
- In the nonarchimedean case, by Lemma 2.3.0.19 it suffices to prove that D is an *L-normed* vector space and that $\|D\| \subset |L|$. For all $\lambda \in L$ and $x \in D$, we have $\|\lambda \cdot x\| = |x\lambda| = |x| \cdot |\lambda| = |\mathrm{nrd}(\lambda)|^{1/e} \cdot \|x\| = |N_{L/F}(\lambda)|^{1/e} \cdot \|x\| = |\lambda| \cdot \|x\|$. We have $\|D^\times\| = |D^\times| = |\Pi^{\mathbb{Z}}| = |\pi|^{\mathbb{Z}/e} = |L^\times|$ since L/F is totally ramified, giving the result.

□

REMARK 2.3.0.21. If L is an unramified splitting field of D, the result is false as there are not enough possible values of $|\cdot|$ on L.

COROLLARY 2.3.0.22. *Use the same notations as in Definition 2.3.0.17. Let $x \in A$ and let λ be an eigenvalue of x in an algebraic extension of F that splits A. Then $|\lambda| \leq \|x\|$.*

PROOF. By Lemma 2.3.0.20, we may assume that A is a matrix algebra and that $\lambda \in F$. Let $x \in A$, assume that $|\lambda| > \|x\|$. Then $\|(x/\lambda)^n\| \leq (\|x\|/|\lambda|)^n \to 0$, but x/λ has a nonzero fixed point: contradiction. □

We are now ready to define local heights by analogy with the commutative case.

DEFINITION 2.3.0.23. Let F be a local field with residual characteristic p (with the convention that $p = \infty$ when $F = \mathbb{R}$ or $\mathbb{C}$), d a positive integer, D a central division algebra of degree e over F, and $A = \mathcal{M}_d(D)$. For an element $x \in A$, we define the *height* $\mathrm{H}(x)$ to be

$$\mathrm{H}(x) = \max\Big(1, \|x\|\Big)^{[F:\mathbb{Q}_p]}.$$

We define the *logarithmic height* of x to be $\mathrm{h}(x) = \log \mathrm{H}(x)$.

We prove some natural properties of the local height, which will be useful for the global case.

LEMMA 2.3.0.24. *Use the same notations as in Definition 2.3.0.23.*

(i) For all $\lambda \in F^\times$,

$$\mathrm{H}(\lambda) = \mathrm{H}_F(\lambda).$$

(ii) For all $x, y \in A$,

$$\mathrm{H}(xy) \leq \mathrm{H}(x)\mathrm{H}(y).$$

(iii) For all $x \in A$,

$$\mathrm{H}_F(\mathrm{nrd}(x)) \leq \mathrm{H}(x)^{ed}.$$

(iv) For all $x \in A$,

$$\Big(\mathrm{H}(x) = 1 \text{ and } |\mathrm{nrd}(x)| = 1\Big) \iff x \in K,$$

where $K = \mathrm{GL}_d(\Lambda)$ if F is nonarchimedean and $K = \mathrm{U}_d(D)$ otherwise.

PROOF.

(i) For all $\lambda \in F^\times$, we have $\|\lambda\| = |\lambda|$, giving the result.

(ii) For all $x, y \in A$, we have $\|xy\| \leq \|x\| \cdot \|y\|$, giving the result.

(iii) Let $x \in A$. Since $\mathrm{nrd}(x)$ is the product of the eigenvalues of x with multiplicity, we have $|\mathrm{nrd}(x)| \leq \|x\|^{ed}$ by Corollary 2.3.0.22, giving the result.

(iv) The right-to-left implication is clear. Assume $x \in A$ satisfies the left hand side. If F is nonarchimedean, then $\|x\| \leq 1$, so by Lemma 2.3.0.18 we have $x \in \mathcal{M}_d(\Lambda)$. Since $\mathrm{nrd}(x) \in \mathbb{Z}_F^\times$, we get $x \in K$. If F is archimedean, by Lemma 2.3.0.18 it suffices to prove the result when x is diagonal with positive real coefficients (a_i). The condition $\|x\| \leq 1$ gives $\max_i a_i \leq 1$, and the condition $|\mathrm{nrd}(x)| = 1$ gives $\prod_i a_i = 1$: we get $x = 1_A \in K$.

□

Finally, we prove an important relation between the height and the distance on the Riemannian symmetric space corresponding to the group of elements of reduced norm 1.

LEMMA 2.3.0.25. *Use the same notations as in Definition 2.3.0.23 and assume that F is archimedean. Let $g \in \mathrm{SL}_d(D)$ and denote by $\bar{d}(\cdot,\cdot)$ the canonical distance on the symmetric space $X = \mathrm{SL}_d(D)/\mathrm{SU}_d(D)$. Then*

$$\mathrm{h}(g)^2 \leq \frac{\bar{d}(g,1)^2}{2ed} \leq d \cdot \mathrm{h}(g)^2.$$

PROOF. By Cartan decomposition, it suffices to prove the result when g is a diagonal matrix with positive real coefficients (a_i). Let $n = [F : \mathbb{R}]$. Since the orbit of the set of such matrices on the symmetric space is a flat, we have

$$\bar{d}(g,1)^2 = 2edn\Big(\sum_i (\log a_i)^2\Big).$$

On the other hand, we have $\mathrm{h}(g) = n\max(0, \log\|g\|) = n\max(0, \log(\max_i a_i))$ by Lemma 2.3.0.18. Since $\prod_i a_i = 1$, the maximum is larger or equal to 1 and $\mathrm{h}(g)^2 = n\max_i(\log a_i)^2$. The claimed result is now equivalent to the simple inequality

$$\max_i(\log a_i)^2 \leq \sum_i (\log a_i)^2 \leq d\max_i(\log a_i)^2.$$

□

We also prove the p-adic version of this bound in the case of quaternion algebras: the natural space here is the Bruhat-Tits tree.

LEMMA 2.3.0.26. *Let F be a p-adic field and let $A = \mathcal{M}_2(F)$. Let P_0 be the fixed point of $\mathrm{GL}_2(\mathbb{Z}_F)$ in the Bruhat-Tits tree $\mathcal{T}_F$. Then for all $g \in A^1$, we have*

$$\mathrm{h}(g) = \tfrac{1}{2}d(g \cdot P_0, P_0) \cdot \log q,$$

where q is the cardinality of the residue field.

PROOF. Since both sides of the equality are invariant when we multiply g on either side by an element of $\mathrm{SL}_2(\mathbb{Z}_F)$, it suffices to prove the equality for a matrix of the form $g = \left(\begin{smallmatrix} \pi^t & 0 \\ 0 & \pi^{-t} \end{smallmatrix}\right)$ for some $t \in \mathbb{Z}_{>0}$. In this case we have $\mathrm{h}(g) = \log(|\pi^{-t}|^{[F:\mathbb{Q}_p]}) = t\log q$, and $d(g \cdot P_0, P_0) = 2t$ since g is proportional to $\left(\begin{smallmatrix} \pi^{2t} & 0 \\ 0 & 1 \end{smallmatrix}\right)$. This proves the lemma. □

We now turn to the global case and define a notion of height on a central simple algebra over a number field. In contrast with the commutative case, the height is not canonical: there are several heights on such an algebra, depending on a choice of a maximal order and an embedding into a product of matrix algebras. This reflects the fact that central simple algebras have a lot of automorphisms.

DEFINITION 2.3.0.27. Let F be a number field of degree n and let A be a central simple algebra of degree d over F. Let $\iota = (\iota_v)_{v\in\mathcal{V}_\infty}$ be a choice of isomorphism $\iota : A \otimes_{\mathbb{Q}} \mathbb{R} \to \prod_{v\in\mathcal{V}_\infty} \mathcal{M}_{d_v}(D_v)$ extending the embeddings $v \in \mathcal{V}_\infty$ and let $\mathcal{O}$ be a maximal order in A. We define a height on A depending on the pair $(\mathcal{O}, \iota)$. For every

finite place v, choose an isomorphism $\iota_v : A \otimes_F F_v \to \mathcal{M}_{d_v}(D_v)$ such that $\iota_v(\mathcal{O}) \subset \mathcal{M}_{d_v}(\Lambda_v)$. For an element $x \in A$ we define its *height* by the formula

$$\mathrm{H}(x) = \prod_{v \in \mathcal{V}_F} \mathrm{H}(\iota_v(x)).$$

More generally for a set S of places of F we define the S-part of the height of x to be $\mathrm{H}_S(x) = \prod_{v \in S} \mathrm{H}(\iota_v(x))$, which we also write $\mathrm{H}_f(x)$ when $S = \mathcal{V}_f$ is the set of all finite places and $\mathrm{H}_\infty(x)$ when $S = \mathcal{V}_\infty$ is the set of all infinite places. In every case we also define the *logarithmic height* $h_S(x)$ to be the logarithm of the corresponding height $\mathrm{H}_S(x)$.

Remarks 2.3.0.28.

(1) Given a maximal order $\mathcal{O}$ and a finite place v, when we choose an embedding ι_v the other possible choices are the conjugates of ι_v by $D_v^\times \cdot \mathrm{GL}_{d_v}(\Lambda_v)$, so $\mathrm{H}(\iota_v(x))$ does not depend on the choice of the particular embedding.
(2) This definition of the height is not exactly the same as in [**CS12**]. On the infinite part they are within a multiplicative factor of each other, the constant depending only on the dimension. Our definition is more adapted to our use since it is bi-K-invariant. On the finite part, they differ only at ramified places, where their height is $\mathrm{H}(\cdot)^{e_v}$. Our definition turned out to be technically simpler for our use.
(3) The name "height" is justified by the fact that there are finitely many elements of bounded height: the finite part bounds the denominator so we are left with a lattice in $A \otimes \mathbb{R}$, and the infinite part bounds the value of a norm on $A \otimes \mathbb{R}$, and the finiteness follows. Proposition 2.3.0.37 provides us with a quantitative version of this property.

We prove some properties of the height that are analogous to those of heights in number fields. The properties (i), (iii) and (iv) show some compatibility with the usual notion of height. The submultiplicativity (ii) is a natural property. The property (v) is analogous to Kronecker's theorem, except that there can be elements of finite order that do not have height 1: if there is one such noncentral element, then there are infinitely many of them by conjugating it.

Proposition 2.3.0.29. *Use the same notations as in Definition 2.3.0.27.*

(i) For all $\lambda \in F^\times$,

$$\mathrm{H}(\lambda) = \mathrm{H}_F(\lambda).$$

(ii) For all $x, y \in A$,

$$\mathrm{H}(xy) \leq \mathrm{H}(x)\mathrm{H}(y).$$

(iii) Let $x \in A$ and let L be a field that is a quotient of $F(x)$. Then

$$\mathrm{H}_L(x) \leq \mathrm{H}(x)^{[L:F]}.$$

(iv) For all $x \in A$,

$$\mathrm{H}_F(\mathrm{nrd}(x)) \leq \mathrm{H}(x)^d.$$

(v) For all $x \in A^\times$,

$$\mathrm{H}(x) = 1 \iff x \in \mathcal{O}^\times \text{ and } \iota(x) \in K,$$

where $K = \prod_{v \in \mathcal{V}_\infty} \mathrm{U}_{d_v}(D_v)$. In particular, any such x is a root of unity.

PROOF. To prove (i), (ii) and (iv), multiply the corresponding local inequalities from Lemma 2.3.0.24. To prove (iii), let α be the image of the element x in the number field L. We have

$$\mathrm{H}_L(\alpha) = \prod_v \prod_{w|v} \max\Big(1, |\alpha|_w^{[L_w:\mathbb{Q}_p]}\Big).$$

Fix a place v of F, and note that for all $w \mid v$, we have $|\alpha|_w = |\lambda|_v$ for some eigenvalue λ of x in an algebraic extension of F_v. By Corollary 2.3.0.22, we have $|\lambda|_v \leq \|\iota_v(x)\|$, giving $\max\Big(1, |\alpha|_w^{[L_w:\mathbb{Q}_p]}\Big) \leq \mathrm{H}(\iota_v(x))^{[L_w:F_v]}$. Using the relation $\sum_{w|v}[L_w : F_v] = [L : F]$ and taking the product over all places gives the result. The right-to-left part of (v) is clear. Assume $x \in A^\times$ has height 1. By (iv) and Kronecker's theorem, $\mathrm{nrd}(x)$ is a root of unity, so we can apply (iv) of Lemma 2.3.0.24: for every finite place v of F, $\iota_v(x) \in \mathrm{GL}_{d_v}(\Lambda_v)$ and every infinite place v of F, $\iota_v(x) \in \mathrm{U}_{d_v}(D_v)$. This implies that $x \in \mathcal{O}^\times$ and $\iota(x) \in K$. Since $\iota(\mathcal{O})$ is discrete and K is compact, x is a root of unity. □

Finally, we give the global version of the comparison between the height and the distance on the Riemannian symmetric space.

PROPOSITION 2.3.0.30. *Use the same notations as in Definition 2.3.0.27. Let r_1, r_2 denote the number of real and complex places of F, respectively. Let $g \in \mathcal{O}^1$ and denote by $\bar{d}(\cdot,\cdot)$ the canonical distance on the symmetric space $X = (A \otimes_{\mathbb{Q}} \mathbb{R})^1/K$. Then*

$$\sqrt{\frac{2d}{r_1 + r_2}} \cdot \mathrm{h}(g) \leq \bar{d}(\iota(g), 1) \leq d\sqrt{2} \cdot \mathrm{h}(g).$$

PROOF. Let $x \in \mathcal{O}^1$, so that $\mathrm{h}(x) = \mathrm{h}_\infty(x)$. Let

$$H_1 = \mathrm{h}(x) = \sum_{v|\infty} \mathrm{h}(\iota_v(x)) \text{ and } H_2 = \Big(\sum_{v|\infty} \mathrm{h}(\iota_v(x))^2\Big)^{1/2}.$$

By the standard inequalities between L^1 and L^2 norms we have

$$H_2 \leq H_1 \leq \sqrt{r_1 + r_2} \cdot H_2.$$

On the other hand, since the symmetric space X is the direct sum of its simple components, we have

$$\bar{d}(\iota(g), 1)^2 = \sum_{v|\infty} \bar{d}(\iota_v(g), 1)^2.$$

Lemma 2.3.0.25 now provides the inequality $2d \cdot H_2^2 \leq \bar{d}(\iota(g), 1)^2 \leq 2d^2 \cdot H_2^2$, proving the result. □

In fact, the Riemannian distance on G/K is not very well adapted to the estimation of heights. We will use the following modified notion of distance.

DEFINITION 2.3.0.31. Use the same notations as in Definition 2.3.0.27. Consider the group

$$G = \prod_{v \in \mathcal{V}_\infty} \mathrm{SL}_{d_v}(D_v).$$

We define a symmetric, subadditive, left G-invariant function δ corresponding to the symmetric subadditive function ρ defined as follows. For all $g \in G$,

$$\rho(g) = \sum_{v \in \mathcal{V}_\infty} [F_v : \mathbb{R}] \cdot \log \max(\|g_v\|, \|g_v^{-1}\|).$$

We give a comparison between this modified distance, the height and the canonical Riemannian distance:

LEMMA 2.3.0.32. *Use the same notations as in Definition 2.3.0.31. Let r_1, r_2 denote the number of real and complex places of F, respectively. For all $g \in G$ we have*

$$\mathrm{h}(g) \leq \rho(g) \leq \sqrt{\frac{r_1 + r_2}{2d}} \cdot \bar{d}(g, 1).$$

PROOF. For all $v \in \mathcal{V}_\infty$, we have $\|g_v\| \geq 1$ by Corollary 2.3.0.22, since $\mathrm{nrd}(g_v) = 1$. This gives $\mathrm{h}(g) = \sum_{v \in \mathcal{V}_\infty} [F_v : \mathbb{R}] \cdot \log \|g_v\| \leq \rho(g)$. By Lemma 2.3.0.25 we have for all $v \in \mathcal{V}_\infty$, $2d[F_v : \mathbb{R}] \log \|g_v\|^2 \leq \bar{d}(g_v, 1)^2$ and similarly for g_v^{-1}. This gives the bound $\sqrt{2d} \cdot \rho(g) \leq \sum_{v \in \mathcal{V}_\infty} \bar{d}(g_v, 1)$, and the result follows from the Cauchy-Schwarz inequality. □

The algorithmic relevance of this notion of height is twofold. First, we can enumerate the set of elements of height bounded by some value. This is clear from the argument in Remarks 2.3.0.28, a more precise version is contained in Proposition 2.3.0.37. Second, the height of an element is related to the number of digits required to write this element as a linear combination of an integral basis, so it indicates whether an element is "small" and should be manipulated as is, or whether it is "big" and should be represented in a compact way. This is the content of Proposition 2.3.0.37. For this purpose, we need a quadratic form with respect to which we can reduce the integral basis of an order. Again, in the number field case there is a canonical quadratic form that we can use [**Bel04**, Section 4]; our quadratic form is constructed in analogy with the number field case but depends on a choice of embedding.

DEFINITION 2.3.0.33. Let $F = \mathbb{R}$ or $\mathbb{C}$, let D be a division algebra of degree e over F, let d be a positive integer and let $A = \mathcal{M}_d(D)$. We define the L^2 *norm* $\|M\|_2$ of a matrix $M \in A$ by

$$\|M\|_2^2 = \mathrm{trd}(M\overline{M}^t).$$

Now let $A = \prod_i A_i$ with $A_i = \mathcal{M}_{d_i}(D_i)$ where D_i a central division algebra of degree e_i over $F_i \in \{\mathbb{R}, \mathbb{C}\}$. The *quadratic form* T_2 is defined for all $x \in A$ by

$$T_2(x) = \sum_i [F_i : \mathbb{R}] \cdot \|x_i\|_2^2.$$

Finally let F be a number field of degree n and A be a central simple algebra of degree d over F. Let $\iota = (\iota_v)_{v\in\mathcal{V}_\infty}$ be a choice of isomorphism $\iota : A \otimes_{\mathbb{Q}} \mathbb{R} \to \prod_{v\in\mathcal{V}_\infty} \mathcal{M}_{d_v}(D_v)$ extending the embeddings $v \in \mathcal{V}_\infty$. The *quadratic form* T_2 corresponding to the isomorphism ι is the positive definite quadratic form defined for all $x \in A \otimes_{\mathbb{Q}} \mathbb{R}$ by

$$T_2(x) = T_2(\iota(x)) = \sum_{v\in\mathcal{V}_\infty} [F_v : \mathbb{R}] \cdot \|\iota_v(x)\|_2^2.$$

We give simple properties of this quadratic form. The first one is used to prove that there is no very short vector in an order of the algebra, and the second one is used to prove that there is a basis of which we an control the size in terms of the discriminant of the algebra.

LEMMA 2.3.0.34. *Use the same notations as in Definition 2.3.0.33. Let $\mathcal{O}$ be an order in A, and let $N = nd^2 = \dim_{\mathbb{Q}} A$.*

(i) For all $x \in A$,

$$|N_{A\otimes\mathbb{R}/\mathbb{R}}(x)| \leq \left(\frac{T_2(x)}{nd}\right)^{\frac{N}{2}};$$

(ii) The covolume of the lattice $\mathcal{O}$ with respect to T_2 is $\Delta_{\mathcal{O}}^{1/2}$.

PROOF.

(i) It is equivalent to prove that for all $M = (M_v) \in \prod_{v\in\mathcal{V}_\infty} \mathcal{M}_{d_v}(D_v)$ we have

$$\prod_{v\in\mathcal{V}_\infty} |\mathrm{nrd}(M_v)|^{2[F_v:\mathbb{R}]d} \leq (nd)^{-N} T_2(M)^N.$$

By Cartan decomposition it suffices to show this when all the components of M are diagonal matrices with positive real coefficients $(a_{v,i})$. In that case the inequality we want to prove is rewritten

$$\left(\prod_{v\in\mathcal{V}_\infty}\prod_{i=1}^{d_v}(a_{v,i}^2)^{[F_v:\mathbb{R}]e_v d}\right)^{\frac{1}{N}} \leq \frac{1}{N}\sum_{v\in\mathcal{V}_\infty}[F_v:\mathbb{R}]e_v d\sum_{i=1}^{d_v} a_{v,i}^2.$$

But this is just the arithmetic and geometric means inequality applied to the $a_{v,i}^2$ with multiplicity $[F_v : \mathbb{R}]e_v d$ since we have $d_v e_v = d$ for all $v \in \mathcal{V}_\infty$ and $\sum_{v\in\mathcal{V}_\infty}[F_v : \mathbb{R}] = n$.

(ii) We have $\Delta_{\mathcal{O}} = |\det(\mathrm{Tr}_{F/\mathbb{Q}}(\mathrm{trd}(w_i w_j)))|$ where (w_i) is a $\mathbb{Z}$-basis of $\mathcal{O}$, so it suffices to find a basis (e_i) of $\prod_{v\in\mathcal{V}_\infty} \mathcal{M}_{d_v}(D_v)$ that is orthonormal with respect to T_2 and such that $|\det(T(e_i e_j))| = 1$, where $T = \sum_{v\in\mathcal{V}_\infty} \mathrm{Tr}_{K_v/\mathbb{R}} \circ \mathrm{trd}$. It is enough to do so for each simple factor. Let $E_{i,j}$ denote the matrix that is zero everywhere except for a 1 in the i-th row and j-th column. We denote by G the matrix with coefficients $T(e_i e_j)$.

- $\mathcal{M}_d(\mathbb{R})$: the basis $(E_{s,t})_{1\leq s,t\leq d}$ is orthonormal for T_2, and $T = \mathrm{Tr}$ is the usual matrix trace. We compute $E_{s,t}E_{u,v} = \mathbf{1}_{t=u}E_{s,v}$, so that

$$T(E_{s,t}E_{u,v}) = \mathbf{1}_{t=u,\, s=v}.$$

The matrix G is a permutation matrix, so it has determinant ± 1.

- $\mathcal{M}_d(\mathbb{C})$: the basis $(2^{-1/2}\alpha E_{s,t})_{1\leq s,t\leq d,\,\alpha\in\{1,i\}}$ is orthonormal for T_2, and we have $T = 2\,\mathrm{Re}\circ\mathrm{Tr}$. We compute $2^{-1/2}\alpha E_{s,t}\cdot 2^{-1/2}\beta E_{u,v} = 2^{-1}\alpha\beta\mathbf{1}_{t=u}E_{s,v}$, so that
$$T(2^{-1/2}\alpha E_{s,t}2^{-1/2}\beta E_{u,v}) = \pm\mathbf{1}_{t=u,\,s=v,\,\alpha=\beta}.$$
The matrix G is a signed permutation matrix, so it has determinant ± 1.
- $\mathcal{M}_{d/2}(\mathbb{H})$: the basis $(2^{-1/2}\alpha E_{s,t})_{1\leq s,t\leq d/2,\,\alpha\in\{1,i,i,ij\}}$ is orthonormal for T_2, and we have $T = \mathrm{trd}$. We compute $2^{-1/2}\alpha E_{s,t}\cdot 2^{-1/2}\beta E_{u,v} = 2^{-1}\alpha\beta\mathbf{1}_{t=u}E_{s,v}$ since $E_{s,t}$ commutes with β, so that
$$T(2^{-1/2}\alpha E_{s,t}2^{-1/2}\beta E_{u,v}) = \pm\mathbf{1}_{t=u,\,s=v,\,\alpha=\beta}.$$
The matrix G is a signed permutation matrix, so it has determinant ± 1.

□

We want to compare the quadratic form T_2 with the height. We start by comparing the norms. The reason for having two different norms on the local factors $\mathcal{M}_{d_v}(D_v)$ of the algebra A is that the norm $\|\cdot\|$ has nicer properties, but the norm $\|\cdot\|_2$ comes from a quadratic form and is easier to compute.

Lemma 2.3.0.35. *Let D be a division algebra over $\mathbb{R}$, let d be a positive integer and let $A = \mathcal{M}_d(D)$. For all $M \in A$ we have*
$$\|M\| \leq \|M\|_2 \leq \sqrt{d}\cdot\|M\|.$$

Proof. By Lemma 2.3.0.18 it suffices to consider the case where M is diagonal with positive real coefficients (a_i). But in this case we have $\|M\| = \max_i a_i$ and $\|M\|_2^2 = \sum_i a_i^2$. We get $\|M\|^2 \leq \|M\|_2^2 \leq d\|M\|$, giving the result. □

Now we can compare T_2 and the height.

Lemma 2.3.0.36. *Use the same notations as in Definition 2.3.0.33. Let $\mathcal{O}$ be a maximal order in A and* H *the height attached to $(\mathcal{O},\iota)$.*

(i) For all $x \in A$,
$$T_2(x) \leq nd\cdot\mathrm{H}(x)^2.$$

(ii) For all $x \in \mathcal{O}$,
$$\mathrm{H}(x) \leq \left(1+\frac{T_2(x)}{n}\right)^{\frac{n}{2}}.$$

Proof.

(i) For all $v \in \mathcal{V}_\infty$ and $M \in \mathcal{M}_{d_v}(D_v)$ we have $\|M\|_2^2 \leq d\,\|M\|^2 \leq d\,\mathrm{H}(M)^2$ by Lemma 2.3.0.35. Taking the sum over v gives the result.

(ii) For all $v \in \mathcal{V}_\infty$ and $M \in \mathcal{M}_{d_v}(D_v)$ we have $\mathrm{H}(M)^2 = \max(1, \|M\|^2)^{[F_v:\mathbb{R}]} \leq (1 + \|M\|^2)^{[F_v:\mathbb{R}]}$. If $x \in \mathcal{O}$, then $\mathrm{H}_f(x) = 1$, so

$$\begin{aligned}
\mathrm{H}(x)^{2/n} &= \mathrm{H}_\infty(x)^{2/n} \\
&\leq \Big(\prod_{v \in \mathcal{V}_\infty} (1 + \|\iota_v(x)\|^2)^{[F_v:\mathbb{R}]} \Big)^{1/n} \\
&\leq \Big(\prod_{v \in \mathcal{V}_\infty} (1 + \|\iota_v(x)\|_2^2)^{[F_v:\mathbb{R}]} \Big)^{1/n} \text{ by Lemma 2.3.0.35} \\
&\leq \frac{T_2(x)}{n} + 1
\end{aligned}$$

by the arithmetic and geometric means inequality applied to $\big(1+\|\iota_v(x)\|^2\big)_{v \in \mathcal{V}_\infty}$ with multiplicities $\big([F_v : \mathbb{R}]\big)_{v \in \mathcal{V}_\infty}$.

□

Finally, we state a precise relationship between the number of digits required to write an element as a linear combination of a reduced basis of an order and the height of this element. In particular, this provides an algorithm, most likely very inefficient, to enumerate the set of elements in an algebra with height bounded by a given constant.

Proposition 2.3.0.37. *Let A be a central simple algebra over the number field F. Let $\mathcal{O}'$ be an order in A and let* h *be the logarithmic height attached to a pair $(\mathcal{O}, \iota)$, where $\mathcal{O}$ is a maximal order containing $\mathcal{O}'$. Let $w_1, \ldots, w_N$ be a $\mathbb{Z}$-basis of $\mathcal{O}'$ that is LLL-reduced with respect to the quadratic form T_2 attached to ι. Let $x \in A$. If we write $x = \sum_{i=1}^N x_i w_i$, we have for all $1 \leq i \leq N$*

$$\log |x_i| \leq \mathrm{h}(x) + (i-1)\log 2 + (N-i)\log 3.$$

Conversely if $x \in \mathcal{O}$ we have

$$\mathrm{h}(x) \leq \frac{n}{2} \log \Delta_{\mathcal{O}'} + n \log\Big(\sum_{i=1}^N |x_i| \Big) + \frac{N(N-1)}{4} \log 2.$$

Let $x \in A$. Let $D \in \mathbb{Z}_{>0}$ be such that $Dx \in \mathcal{O}$. Then we have

$$\mathrm{h}(x) \leq n \log D + \mathrm{h}(Dx).$$

Conversely, there exists $D \in \mathbb{Z}_{>0}$ such that $Dx \in \mathcal{O}$ and

$$\log D \leq \mathrm{h}(x) \text{ and } \mathrm{h}(Dx) \leq (n+1)\mathrm{h}(x).$$

The coefficients $x_i \in \mathbb{Z}$ of $Dx = \sum_{i=1}^N x_i w_i$ satisfy for all $1 \leq i \leq N$

$$\log |x_i| \leq 2\mathrm{h}(x) + (i-1)\log 2 + (N-i)\log 3.$$

PROOF. Let $x \in A$. By considering the components of x on the basis (w_i^*) we get for all $1 \leq i \leq N$:

$$\left(x_i + \sum_{j>i} \mu_{j,i} x_j\right)^2 \cdot T_2(w_i^*) \leq T_2(x).$$

By (iii) of Proposition 1.2.1.2, we have $T_2(w_i^*) \geq T_2(w_i)/2^{i-1}$. Since every nonzero element $w \in \mathcal{O}$ has $N_{A/\mathbb{Q}}(w) \geq 1$, (i) of Lemma 2.3.0.34 gives $T_2(w_i) \geq nd$. Let $B = T_2(x)^{1/2} \cdot 2^{N-1}/\sqrt{nd}$. Then for all $1 \leq i \leq N$ we get

$$|x_{N-i}| \leq 2^{-i} B + \frac{1}{2} \sum_{j=0}^{i-1} |x_{N-j}|.$$

Let (u_i) be the sequence such that for all $i \geq 0$, $u_i = 2^{-i} + \frac{1}{2}\sum_{j=0}^{i-1} u_j$, so that $|x_{N-i}| \leq u_i B$. By solving the recurrence relation we obtain that for all $i \geq 0$, it is $u_i = \frac{1}{2}\left(\left(\frac{3}{2}\right)^i + \left(\frac{1}{2}\right)^i\right)$. Adding (i) of Lemma 2.3.0.36, we obtain

$$|x_{N-i}| \leq \mathrm{H}(x) \cdot 2^{N-1} \left(\frac{3}{2}\right)^i$$

as claimed.

Let $x \in \mathcal{O}$. By (iv) of Proposition 1.2.1.2 and (ii) of Lemma 2.3.0.34, for all $1 \leq i \leq N$ we have

$$T_2(w_i) \leq \frac{\Delta_A}{(nd)^{N-1}} \cdot 2^{\frac{N(N-1)}{2}}.$$

By (ii) of Lemma 2.3.0.36 we have

$$\mathrm{H}(x) \leq \left(1 + \frac{T_2(x)}{n}\right)^{n/2} \leq \left(\left(\frac{1}{dn} + \frac{1}{n}\right) T_2(x)\right)^{n/2} \leq \left(\frac{2}{n} T_2(x)\right)^{n/2},$$

where the second inequality comes from $T_2(x) \geq nd$. By triangle inequality we have

$$T_2(x)^{1/2} \leq \sum_{i=1}^{N} |x_i| \cdot T_2(w_i)^{1/2}.$$

Putting everything together we obtain

$$\mathrm{h}(x) \leq \tfrac{n}{2} \log \Delta_A + n \log(\textstyle\sum_i |x_i|) + \frac{N(N-1)}{4} \log 2 - \frac{N-1}{2} \log(nd) - \frac{n}{2} \log(\frac{n}{2}),$$

giving the result.

Let $x \in A$ and $D \in \mathbb{Z}_{>0}$ such that $Dx \in \mathcal{O}$. Then $x = D^{-1}(Dx)$ and $\mathrm{H}_F(D^{-1}) = D^n$, so (i) and (ii) of Lemma 2.3.0.29 yield the bound.

For the last statement, first consider a nonarchimedean local field F with residue field of size q and $A = \mathcal{M}_d(D)$. We have $|q| \leq q^{-1}$. For all $M \in \mathcal{M}_d(D)$, if $M \notin \mathcal{M}_d(\Lambda)$ let $D = \|M\| \in q^{\mathbb{Z}_{>0}}$. For all $1 \leq i, j \leq d$, we have $|(DM)_{i,j}| \leq |D| \cdot \|M\| \leq D^{-1}\|M\| = 1$, so $DM \in \mathcal{M}_d(\Lambda)$.

Now return to the global case. Let $x \in A$. Let $D = \mathrm{H}_f(x) \in \mathbb{Z}_{>0}$, then by the local case we have $Dx \in \mathcal{O}$, and $D = \mathrm{H}_f(x) \leq \mathrm{H}_f(x)\mathrm{H}_\infty(x) = \mathrm{H}(x)$. By (i) and (ii) of Lemma 2.3.0.29 we have $\mathrm{H}(Dx) \leq \mathrm{H}_F(D)\mathrm{H}(x) = D^n \mathrm{H}(x) \leq \mathrm{H}(x)^{n+1}$. The bound on the coefficients of Dx follows immediately from the first inequality for x. □

In particular, we immediately obtain a bound on the size of the coefficients of the multiplication table of an order.

COROLLARY 2.3.0.38. *Use the same notations as in Proposition 2.3.0.37. Then the coefficients $c_k^{i,j}$ of the multiplication table of the basis (w_i) satisfy*

$$\log |c_k^{i,j}| \leq n \log \Delta_{\mathcal{O}'} + \frac{N(N-1)}{2} \log 2 + (N-1) \log 3.$$

PROOF. This follows directly from the first two inequalities of Proposition 2.3.0.37 and $\mathrm{h}(xy) \leq \mathrm{h}(x) + \mathrm{h}(y)$ from Proposition 2.3.0.29. □

REMARK 2.3.0.39. Using the height quickly gives an bound here, but it is wasteful. A direct method would lead to a similar inequality with $n \log \Delta_{\mathcal{O}'}$ replaced by $\log \Delta_{\mathcal{O}'}$.

4. Units in division algebras

In this section, we make all the constants of Section 2 completely explicit to obtain bounds on the size of generators of S-units in division algebras.

4.1. Initial case: units of reduced norm 1. Now that we have a good notion of height to measure the size of elements, we exhibit explicit versions of the estimates of Section 2 in the case of division algebras. We proceed in three steps. First, we give estimates for the group of S-units of reduced norm 1 when S is a minimal set with the Eichler property. In the case of a totally definite quaternion algebra, this is the case that we considered in Section 1. In the other cases, we are simply considering the group of units of reduced norm 1, to which we apply precisely the methods of Section 2. The second step consists in using the strong approximation property to deduce a bound for the S-units of reduced norm 1 for large sets S from a bound for the minimal set S. In the third step we use Lenstra's theorem on S-units in number fields to pass from the S-units of reduced norm 1 to the full group of S-units.

To apply our method we need explicit Kazhdan pairs for suitable representations of semisimple groups. These are provided by the work of Shalom. The case where Property (T) holds is the simplest one.

THEOREM 2.4.1.1 (Shalom). *Let F be an archimedean local field, $d \geq 3$ an integer and D a central division algebra over F. Let $G = \mathrm{SL}_d(D)$ and consider the set*

$$Q = \left\{ \begin{pmatrix} 1 & \pm 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pm 2 & 1 \end{pmatrix} \right\},$$

which we see as embedded in the upper left corner of $\mathrm{SL}_d(D)$, that is

$$\begin{pmatrix} * & * & \\ * & * & \\ & & \mathrm{Id}_{d-2} \end{pmatrix}.$$

Let $\varepsilon = 2 - \sqrt{3}$. Then (Q, ε) is Kazhdan pair for G.

PROOF. [**Sha00**, Theorem A] □

When Property (T) does not hold, that is to say when the rank is 1 in our case, we have to work a bit more: we derive explicit estimates from the proof of Property (τ). We first describe a second theorem of Shalom. If K is a maximal compact subgroup of G, the family of representations without a K-invariant vector admits a Kazhdan pair (Lemma 5.1 of [**Sha00**]), so it suffices to restrict to study irreducible unitary representations with a K-invariant vector. Such representations, called *class one representations*, have a simple classification in terms of a parameter $\lambda \in i\mathbb{R} \cup [-\rho, \rho]$ where ρ is half the sum of the positive roots of G with the usual normalization [**Sha00**, Section 5]: $\rho = 1/2$ if $G = \mathrm{SL}_2(\mathbb{R})$, $\rho = 1$ if $G = \mathrm{SL}_2(\mathbb{C})$ and $\rho = 2$ if $G = \mathrm{SL}_2(\mathbb{H})$. We write π_λ the representation with parameter λ. The diagonal matrix coefficient $\langle \pi_\lambda(g)v_\lambda, v_\lambda \rangle$ where v_λ is a K-fixed vector is called a *spherical function*.

THEOREM 2.4.1.2 (Shalom). *Let $G = \mathrm{SL}_2(D)$, $K = \mathrm{SU}_2(D)$ and ρ be as above, and fix some $0 \leq \lambda_0 < \rho$. Let $\mathcal{F}_{\lambda_0}$ be the family of all the G-representations that do not weakly contain any representation π_λ with $\mathrm{Re}(\lambda) > \lambda_0$. Let n be an even integer satisfying*

$$n \geq \frac{\rho}{\rho - \lambda_0}.$$

Then (Q, ε) is a Kazhdan pair for $\mathcal{F}_{\lambda_0}$, where

$$Q = K \cup \left\{ \begin{pmatrix} 1 & \pm 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pm 2 & 1 \end{pmatrix} \right\} \subset G$$

and

$$\varepsilon = 1 - (\sqrt{3}/2)^{1/n}.$$

PROOF. [**Sha00**, Theorem 5.3] □

This allows us to obtain an explicit version of property (τ) for congruence groups in the case where we need it.

THEOREM 2.4.1.3 (Blomer–Brumley, Jacquet–Langlands, Burger–Sarnak, Shalom). *Let F be an archimedean local field and D a central division algebra over F. Let $G = \mathrm{SL}_2(D)$, $K = \mathrm{SU}_2(D)$ and consider the set*

$$Q = K \cup \left\{ \begin{pmatrix} 1 & \pm 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pm 2 & 1 \end{pmatrix} \right\} \subset G.$$

Let A be a central division algebra over a number field, let $\mathbf{G}$ be the algebraic group over $\mathbb{Q}$ such that $\mathbf{G}(\mathbb{Q}) = A^1$. Assume that G is one of the simple factors of $\mathbf{G}(\mathbb{R})$, and let Γ be a congruence subgroup of $\mathbf{G}(\mathbb{Q})$. Let $m = 2[F : \mathbb{R}]$, and let

$$\varepsilon = 1 - (\sqrt{3}/2)^{1/m}.$$

Then (Q, ε) is a Kazhdan pair for $L^2_0(\Gamma \backslash \mathbf{G}(\mathbb{R}))$ as a unitary representation of G.

PROOF. We view $L^2_0(\Gamma \backslash \mathbf{G}(\mathbb{R}))$ as a unitary representation of G. A division algebra as in the statement of the theorem can be of the following types:

(i) a quaternion algebra that is not totally definite;

(ii) a central division algebra of degree 4 over a totally real field, that is ramified at a real place v_0 such that $G \cong A^1_{v_0}$.

In case (i), we will see that the parameters λ of the irreducible class one representations of G weakly contained in $L^2_0(\Gamma\backslash\mathbf{G}(\mathbb{R}))$ satisfy $|\mathrm{Re}(\lambda)| \leq \frac{7}{64}$. By the Jacquet-Langlands correspondence, such irreducible representations are weakly contained in $L^2(\Gamma'\backslash\mathbf{G}'(\mathbb{R}))$ where $\mathbf{G}'$ is the restriction of scalars from $Z(A)$ to $\mathbb{Q}$ of SL_2 and Γ' is a congruence group. In that case, Blomer and Brumley [**BB11**] prove that the parameters λ of the irreducible class one representations weakly contained in $L^2_0(\Gamma\backslash\mathbf{G}(\mathbb{R}))$ satisfy $|\mathrm{Re}(\lambda)| \leq \frac{7}{64}$.

In case (ii), we will see that the parameters λ of the irreducible class one representations weakly contained in $L^2_0(\Gamma\backslash\mathbf{G}(\mathbb{R}))$ satisfy $\rho - \mathrm{Re}(\lambda) \geq \frac{57}{64}$. By the Grunwald–Wang theorem, A admits a splitting field L' that is a cyclic extension of $Z(A)$ of degree 4. The field L' embeds into A. Let L be the quadratic subfield of L' and let B be the centralizer of L in A. Then B is a central division quaternion algebra over L. Let $\mathbf{H}$ be the $\mathbb{Q}$-subgroup of $\mathbf{G}$ such that $\mathbf{H}(\mathbb{Q}) = B^1$. Since L' splits A, L has a complex w_0 above v_0 so that $\mathbf{H}(\mathbb{R})$ has a simple factor $\mathrm{SL}_2(\mathbb{C})$ corresponding to w_0. Then by a theorem of Burger and Sarnak [**BS91**], for every irreducible representation π weakly contained in $L^2(\Gamma\backslash\mathbf{G}(\mathbb{R}))$, the restriction $\pi' = \mathrm{Res}^{\mathbf{G}(\mathbb{R})}_{\mathbf{H}(\mathbb{R})}\pi$ is weakly contained in $L^2(\Gamma'\backslash\mathbf{H}(\mathbb{R}))$ for some congruence subgroup Γ' of $\mathbf{H}(\mathbb{Q})$. We may apply the case (i) to B to deduce that the irreducible representations weakly contained in π' have their parameters λ such that $|\mathrm{Re}(\lambda)| \leq \frac{7}{64}$. We apply the same method as in [**BS91**, Paragraph 4] to deduce the bound on π. Let $H = G \cap \mathbf{H}(\mathbb{R}) \cong \mathrm{SL}_2(\mathbb{C})$. Let $K = \mathrm{SU}_2(\mathbb{H})$ viewed as a subgroup of $G \subset \mathbf{G}(\mathbb{R})$ and $K_0 = K \cap \mathbf{H}(\mathbb{R})$. Consider an irreducible representation π_λ weakly contained in π with parameter $0 < \lambda < \rho$ (where $\rho = 2$), and let φ_λ be the associated spherical function. Then, considered as a function on H, φ_λ is bi-K_0-invariant of positive type and therefore by the theory of direct integrals (see [**BdlHV08**, Appendix F]) there exists a probability measure μ on $E = i\mathbb{R} \cup [0, 1]$ (viewed as the class one dual of H) such that for all $h \in H$,

$$\varphi_\lambda(h) = \int_E \varphi'_r(h) d\mu(r),$$

where φ'_r is the spherical function of H corresponding to the parameter $r \in E$. We have seen that for all r in the support of μ, we have $|\mathrm{Re}(r)| \leq \frac{7}{64}$ since π' has no H-invariant vectors. Let $X \in \mathfrak{sl}_2(\mathbb{H})$ be diagonal real and have norm 1 for the Killing form. We have $|\varphi'_r(\exp(tX))| \leq \exp((r-1)t + o(t))$ (see [**Kna01**, 8.47]), so that

$$\varphi_\lambda(\exp(tX)) = \left|\int_E \varphi'_r(h) d\mu(r)\right| \leq \exp\Big(-\frac{57}{64}t + o(t)\Big).$$

On the other hand, φ_λ being a spherical function for G gives

$$\varphi_\lambda(\exp(tX)) \sim_{t\to\infty} \exp((\lambda - \rho)t + o(t)).$$

We obtain $\rho - \mathrm{Re}(\lambda) \geq \frac{57}{64}$ as claimed.

We will now apply Theorem 2.4.1.2. From the above, the integer m of the theorem is an even integer such that the parameter λ of every irreducible representation

weakly contained in $L^2_0(\Gamma\backslash\mathbf{G}(\mathbb{R}))$ satisfies

$$m \geq \frac{\rho}{\rho - \mathrm{Re}(\lambda)}.$$

From this, Shalom's theorem provides the result. □

The second ingredient that we need is a lower bound on the volume of every ball in the quotient $\Gamma\backslash G$ of a suitably chosen small radius. If the group Γ were torsion-free, we could simply take the ball with radius half the length of the shortest geodesic, and this would amount to give a lower bound on the height of elements of $\mathcal{O}^1$: this is Lehmer's problem. More precisely, Lehmer conjectured that there is a lower bound on the height of all the algebraic numbers that are not roots of unity. Any bound towards this conjecture gives us the estimate we need. However, we also have to take into account torsion in $\mathcal{O}^1$. For this, we use an explicit version of the Margulis Lemma to reduce the local study around a point to the simplest possible groups.

THEOREM 2.4.1.4 (Wang, explicit Margulis Lemma). *Let $G = G_1 \times G_2 \times \cdots \times G_s$, where $G_i = \mathrm{SL}_{d_i}(D_i)$ with D_i a division algebra over $\mathbb{R}$. Define $C_{i,1}$ and $C_{i,2}$ as follows:*

- *If $G_i = \mathrm{SL}_{d_i}(\mathbb{R})$, $C_{i,1} = C_{i,2} = 1/\sqrt{d_i}$;*
- *if $G_i = \mathrm{SL}_{d_i}(\mathbb{C})$, $C_{i,1} = C_{i,2} = 1/\sqrt{2d_i}$;*
- *if $G_i = \mathrm{SL}_{d_i}(\mathbb{H})$, $C_{i,1} = C_{i,2}/\sqrt{2} = 1/\sqrt{4d_i}$.*

Let R_i be the least positive zero of the function

$$F_i(t) = \exp(C_{i,1}t) - 1 + 2\sin(C_{i,2}t) - C_{i,1}t/(\exp(C_{i,1}t) - 1).$$

Let $N = \{g \in G \mid d(g_i, 1) \leq R_i \text{ for all } i\}$. Then for any discrete subgroup Γ of G, the intersection $N \cap \Gamma$ generates a nilpotent group.

PROOF. [**Wan69**] □

We give a simple lower bound for the constants appearing in Wang's estimate.

LEMMA 2.4.1.5. *Let $a > 0$. Consider*

$$F(t) = \exp(t) - 1 + 2\sin(at) - \frac{t}{\exp(t) - 1}.$$

Let $b = \min(1, \pi/(2a))$. Then F is strictly increasing in $[0, b]$ and $F(b) > 0$. In Theorem 2.4.1.4, we have

$$R_i \geq \frac{1}{5C_{i,1}}.$$

PROOF. Let $g(t) = -t/(\exp(t) - 1)$. Since exp is convex, g is nondecreasing. Since $\sin(at)$ is nondecreasing in $[0, b]$, F is strictly increasing in $[0, b]$.

For all $t \in [0, b]$, we have $\exp(t) - 1 \geq t$, $2\sin(at) \geq 4at/\pi$ and $g(t) \geq -1$, giving $F(t) \geq t + 4at/\pi - 1$. If $b = 1$ then $t - 1 \geq 0$; if $b = \pi/(2a)$ then $4at/\pi - 1 \geq 0$, so that $F(b) > 0$.

By computing F with an explicitly bounded error term, we can prove that $F(1/5)$ is strictly negative when $a = 1$ or $a = \sqrt{2}$. In those cases we have $b = 1$, so the above shows that the least positive zero of F is larger than $1/5$, giving the result. □

To use the Margulis Lemma efficiently, we need some information on what the nilpotent groups that we encounter can be. This is provided by the following theorem.

THEOREM 2.4.1.6. *Let D be a division algebra of degree d over its center F, and let Γ be a nilpotent subgroup of $D^\times$. Then Γ has an abelian subgroup of index dividing d.*

PROOF. [**Weh07**] □

As mentioned before, a final ingredient is a bound towards Lehmer's conjecture. We use the very slowly decreasing bound of Dobrowolski, for which a good constant was proved by Voutier. In the case of degree 2 where the bound is trivial, we use a bound of Schinzel instead.

THEOREM 2.4.1.7 (Voutier, Schinzel). *Let α be an irrational algebraic number that is not a root of unity, let $L = \mathbb{Q}(\alpha)$ and let $d = [F : \mathbb{Q}]$. Then*

$$\mathrm{h}_L(\alpha) \geq \frac{1}{4}\left(\frac{\log\log d}{\log d}\right)^3.$$

If $d = 2$, then $\mathrm{h}_L(\alpha) \geq \log((1+\sqrt{5})/2)$.

PROOF. [**Smy08**, Sections 4.2 and 6.1] □

For later reference, we define a function $c_1 : \mathbb{Z}_{\geq 2} \to \mathbb{R}_{>0}$ by $c_1(2) = \log((1+\sqrt{5})/2)$ and $c_1(d) = \frac{1}{4}\left(\frac{\log\log d}{\log d}\right)^3$ if $d \geq 2$. Since the volume of a ball is not easy to compute exactly, we estimate it by using bounds on the curvature and Günther's comparison theorem.

LEMMA 2.4.1.8. *Let $d > 1$, $G = \mathrm{SL}_d(\mathbb{R})^s \times \mathrm{SL}_{\frac{d}{2}}(\mathbb{H})^r \times \mathrm{SL}_d(\mathbb{C})^{r_2}$ and $K = \mathrm{SO}_d(\mathbb{R})^s \times \mathrm{SU}_{\frac{d}{2}}(\mathbb{H})^r \times \mathrm{SU}_d(\mathbb{C})^{r_2}$. Let $0 \leq r \leq \frac{\pi}{2}\sqrt{d}$ and let $B = \{g \in G \mid d(g,1) \leq r\}$ be the closed ball of radius r in G. Then*

$$\mu(B) \geq v_{N_1} v_{N_2} \left(\frac{2}{\pi}\right)^{N_1-1} \left(\frac{r}{2}\right)^{N_1+N_2},$$

where $N_1 = \dim K$, $N_2 = \dim(G/K)$ and $v_N = \pi^{\frac{N}{2}}/\Gamma(1+\frac{N}{2})$ is the volume of the unit ball in N-dimensional Euclidean space.

PROOF. We have

$$\begin{aligned}\mu(B) &= \int_G \mathbf{1}_{d(x,1)\leq r} dx \\ &= \int_{G/K} \left(\int_K \mathbf{1}_{d(xk,1)\leq r} dk \right) d\mu(xK) \\ &\geq \int_{G/K} \left(\int_K \mathbf{1}_{d(k,1)\leq \frac{r}{2}} dk \right) \mathbf{1}_{d(x,K)\leq \frac{r}{2}} d\mu(xK) \\ &= \mu_K(B_1)\mu_{G/K}(B_2),\end{aligned}$$

where B_1 is the ball of radius $r/2$ in K and B_2 is the ball of radius $r/2$ in G/K. Since G/K has nonpositive sectional curvature, by Günther's comparison theorem [**Gün60**] we have

$$\mu_{G/K}(B_2) \geq v_{N_2} \left(\frac{r}{2} \right)^{N_2}.$$

The Riemannian metric is bi-invariant under K, so the sectional curvature on K satisfies $K(\sigma) = \frac{1}{4}\|[X,Y]\|^2$ where X, Y are orthonormal vectors of the plane σ and the norm is given by the Riemannian metric ([**CE75**, Corollary 3.19]). By [**Wan69**], we have $K(\sigma) \leq \kappa$ with $\kappa = \frac{1}{4d}$. By Günther's comparison theorem we get

$$\begin{aligned}\mu_K(B_1) &\geq N_1 v_{N_1} \int_{t=0}^{\frac{r}{2}} \kappa^{\frac{N_1-1}{2}} \sin(\sqrt{\kappa}t)^{N_1-1} dt \\ &\geq N_1 v_{N_1} \int_{t=0}^{\frac{r}{2}} \left(\frac{2}{\pi} t \right)^{N_1-1} dt \quad \text{since} \quad \frac{r}{2} \leq \frac{\pi}{2\sqrt{\kappa}} \\ &= v_{N_1} \left(\frac{2}{\pi} \right)^{N_1-1} \left(\frac{r}{2} \right)^{N_1}.\end{aligned}$$

Putting the two bounds together gives the result. □

Again, for later reference we define a function $c_2 : \mathbb{Z}_{\geq 1} \times \mathbb{Z}_{\geq 1} \times \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ by the formula

$$c_2(N_1, N_2, r) = v_{N_1} v_{N_2} \left(\frac{2}{\pi} \right)^{N_1-1} \left(\frac{r}{2} \right)^{N_1+N_2},$$

and we also set

$$c_2(G, r) = c_2(\dim K, \dim G/K, r)$$

for G, K as in Lemma 2.4.1.8. To account for torsion we use the simple bound of Lemma 2.1.2.2 on the number of roots of unity in a number field of given degree. We can finally give the required lower bound on the volume of balls in quotients $\Gamma\backslash G$.

PROPOSITION 2.4.1.9. *Let A be a central division algebra of degree d over a number field of degree n. Let $\iota : A \otimes_{\mathbb{Q}} \mathbb{R} \to \prod_{v|\infty} \mathcal{M}_{d_v}(D_v)$ be an isomorphism as in Definition 2.3.0.27. Let $\mathcal{O}$ be an order in A and let $\Gamma = \mathcal{O}^1$. Let $G = \prod_{v|\infty} \mathrm{SL}_{d_v}(D_v)$ and $\pi : G \to \Gamma\backslash G$ be the canonical projection. Let $\eta = \frac{1}{4}\sqrt{\frac{2}{d(r_1+r_2)}} c_1(nd)$ and let $B = \{g \in G \mid d(g,1) \leq \eta\}$ be the closed ball of radius η in G. Then*

$$\mu_{\Gamma\backslash G}(\pi(B)) \geq \frac{c_2(G,\eta)}{d(2nd)^{\frac{\log 3}{\log 2}}}.$$

PROOF. Let $g \in \mathcal{O}^1$ have infinite order. We want to bound $\bar{d}(\iota(g), 1)$ from below. Consider the logarithmic height h attached to a pair $(\mathcal{O}', \iota)$ where $\mathcal{O}'$ is a maximal order containing $\mathcal{O}$. By Proposition 2.3.0.30, we have $\bar{d}(\iota(g), 1) \geq \sqrt{\frac{2d}{r_1+r_2}}\mathrm{h}(g)$. By Proposition 2.3.0.29 (iii) and Theorem 2.4.1.7, we have $\mathrm{h}(g) \geq \frac{c_1(nd)}{d}$ since $\dim_F(F(g)) \leq d$. This gives

$$\bar{d}(\iota(g), 1) \geq \sqrt{\frac{2}{d(r_1+r_2)}}c_1(nd) = 4\eta.$$

Let Σ be the set of elements $g \in \mathcal{O}^1$ such that $gB \cap B \neq \emptyset$ and let N be the group generated by Σ. By Theorem 2.4.1.4 and Lemma 2.4.1.5, since $\mathcal{O}^1$ is discrete in G and $\eta \leq R_i/2$, the group N is nilpotent. By Theorem 2.4.1.6, it admits an abelian subgroup N' of index at most d. Since N' is abelian, it is contained in a subfield L of A, so that $[L : \mathbb{Q}] \leq nd$. Since the group of roots of unity in L is cyclic of cardinality at most $m = (2nd)^{\log 3/\log 2}$ by Lemma 2.1.2.2, N' has a torsion free abelian subgroup N'' of index at most m, and N'' has index at most dm in N.

Assume that $\#\Sigma > dm$. Then there exists two distinct elements $g, h \in N$ such that $gh^{-1} \in N''$. We get $\bar{d}(\iota(gh^{-1}), 1) \leq \bar{d}(\iota(g), 1) + \bar{d}(\iota(h), 1) \leq 4\eta$, and gh^{-1} is not a root of unity since N'' is torsion-free: this is impossible by the above. So we have $\#\Sigma \leq dm$, so the projection $B \to \pi(B)$ is at most dm-to-1 and $\mu(\pi(B)) \geq \mu(B)/dm$. Now Lemma 2.4.1.8 gives the result since $\eta \leq \frac{\pi}{2}\sqrt{d}$. □

We define $c_3(G) = \frac{c_2(G,\eta)}{d(2nd)^{\log 3/\log 2}}$ where $\eta = \frac{1}{4}\sqrt{\frac{2}{d(r_1+r_2)}}c_1(nd)$. The final ingredient is a bound on the volume of $\Gamma\backslash G$. In fact, there is an exact formula for this volume. We derive this formula from Prasad's general theorem. The formula is expressed in terms of Bruhat–Tits theory. Since we only use it to extract the volume formula, we do not introduce the complete definition. To a group $A^\times$ where A is a central simple algebra over a nonarchimedean local field, Bruhat–Tits theory attaches a finite-dimensional simplicial complex called a building, which is a generalization of Bruhat–Tits trees (Section 2.5). A parahoric subgroup of $A^\times$ is the stabilizer of a simplex in the building. Hyperspecial groups have a more complicated definition, also in terms of the building.

THEOREM 2.4.1.10 (Prasad). *Let A be a central simple algebra of degree d over a number field F of degree n, and let $\mathcal{O}$ be a maximal order in A. Let $G = (A \otimes_{\mathbb{Q}} \mathbb{R})^1$, and assume that G is not compact. Then*

$$\mu(\mathcal{O}^1\backslash G) = \left(\frac{\Delta_A}{|\Delta_F|}\right)^{\frac{1}{2}} (2d)^{\frac{n(d^2-1)}{2}} 2^{\frac{n(d-1)}{2}} \prod_{j=2}^{d} \zeta_F(j) \prod_{\mathfrak{p}|\delta_A} \phi(A, \mathfrak{p}),$$

where

$$\phi(A, \mathfrak{p}) = \prod_{0<i<d,\, e_\mathfrak{p} \nmid i} (1 - N(\mathfrak{p})^{-i}).$$

PROOF. We unfold Prasad's theorem [**Pra89**] in the case of interest to us. He starts with a number field k, which we will continue to write F. Similarly he writes $\mathfrak{f}_v$ the residue field at a finite place v, which we will continue to write $\mathbb{F}_v$. We should

take G an absolutely quasi-simple, simply connected group over F, which for us is the group such that $\mathrm{G}(F) = A^1$. Then we need $\mathscr{G}$, an absolutely quasi-simple, simply connected, quasi-split group over F, such that $\mathbf{G}$ is an inner form of $\mathscr{G}$: we take $\mathscr{G} = \mathrm{SL}_d$. Prasad then fixes an extension ℓ/F and an integer $\mathfrak{s}(\mathscr{G})$, but since $\mathscr{G}$ splits in our case, we have $\mathfrak{s}(\mathscr{G}) = 0$ and $\ell = F$. He lets r be the absolute rank of G and $m_1, \dots, m_r$ be the exponents of the simple, simply connected, compact real-analytic Lie group of the same type as $\mathscr{G}$. Since in our case $\mathscr{G}$ is of type A_{d-1}, we have $r = d - 1$ and $m_i = i$. We should also choose a finite set S of places of F: we simply take S to be the set $\mathcal{V}_\infty$ of infinite places.

The arithmetic groups considered by Prasad are defined locally, so we make choices so that this group is $\mathcal{O}^1$. For all finite v, we should fix a hyperspecial parahoric subgroup $\mathscr{P}_v$ of $\mathscr{G}(F_v)$, such that the family of such parahoric groups is coherent: we take $\mathscr{P}_v = \mathrm{SL}_d(\mathbb{Z}_{F_v})$. Bruhat-Tits theory then associates with $\mathscr{P}_v$ a smooth affine group scheme $\mathscr{G}_v$ over $\mathbb{Z}_{F_v}$ such that $\mathscr{G}_v(\mathbb{Z}_{F_v}) = \mathscr{P}_v$: in our case this is just $\mathscr{G}_v = \mathrm{SL}_{d/\mathbb{Z}_{F_v}}$. Turning to G again, we should choose a coherent family of parahoric subgroups $\mathrm{P}_v \subset \mathrm{G}(F_v)$ for all finite v: we take $\mathrm{P}_v = \mathrm{SL}_{d_v}(\Lambda_v)$. Again, Bruhat-Tits theory associates with P_v a smooth affine group scheme G_v over $\mathbb{Z}_{F_v}$ such that $\mathrm{G}_v(\mathbb{Z}_{F_v}) = \mathrm{P}_v$. The S-arithmetic group he considers is then $\Lambda = \mathrm{G}(F) \cap \prod_{v\in S} \mathrm{G}(F_v) \prod_{v\notin S} \mathrm{P}_v$, viewed as a subgroup of $\mathrm{G}_S = \prod_{v\in S} \mathrm{G}(F_v)$. In our case we obtain $\Lambda = \mathcal{O}^1$ and $\mathbf{G}_S = G$.

We then need to consider the reduction of the chosen parahoric groups over the residue fields. Let v be a finite place of F. Let $\overline{\mathscr{G}}_v$ (resp. $\overline{\mathrm{G}}_v$) be the group $\mathscr{G}_v \times_{\mathbb{Z}_{F_v}} \mathbb{F}_v$ (resp. $\mathbf{G}_v \times_{\mathbb{Z}_{F_v}} \mathbb{F}_v$). In our case we have $\overline{\mathscr{G}}_v = \mathrm{SL}_{d/\mathbb{F}_v}$ and $\overline{\mathrm{G}}_v$ is the group over $\mathbb{F}_v$ such that $\overline{\mathrm{G}}_v(\mathbb{F}_v) = \mathrm{SL}_{d_v}(\mathbb{L}_v)$ where $\mathbb{L}_v$ is the extension of $\mathbb{F}_v$ of degree e_v. We should then fix $\overline{\mathscr{M}}_v$ (resp. $\overline{\mathrm{M}}_v$) to be a maximal connected reductive $\mathbb{F}_v$-subgroup of $\overline{\mathscr{G}}_v$ (resp. $\overline{\mathrm{G}}_v$). In our case we simply take $\overline{\mathscr{M}}_v = \overline{\mathscr{G}}_v$ and $\overline{\mathrm{M}}_v = \overline{\mathrm{G}}_v$ as they are already reductive.

Now Prasad defines a Haar measure on $\mathrm{G}(F_v)$ for each infinite place v to be the unique Haar measure such that the induced volume of a maximal compact subgroup of $\mathrm{Res}_{F_v/\mathbb{R}}(\mathrm{G})(\mathbb{C})$ is 1. We will write this measure μ_{Pras}. Let $S = \mathcal{V}_\infty$. Since the Tamagawa number of G is $\tau_F(\mathrm{G}) = 1$, Prasad's formula reads

$$\mu_{\mathrm{Pras}}(\Lambda\backslash \mathrm{G}_S) = |\Delta_F|^{\frac{\dim \mathrm{G}}{2}} \left(\prod_{i=1}^{r} \frac{m_i!}{(2\pi)^{m_i+1}} \right)^n \prod_{v\notin S} \frac{q_v^{(\dim \overline{\mathrm{M}}_v + \dim \overline{\mathscr{M}}_v)/2}}{\#\overline{\mathrm{M}}_v(\mathbb{F}_v)}.$$

We have:

- $\dim \mathrm{G} = d^2 - 1$,
- $\dim \overline{\mathscr{M}}_v = d^2 - 1$,
- $\dim \overline{\mathrm{M}}_v = e_v d_v^2 - 1 = d d_v - 1$,
- $\#\overline{\mathrm{M}}_v(\mathbb{F}_v) = (q_v - 1)^{-1} \#\mathrm{GL}_{d_v}(\mathbb{L}_v) = (q_v - 1)^{-1} \prod_{i=0}^{d_v - 1} (q_v^d - q_v^{i e_v})$.

For all but finitely many v, the factor is $f(q_v) = \frac{q_v^{\dim \overline{\mathscr{M}}_v}}{\#\overline{\mathscr{M}}_v(\mathbb{F}_v)}$, so we start by this case:

$$\begin{aligned} f(q_v) &= \frac{q_v^{\dim \overline{\mathscr{M}}_v}}{\#\overline{\mathscr{M}}_v(\mathbb{F}_v)} \\ &= \frac{q_v^{d^2-1}}{(q_v-1)^{-1}\prod_{i=0}^{d-1}(q_v^d - q_v^i)} \\ &= \frac{1-q_v^{-1}}{\prod_{i=0}^{d-1}(1-q_v^{i-d})} \\ &= \frac{1-q_v^{-1}}{\prod_{j=1}^{d}(1-q_v^{-j})} \\ &= \prod_{j=2}^{d}(1-q_v^{-j})^{-1}, \end{aligned}$$

so that the product of $f(q_v)$ over all finite places v is $\prod_{j=2}^d \zeta_F(j)$. For ramified $v \notin S$, we should correct with the factor

$$\begin{aligned} & \frac{q_v^{(\dim \overline{\mathrm{M}}_v - \dim \overline{\mathscr{M}}_v)/2}}{\#\overline{\mathrm{M}}_v(\mathbb{F}_v)/\#\overline{\mathscr{M}}_v(\mathbb{F}_v)} \\ = & \frac{q_v^{d(d_v-d)/2}\prod_{i=1}^{d-1}(q_v^d - q_v^i)}{\prod_{i=1}^{d_v-1}(q_v^d - q_v^{ie_v})} \\ = & q_v^{\frac{d(d_v-d)}{2}} \prod_{0<i<d,\, e_v\nmid i} (q_v^d - q_v^i) \\ = & q_v^{\frac{d(d-d_v)}{2}} \prod_{0<i<d,\, e_v\nmid i} (1 - q_v^{i-d}) \\ = & q_v^{\frac{d(d-d_v)}{2}} \prod_{0<i<d,\, e_v\nmid i} (1 - q_v^{-i}). \end{aligned}$$

Since the reduced discriminant of A is $\delta_A = \prod_{\mathfrak{p}} \mathfrak{p}^{d-d_{\mathfrak{p}}}$, this finally gives the formula

$$\mu_{\mathrm{Pras}}(\mathcal{O}^1\backslash G) = |\Delta_F|^{\frac{d^2-1}{2}} N(\delta_A)^{\frac{d}{2}} \left(\prod_{i=1}^{r} \frac{m_i!}{(2\pi)^{m_i+1}}\right)^n \prod_{j=2}^{d} \zeta_F(j) \prod_{\mathfrak{p}\mid\delta_A} \phi(A,\mathfrak{p}),$$

where

$$\phi(A,\mathfrak{p}) = \prod_{0<i<d,\, e_{\mathfrak{p}}\nmid i} (1 - N(\mathfrak{p})^{-i}).$$

Now in the Lie algebra of $\mathrm{SL}_d(\mathbb{C})$, the basis formed by the matrices $E_{i,i} - E_{i+1,i+1}$ for $1 \leq i < d$ and the matrices $E_{i,j}$ for $1 \leq i \neq j \leq d$ is a Chevalley basis. The determinant of the Gram matrix of this basis relatively to our choice of scalar product is $(2d)^{d^2-1}2^{d-1}$, so for our normalization, the volume of a maximal compact

subgroup of $\mathrm{Res}_{F_v/\mathbb{R}}(\mathrm{G})(\mathbb{C})$ is

$$\left((2d)^{\frac{d^2-1}{2}}2^{\frac{d-1}{2}}\prod_{i=1}^{r}\frac{(2\pi)^{m_i+1}}{m_i!}\right)^{[F_v:\mathbb{R}]}.$$

Changing the normalization from μ_{Pras} to μ and noting that $\Delta_A = |\Delta_F|^{d^2}N(\delta_A)^d$, we finally obtain the formula

$$\mu(\mathcal{O}^1\backslash G) = \left(\frac{\Delta_A}{|\Delta_F|}\right)^{\frac{1}{2}}(2d)^{\frac{n(d^2-1)}{2}}2^{\frac{n(d-1)}{2}}\prod_{j=2}^{d}\zeta_F(j)\prod_{\mathfrak{p}|\delta_A}\phi(A,\mathfrak{p})$$

as claimed. □

Putting all the ingredients together finally gives the desired bound.

Proposition 2.4.1.11. *Let A be a central division algebra of degree d over a number field F of degree n. Let ι be an isomorphism $A\otimes_{\mathbb{Q}}\mathbb{R}\to\prod_{v\in\mathcal{V}_\infty}\mathcal{M}_{d_v}(D_v)$ as in Definition 2.3.0.27 and $G=\prod_{v\in\mathcal{V}_\infty}\mathrm{SL}_{d_v}(D_v)$. Let $\mathcal{O}$ be a maximal order in A. Recall Definition 2.3.0.31: for $g,h\in G$*

$$\delta(g,h)=\sum_{v\in\mathcal{V}_\infty}\log\max(\|h_v^{-1}g_v\|,\|g_v^{-1}h_v\|).$$

Then the Dirichlet domain

$$\{g\in G\mid \delta(g,1)\leq\delta(\gamma g,1)\text{ for all }\gamma\in\Gamma\}$$

relative to δ for the group $\Gamma=\iota(\mathcal{O}^1)$ acting on G satisfies

$$\max_{g\in D}\delta(g,1)\leq R,$$

and Γ is generated by the set of elements $\gamma\in\Gamma$ such that

$$\delta(\gamma,1)\leq 2R$$

where

$$R=C_1\log\left(\frac{\Delta_A}{|\Delta_F|}\right)+C_2,$$

and C_1,C_2 are defined from the following ε, d_0 and r:

- *if F is totally real, $d=4$ and A is ramified at every real place, $\varepsilon=1-(\sqrt{3}/2)^{1/2}$, $d_0=2$ and $r=\frac{1}{2}\log(3+2\sqrt{2})$;*
- *otherwise, if $d\geq 3$, $\varepsilon=2-\sqrt{3}$, $d_0=d/2$, and $r=\frac{1}{2}\log(3+2\sqrt{2})$ if F is totally real and every real place is ramified, $d_0=d$ and $r=\log(3+2\sqrt{2})$ if F is not totally real and every real place is ramified, $d=d_0$ and $r=\frac{1}{2}\log(3+2\sqrt{2})$ otherwise;*
- *if $d=2$ and every real place is ramified, $\varepsilon=1-(\sqrt{3}/2)^{1/4}$, $d_0=2$ and $r=\log(3+2\sqrt{2})$;*
- *otherwise, $\varepsilon=1-(\sqrt{3}/2)^{1/2}$, $d_0=d$ and $r=\frac{1}{2}\log(3+2\sqrt{2})$.*

Let $V_1 = (2d)^{\frac{n(d^2-1)}{2}} 2^{\frac{n(d-1)}{2}} \prod_{j=2}^{d} \zeta(j)^n$. *Then*

$$C_1 = \frac{r}{\lfloor \frac{d_0}{2} \rfloor \log(1+\varepsilon/4)} \text{ and } C_2 = 2C_1 \log(V_1/(2c_3(G))) + 2r + \frac{c_1(nd)}{2d}.$$

Proof. We could apply Proposition 2.2.0.14 with the symmetric subadditive function $\delta(\cdot,\cdot)$ and the Kazhdan pairs of Theorems 2.4.1.1 and 2.4.1.3, but that would be wasteful since we would only use a very small subgroup of the group G to cover the Dirichlet domain. Instead, we are going to use *several* Kazhdan pairs in turn.

Let $H \subset G$ be the following subgroup:

- if F is totally real, $d = 4$ and A is ramified at every real place, H is one of the factors $\mathrm{SL}_2(\mathbb{H})$;
- otherwise, if $d \geq 3$, H is a factor $\mathrm{SL}_d(\mathbb{C})$ if F is not totally real and every real place is ramified, H is a factor $\mathrm{SL}_{d/2}(\mathbb{H})$ if F is totally real and every real place is ramified, and H is a factor $\mathrm{SL}_d(\mathbb{R})$ otherwise;
- if $d = 2$ and every real place is ramified, H is a factor $\mathrm{SL}_2(\mathbb{C})$;
- otherwise, H is a factor $\mathrm{SL}_2(\mathbb{R})$.

Let $v_0 \in \mathcal{V}_\infty$ be such that $H = \mathrm{SL}_{d_{v_0}}(D_{v_0})$. For all $1 \leq i \leq \lfloor \frac{d_{v_0}}{2} \rfloor$, let Q_i be the set

$$Q_i = \mathrm{SU}_2(D_{v_0}) \cup \left\{ \begin{pmatrix} 1 & \pm 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pm 2 & 1 \end{pmatrix} \right\},$$

seen as embedded in the $(2i-1, 2i-1) - (2i-1, 2i) - (2i, 2i) - (2i, 2i-1)$ square of $\mathrm{SL}_{d_{v_0}}(D_{v_0})$. By Theorems 2.4.1.1 and 2.4.1.3, for all i, the pair (Q_i, ε) is a Kazhdan pair for $L^2_0(\Gamma\backslash G)$ as a representation of H. Let $d_0 = d_{v_0}$ and let

$$Q = \prod_{i=1}^{\lfloor \frac{d_0}{2} \rfloor} Q_i.$$

Let $\eta = \frac{1}{4}\sqrt{\frac{2}{d(r_1+r_2)}} c_1(nd)$. By Proposition 2.4.1.9, $v = c_3(G)$ is a lower bound for the volume of d-balls of radius η in $\Gamma\backslash G$, and these are contained in δ-balls of radius $\eta_0 = \eta\sqrt{\frac{r_1+r_2}{2d}} = \frac{c_1(nd)}{4d}$ by Lemma 2.3.0.32. By Lemma 2.2.0.6, while $\mu(X)/\mu(\Gamma\backslash G) \leq 1/2$, multiplying by Q_i increases the volume by a factor of $1 + \varepsilon/4$. So when multiplying by Q, the volume increases by a factor of $(1+\varepsilon/4)^{\lfloor \frac{d_0}{2} \rfloor}$. Starting with a δ-ball of radius η_0 and letting $r = \max_{g \in Q} \rho(g)$, we obtain that the Dirichlet domain relative to δ for the group Γ acting on G satisfies

$$\max_{g \in D} \delta(g, 1) \leq R$$

with

$$R = \frac{2r}{\lfloor \frac{d_0}{2} \rfloor \log(1+\varepsilon/4)} \log\left(\frac{V}{v}\right) + 2r + 2\eta_0.$$

In order to obtain r, we compute $\|g\|$ for the triangular matrices in Q. For this, let $M = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, and let $M = k_1 a k_2$ be its Cartan decomposition. We have $M^t M = k_2^t a^t k_1^t k_1 a k_2 = k_2^{-1} a^t a k_2$, so it suffices to compute the eigenvalues of $M^t M = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$: those are $3 \pm 2\sqrt{2}$. This gives the values of r as in the proposition.

We bound the volume $V = \mu(\Gamma\backslash G)$ with Prasad's formula: we write

$$V = \left(\frac{\Delta_A}{|\Delta_F|}\right)^{\frac{1}{2}} \cdot V_0.$$

Since for all $j \geq 2$ we have $\zeta_F(j) \leq \zeta(j)^n$ by Lemma 2.1.2.1 and since the product $\prod_{\mathfrak{p}|\delta_A} \phi(A, \mathfrak{p})$ is less than 1, we have $V_0 \leq (2d)^{\frac{n(d^2-1)}{2}} 2^{\frac{n(d-1)}{2}} \prod_{j=2}^{d} \zeta(j)^n = V_1$. □

Remark 2.4.1.12. This bound can probably be improved, for instance in rank one by directly using estimates of the eigenvalues of the Laplace operator, adapting the bounds of [**CGY97**] and working directly in the symmetric space. However, it is not clear how to extend this method to non-cocompact groups, whereas our method does extend as we have seen. In higher rank, the Laplace operator method gives worse bounds than our method. We might be able to obtain sharper bounds by using the spectral theory of semisimple groups in a finer way, but we leave this for a later work.

4.2. Enlarging the set S. In Section 1 and Proposition 2.4.1.11, we have obtained bounds for the generators of the groups of S-units of reduced norm 1 for S a minimal set satisfying the Eichler condition. In this section we show how to extend those bounds to any set of places containing the infinite places. Note that we could use Prasad's formula for the volume of S-arithmetic groups and apply the same method as we did for the group $\mathcal{O}^1$. However, we are going to use another method that describes more explicitly a set of generators of the group $\mathcal{O}_S^1$ for large sets S in terms of generators of $\mathcal{O}'^1$ for *several* orders $\mathcal{O}'$. This structure of proof is more adapted to the design of algorithms for computing these groups.

The idea is that putting together the units in locally conjugated orders will generate the S-units of the orders. We start with a local version of this statement.

Lemma 2.4.2.1. *Let F be a nonarchimedean local field and $d \geq 2$ an integer. Let D be a central division algebra over F and $A = \mathcal{M}_d(D)$. Let Λ be the unique maximal order of D and Π a uniformizer. Let $x \in A^\times$ be the diagonal matrix $(\Pi, 1, \ldots, 1)$. Let $\mathcal{O} = \mathcal{M}_d(\Lambda)$ and $\mathcal{O}' = x\mathcal{O}x^{-1}$. Then the group generated by $\mathcal{O}^1 \cup \mathcal{O}'^1$ is A^1.*

Proof. Let $G \subset A^1$ be the group generated by $\mathcal{O}^1 \cup \mathcal{O}'^1$. Let $2 \leq j \leq d$ and consider the group $H = \mathrm{SL}_2(D)$, seen as embedded into the $(1,1) - (1,j) - (j,j) - (j,1)$ square of $\mathrm{SL}_d(D)$. Then $\mathcal{O}^1 \cap H = \mathrm{SL}_2(\Lambda)$ and $\mathcal{O}'^1 \cap H = x\mathrm{SL}_2(\Lambda)x^{-1}$ is the

set of matrices of the form

$$\begin{pmatrix} \Pi a \Pi^{-1} & \Pi b \\ c\Pi^{-1} & d \end{pmatrix} \text{ with } a, b, c, d \in \Lambda$$

with reduced norm 1. By Ihara's theorem [**Ser80**, Chapter II 1.4 Corollary 1] the group generated by $\mathrm{SL}_2(\Lambda)$ and $x\mathrm{SL}_2(\Lambda)x^{-1}$ is $\mathrm{SL}_2(D)$ (in fact, the group $\mathrm{SL}_2(D)$ is even an amalgamated product of these two groups), so G contains H. Moreover, $\mathcal{O}^1 = \mathrm{SL}_d(\Lambda)$ contains the even permutation matrices. By conjugating with the matrices of those permutations that act transitively on $\{1, \ldots, d\}$, we obtain that G contains every copy of $\mathrm{SL}_2(D)$ embedded in the $(i,i) - (i,j) - (j,i) - (j,j)$ corner of $\mathrm{SL}_d(D)$, so in particular G contains every elementary matrix. This implies that $G = A^1$. □

We now use the strong approximation property to lift the property from local to global.

Lemma 2.4.2.2. *Let A be a central simple algebra over a number field F and let $\mathcal{O}$ be a maximal order. Let S be a finite set of places containing the infinite places and satisfying the Eichler condition. Let T be a finite set of places disjoint from S. For every prime $\mathfrak{p}$ in T, choose a right integral $\mathcal{O}$-ideal $I^{(\mathfrak{p})}$ of norm $\mathfrak{p}$ and let $\mathcal{O}^{(\mathfrak{p})} = \mathcal{O}_l(I^{(\mathfrak{p})})$. Then the group generated by the set*

$$\mathcal{O}_S^1 \cup \bigcup_{\mathfrak{p} \in T} \mathcal{O}_S^{(\mathfrak{p})1}$$

is the group $\mathcal{O}_{S\cup T}^1$.

Proof. Let $\Gamma \subset \mathcal{O}_{S\cup T}^1$ be the group generated by $\mathcal{O}_S^1 \cup \bigcup_{\mathfrak{p}\in T} \mathcal{O}_S^{(\mathfrak{p})1}$. For every $v \in T$ we can choose an isomorphism $\iota_v : A_v \to \mathcal{M}_{d_v}(D_v)$ such that $\iota_v(\mathcal{O}_v) = \mathcal{M}_{d_v}(\Lambda_v)$ and $\iota_v(I_v^{(v)}) = x_v \mathcal{M}_{d_v}(\Lambda_v)$ with x_v the diagonal matrix $(\Pi_v, 1, \ldots, 1)$.

We first claim that $\iota(\Gamma)$ is dense in $G = \prod_{v\in T} \mathrm{SL}_{d_v}(D_v)$. By strong approximation (Theorem 1.1.2.2), $\iota(\mathcal{O}_S^1)$ is dense in $\prod_{v\in T} \mathrm{SL}_{d_v}(\Lambda_v)$ and for every $\mathfrak{p} \in T$, $\iota(\mathcal{O}_S^{(\mathfrak{p})1})$ is dense in $\prod_{v\in T,\, v\neq\mathfrak{p}} \mathrm{SL}_{d_v}(\Lambda_v) \times x_\mathfrak{p}\mathrm{SL}_{d_\mathfrak{p}}(\Lambda_\mathfrak{p})x_\mathfrak{p}^{-1}$. By Lemma 2.4.2.1, the closure of $\iota(\Gamma)$ contains $\mathrm{SL}_{d_\mathfrak{p}}(D_\mathfrak{p})$ for all $\mathfrak{p} \in T$, which proves the claim.

Now let $g \in \mathcal{O}_{S\cup T}^1$. Since $\prod_{v\in T} \mathrm{SL}_{d_v}(\Lambda_v)$ is open in G, there exists an element $\gamma \in \Gamma$ such that $\iota(g\gamma^{-1}) \in \prod_{v\in T} \mathrm{SL}_{d_v}(\Lambda_v)$. Since $g\gamma^{-1} \in \mathcal{O}_{S\cup T}^1$, this implies that $g\gamma^{-1} \in \mathcal{O}_S^1$. But Γ contains $\mathcal{O}_S^1$ by definition, so $g \in \Gamma$. This proves the lemma. □

Finally, we put together the sets of generators of the unit groups of the conjugated orders to generate the group of S-units. To obtain a bound on these generators, we relate the heights attached to the various occuring orders.

Proposition 2.4.2.3. *Let A be a central simple algebra over a number field F. Let S be a finite set of places containing the infinite places and satisfying the Eichler condition. Fix an isomorphism ι as in Definition 2.3.0.27. Let $B > 0$, and assume that for every maximal order $\mathcal{O}$ of A, the group $\mathcal{O}_S^1$ is generated by its elements of logarithmic height less than or equal to B, where the height corresponds to the pair $(\mathcal{O}, \iota)$. Let T be a finite set of places disjoint from S, and let m_T be the maximum*

of 1 *and* $N(\mathfrak{p})^{1/e_\mathfrak{p}}$ *for* $\mathfrak{p} \in T$. *Then for every maximal order* $\mathcal{O}$ *of* A *the group* $\mathcal{O}^1_{S\cup T}$ *is generated by its elements of logarithmic height less than or equal to* $B + \log m_T$, *where the height corresponds to the pair* $(\mathcal{O}, \iota)$.

PROOF. Let $\mathcal{O}$ be a maximal order. By Lemma 2.4.2.2, it suffices to compare, for every prime $\mathfrak{p}$, the height corresponding to $\mathcal{O}$ and the height corresponding to $\mathcal{O}^{(\mathfrak{p})}$. Let $\mathfrak{p}$ be a prime of F, and let $\iota_\mathfrak{p} : A_\mathfrak{p} \to \mathcal{M}_{d_\mathfrak{p}}(D_\mathfrak{p})$ be an isomorphism such that $\iota_\mathfrak{p}(\mathcal{O}) \subset \mathcal{M}_{d_\mathfrak{p}}(\Lambda_\mathfrak{p})$ and $\iota_\mathfrak{p}(\mathcal{O}^{(\mathfrak{p})}) \subset x\mathcal{M}_{d_\mathfrak{p}}(\Lambda_\mathfrak{p})x^{-1}$ where x is the diagonal matrix $(\Pi_\mathfrak{p}, 1, \dots, 1)$. Then the coefficients of an element $xMx^{-1} \in x\mathcal{M}_{d_\mathfrak{p}}(D_\mathfrak{p})x^{-1}$ can be of the form:

- c where c is a coefficient of M;
- $\Pi c \Pi^{-1}$ where c is a coefficient of M, in which case $|\Pi c \Pi^{-1}| = |c|$;
- $c\Pi^{-1}$ where c is a coefficient of M, in which case $|c\Pi^{-1}| = |c| \cdot |\Pi^{-1}| = |c| \cdot |\pi^{-1}|^{1/e_\mathfrak{p}} = |c| \cdot N(\mathfrak{p})^{1/e_\mathfrak{p}[F_\mathfrak{p}:\mathbb{Q}_p]}$;
- Πc where c is a coefficient of M, in which case $|\Pi c| = |\Pi| \cdot |c| \leq |c|$.

This gives $\|xMx^{-1}\| \leq \|M\| \cdot N(\mathfrak{p})^{1/e_\mathfrak{p}[F_\mathfrak{p}:\mathbb{Q}_p]}$ by Lemma 2.3.0.18. Let h be a logarithmic height attached to $\mathcal{O}$. In order to compute a height attached to $\mathcal{O}^{(\mathfrak{p})}$, we may choose the same embeddings as for $\mathcal{O}$ at every place except at $\mathfrak{p}$ where we can choose $x\iota x^{-1}$: call this height h′. We obtain that for all $a \in A$, $\mathrm{h}(a) \leq \mathrm{h}'(a) + \frac{1}{e_\mathfrak{p}} \log N(\mathfrak{p})$, and $\mathcal{O}_S^{(\mathfrak{p})1}$ is generated by its elements g satisfying $\mathrm{h}(g) \leq B + \log m_T$. This proves the result. □

Finally, we put everything together to derive our bound.

THEOREM 2.4.2.4. *There exist explicit functions of integer variables* $g_1(n,d)$ *and* $g_2(n,d)$ *such that the following holds. Let* F *be a number field of degree* n *and* A *a central division algebra of degree* d *over* F *with absolute discriminant* Δ_A. *Let* $\mathcal{O}$ *be a maximal order in* A, *and* S *a finite set of places of* F *containing every infinite place. Let* m_S *be the maximum of* $N(\mathfrak{p})^{1/e_\mathfrak{p}}$ *for primes* $\mathfrak{p}$ *in* S *that are not totally ramified in* A, *or* $m_S = 1$ *if* S *contains no such place. Let* q_S *be the minimum norm of a split prime in* S *if* A *is a totally definite quaternion algebra and such a prime exists, and* $q_S = 1$ *otherwise. Then the group* $\mathcal{O}^1_S$ *is generated by its elements of logarithmic height less than or equal to*

$$g_1(n,d) \log\left(\frac{\Delta_A}{|\Delta_F|}\right) + \log m_S + \tfrac{5}{2} \log q_S + g_2(n,d).$$

We can take the following values for g_1 *and* g_2:

- *If* A *is a totally definite quaternion algebra,* $g_1 = 1$ *and* $g_2 = 2\log(6) - 2\log(24)n + 4\log\max(20, 3n^{\frac{\log 3}{\log 2}})$;
- *otherwise,* $g_1 = 2C_1$ *and* $g_2 = 2C_2$ *where* C_1, C_2 *are as in Proposition 2.4.1.11.*

Overall we have $2/d \leq g_1 \leq 803/d$.

PROOF. First note that if S is a set of places containing the infinite places and R is a set of finite places that are totally ramified in A, then $\mathcal{O}^1_{S\cup R} = \mathcal{O}^1_S$, so we can ignore the totally ramified places. Next, by Proposition 2.4.2.3, it suffices

to prove the result when S is a minimal set satisfying the Eichler condition: we take $S_0 = \mathcal{V}_\infty \cup \{\mathfrak{p}\}$ with $\mathfrak{p}$ the smallest split prime in S when A is a totally definite quaternion algebra, and $S_0 = \mathcal{V}_\infty$ otherwise. For these cases, we apply Propositions 2.1.2.3 and 2.4.1.11 providing bounds on the size of generators in terms of the distance in the corresponding space, and we relate the height to the distance. In the definite case, such a bound is given by Lemma 2.3.0.26. In the indefinite case, a bound is given by Lemma 2.3.0.32: for all $g \in \mathcal{O}^1_{S_0}$ we have $\mathrm{h}(g) \leq \delta(\iota(g), 1)$. Putting the bounds together gives the result. □

4.3. The full S-unit group. Finally, we pass from the group of S-units of reduced norm 1 to the full group of S-units. We generate this group with the subgroup $\mathcal{O}^1_S$ together with preimages for the reduced norm of generators of S-unit groups of $\mathbb{Z}_F$. However, the reduced norm is not surjective so we need small generators for some subgroups of the S-unit group $\mathbb{Z}^\times_{F,S}$. We derive these bounds directly from Theorem 2.0.0.3.

Corollary 2.4.3.1. *Let F be a number field with r_2 complex places. Let $\mathbb{Z}_F$ be the ring of integers of F, and let S be a finite set of places of F containing every infinite place and every finite place with norm less than or equal to $(2/\pi)^{r_2}|\Delta_F|^{1/2}$, and let m_S be the maximum of the norms of primes in S or $m_S = 1$ if S contains no finite place. Let $s : \mathbb{Z}^\times_{F,S} \to \mathbb{F}_2^r$ be a morphism. Then the group $\Gamma = \ker s$ is generated by its elements with logarithmic height less than or equal to*

$$\frac{r+1}{2}\log|\Delta_F| + (r+1)\log m_S + (r+1)r_2\log\Big(\frac{2}{\pi}\Big).$$

Proof. If $r = 0$ this is Lenstra's theorem, so we may assume $r \geq 1$. Let $\Sigma \subset \mathbb{Z}^\times_{F,S}$ be the set of generators given by Lenstra's theorem. Let V be the image of s, which is an $\mathbb{F}_2$-vector space of dimension less than or equal to r. The image $s(\Sigma)$ is a generating set for V, so it contains a basis $s(B)$ with $B \subset \Sigma$. Every element of V is a sum of at most r elements of $s(B)$: for every element $x \in V$, there exists a subset $C(x) \subset B$ such that $x = \sum_{b\in C(x)} s(b)$. For $g \in \Sigma$, let $\gamma(g) = \prod_{b\in C(s(g))} b$.

Let $\Sigma_0 = \{g\gamma(g)^{-1} : g \in \Sigma\} \cup \{b^2 : b \in B\}$. We claim that Σ_0 is a set of generators for Γ. First, it is a subset of Γ: for every $g \in \Sigma$, $s(g\gamma(g)^{-1}) = s(g\prod_{b\in C(s(g))} b^{-1}) = s(g) - \sum_{b\in C(s(g))} s(b) = 0$ and a square is always in $\ker(s)$. Let Γ_0 be the subgroup of Γ generated by Σ_0. Consider an element $\gamma \in \Gamma$. Since Σ generates Γ, we can write $\gamma = \prod_{i=1}^k g_i$ with $g_i \in \Sigma$. We rewrite this as $\gamma = \prod_{i=1}^k g_i\gamma(g_i)^{-1}\prod_{i=1}^k \gamma(g_i) = \gamma_0\gamma_1$ with $\gamma_0 \in \Gamma_0$ and γ_1 a product of elements in B. By moving squares from γ_1 to γ_0, we can write $\gamma = \gamma_0'\gamma_1'$ with $\gamma_0' \in \Gamma_0$ and γ_1' a product of elements of B where every element appears at most once. We obtain that $0 = s(\gamma) = s(\gamma_1')$ is a sum of elements of $s(B)$, every element appearing at most once. Since $s(B)$ is a basis of V this sum is empty, so $\gamma_1' = 1$ and $\gamma = \gamma_0' \in \Gamma_0$. This proves the claim that Σ_0 generates Γ.

Finally, the elements of Σ_0 are products of at most $r+1$ elements of Σ, so the result follows from the submultiplicativity of the height. □

REMARK 2.4.3.2. When the map s is of the form $s = \prod_{\sigma \in T} s_\sigma$ with T a set of real places of F and $\mathrm{sign}(\sigma(x)) = (-1)^{s_\sigma(x)}$, we could also derive similar bounds from the theorem of Chinburg and Stover as follows. Take A a division algebra of smallest possible discriminant and degree, satisfying the Eichler condition, such that the set of real ramified places is exactly the set T. For instance, if there is an infinite place that is not in T, we can take a quaternion algebra that is either not ramified at any prime or ramified at the smallest prime of F. Then add an estimate of the height of the reduced norm in terms of the height of the element, similar to (iv) of Proposition 2.3.0.29 for Chinburg and Stover's height.

We also need to prove that a small element in $\mathbb{Z}_{F,S}^\times$ admits a small preimage in $\mathcal{O}_S^\times$. Since we not only have a bound on the size of generators of $\mathcal{O}_S^1$, but also on the diameter of a fundamental domain for this group, we can obtain such an estimate. Like in the case of bounds for the generators, we proceed in two steps: a local-global principle using the strong approximation property, and the bound for minimal sets S satisfying the Eichler condition.

PROPOSITION 2.4.3.3. *There exist explicit functions of integer variables $g_3(n,d)$ and $g_4(n,d)$ such that the following holds. Let A be a central division algebra of degree d over a number field F of degree n and let $\mathcal{O}$ be a maximal order in A. Let S be a finite set of places of F containing the infinite places. Let $x \in \mathcal{O}_S^\times$ and let $\lambda = \mathrm{nrd}(x)$. Then there exists $y \in \mathcal{O}_S^1$ such that*

$$\mathrm{h}(yx) \leq \mathrm{h}_F(\lambda) + g_3(n,d) \log\left(\frac{\Delta_A}{|\Delta_F|}\right) + g_4(n,d).$$

We can take the following values for g_3 and g_4.

- *If A is a totally definite quaternion algebra, $g_3 = \frac{1}{2}$ and $g_4 = 2\log(6) - \log(24)n + \log\max(20, 3n^{\frac{\log 3}{\log 2}})$;*
- *otherwise, $g_3 = C_1$ and $g_4 = C_2$ where C_1, C_2 are as in Proposition 2.4.1.11.*

PROOF. Note that if $v \in S$ is a place that is totally ramified in A, then for all $a \in A$ we simply have

$$\mathrm{h}_v(a) = \mathrm{h}_{F_v}(\mathrm{nrd}(a))^{1/d} \leq \mathrm{h}_{F_v}(\mathrm{nrd}(a)).$$

If S does not satisfy the Eichler condition, then we can take $y = 1$, so from here on we assume that S satisfies the Eichler condition. Let $S_0 = \mathcal{V}_\infty \cup \{\mathfrak{p}\}$ with $\mathfrak{p}$ the smallest split prime in S if A is a totally definite quaternion algebra, and $S_0 = \mathcal{V}_\infty$ otherwise. Write S as the disjoint union $S_0 \cup T$ and note that S_0 satisfies the Eichler condition.

Let $G = \prod_{v \in T} A_v^1$. By strong approximation, $\mathcal{O}_S^1$ is dense in G. Let $v \in T$, and let m_v be the diagonal matrix $(\lambda_v, 1, \ldots, 1)$. Then

$$\mathrm{nrd}(m_v) = \lambda_v \text{ and } \mathrm{h}(m) \leq \mathrm{h}_{F_v}(\lambda_v).$$

Let $m \in \prod_{v \in T} A_v^\times$ be the element with component m_v at all $v \in T$, so that $mx^{-1} \in G$. Since $H = \prod_{v \in T} \mathcal{O}_v^1$ is open in G and $\mathcal{O}_S^1$ is dense in G, there exists an element $y_1 \in$

$\mathcal{O}_S^1$ such that $y_1 \in Hmx^{-1}$, so that

$$\mathrm{h}_T(y_1 x) = \mathrm{h}_T(m) \leq \mathrm{h}_{F,T}(\lambda)$$

because multiplication by elements of H does not change the local heights.

Consider the totally definite case, where $S_0 = \mathcal{V}_\infty \cup \{\mathfrak{p}\}$, and let $v = \mathfrak{p}$. Let P_0 be the fixed point of $\mathcal{O}^\times$ in the Bruhat-Tits tree $\mathcal{T}_\mathfrak{p}$. Let g_1 be the diagonal matrix $(\pi_v^a, 1)$ where $a = v(\lambda) \bmod 2$, and let $g_2 \in \mathrm{GL}_2(\mathbb{Z}_{F_v})$ and $k \in \mathbb{Z}$ be such that $\det(\pi^k g_1 g_2) = \lambda$. Let $g = y_1 x (\pi^k g_1 g_2)^{-1}$, so that $\det(g) = 1$, and let $P = g \cdot P_0$. By the proof of Proposition 2.1.2.3, there exists $y_2 \in \mathcal{O}_{S_0}^1$ such that

$$d(y_2 \cdot P, P_0) \cdot \log q \leq R$$

with

$$R = \log(\Delta_A/|\Delta_F|) + 2\log(6) - 2\log(24)n + 2\log\max(20, 3n^{\frac{\log 3}{\log 2}}).$$

By Lemma 2.3.0.26 we have

$$\mathrm{h}_v(y_2 g) \leq \frac{1}{2} d(y_2 g \cdot P_0, P_0) \log q \leq R/2.$$

We get $\mathrm{h}_v(y_2 y_1 x) = \mathrm{h}_v(y_2 g \pi^k g_1 g_2) \leq \mathrm{h}_v(y_2 g) + \mathrm{h}_v(\pi^k g_1 g_2)$ and $\mathrm{h}_v(\pi^k g_1 g_2) \leq \mathrm{h}_{F_v}(\lambda)$. Since elements of $\mathcal{O}_{S_0}^1$ do not change the height at places of T, this proves the result in this case.

Finally consider the case where $S_0 = \mathcal{V}_\infty$. Let $G = \prod_{v \in S_0} \mathrm{SL}_{d_v}(D_v)$. For every place $v \in S_0$, let $s_v \in \{\pm 1\}$ be the sign of λ_v if v is real and $s_v = 1$ if v is complex. Let $g_1 \in G$ have as component the diagonal matrix $(s_v, 1, \ldots, 1)$ at every place $v \in S_0$. For every $v \in S_0$, let $\alpha_v \in F_v$ be a d_v-th root of $s_v \lambda_v$. Let $g = y_1 x (\alpha g_1)^{-1}$. By Proposition 2.4.1.11, there exists $y_2 \in \mathcal{O}_{S_0}^1$ such that

$$\delta(y_2 g, 1) \leq R$$

with

$$R = C_1 \log(\Delta_A/|\Delta_F|) + C_2$$

and C_1, C_2 depending only on A_∞. By Lemma 2.3.0.32 we have

$$\mathrm{h}_{S_0}(y_2 g) \leq \sqrt{\tfrac{1}{2d}} R.$$

We get $\mathrm{h}_{S_0}(y_2 y_1 x) = \mathrm{h}_{S_0}(y_2 g \alpha g_1) \leq \mathrm{h}_{S_0}(y_2 g) + \mathrm{h}_{S_0}(\alpha g_1)$ and we have $\mathrm{h}_{S_0}(\alpha g_1) \leq \mathrm{h}_{F,S_0}(\lambda)$. Since elements of $\mathcal{O}_{S_0}^1$ do not change the height at places of T, this proves the result. □

Finally, we put the pieces together to prove our bound.

THEOREM 2.4.3.4. *There exist explicit functions of integer variables $g_5(n,d)$ and $g_6(n,d)$ such that the following holds. Let F be a number field of degree n and A a central division algebra of degree d over F with absolute discriminant Δ_A. Let $\mathcal{O}$ be a maximal order in A, and S a finite set of places of F containing every infinite place and every finite place with norm less than or equal to $(2/\pi)^{r_2}|\Delta_F|^{1/2}$. Let m_S be the maximum of $N(\mathfrak{p})^{1/e_\mathfrak{p}}$ for primes $\mathfrak{p}$ in S that are not totally ramified in A, or $m_S = 1$ if S contains no such place. Let q_S be the minimum norm of a split prime in S if A is a totally definite quaternion algebra and such a prime exists, and $q_S = 1$*

otherwise. Let r be the number of real places of F that ramify in A if S satisfies the Eichler condition, and $r = n$ otherwise. Then the group $\mathcal{O}_S^\times$ is generated by its elements of logarithmic height less than or equal to

$$g_5(n,d)\log(\Delta_A) + (r+1)\log m_S + \tfrac{5}{2}\log q_S + g_6(n,d).$$

We can take the following values for g_5 and g_6:

- *If A is a totally definite quaternion algebra, $g_5 = \max(1, \frac{n+4}{8})$ and $g_6 = 2\log(6) - 2\log(24)n + 2\log\max(20, 3n^{\frac{\log 3}{\log 2}})$;*
- *otherwise, $g_5 = C_1 + \max(\frac{r+1}{d^2}, C_1)$ and $g_6 = C_2 + (r+1)r_2\log(2/\pi)$ where the constants C_1, C_2 are as in Proposition 2.4.1.11.*

Proof. We describe a generating set for $\mathcal{O}_S^\times$. The theorem then follows from Theorem 2.4.2.4, Corollary 2.4.3.1 and Proposition 2.4.3.3.

First assume that S satisfies the Eichler condition. By Eichler's norm theorem we have an exact sequence

$$1 \longrightarrow \mathcal{O}_S^1 \longrightarrow \mathcal{O}_S^\times \longrightarrow \mathbb{Z}_{F,S,A_\infty}^\times \longrightarrow 1$$

where the group $\mathbb{Z}_{F,S,A_\infty}^\times$ is the kernel of the sign map $s : \mathbb{Z}_{F,S}^\times \to \mathbb{F}_2^r$ corresponding to the ramified places. Let $\Sigma \subset \mathcal{O}_S^\times$ be a subset such that $\mathrm{nrd}(\Sigma)$ generates $\mathbb{Z}_{F,S,A_\infty}^\times$, then $\mathcal{O}_S^1 \cup \Sigma$ generates $\mathcal{O}_S^\times$.

Now assume that S does not satisfy the Eichler condition. Then A is a totally definite quaternion algebra and every place in S is ramified. For every finite place $v \in S$ and for all $x \in \mathcal{O}_S^\times$, we have $v(\mathrm{nrd}(x)) = 0$ so $x \in \Lambda_v^\times$: we can remove v from S without changing the group $\mathcal{O}_S^\times$, so we may assume $S = \mathcal{V}_\infty$. We have an exact sequence

$$1 \longrightarrow \mathcal{O}^1/\{\pm 1\} \longrightarrow \mathcal{O}^\times/\mathbb{Z}_F^\times \longrightarrow \mathbb{Z}_F^\times/(\mathbb{Z}_F^\times)^2.$$

Let G be the image of the last map. Since $\mathbb{Z}_F^\times/(\mathbb{Z}_F^\times)^2$ is an $\mathbb{F}_2$-vector space of dimension at most n, G is the kernel of a morphism $\bar{s} : \mathbb{Z}_F^\times/(\mathbb{Z}_F^\times)^2 \to \mathbb{F}_2^k$ for some $k \leq n$. Let $s : \mathbb{Z}_F^\times \to \mathbb{Z}_F^\times/(\mathbb{Z}_F^\times)^2 \to \mathbb{F}_2^k$ be the lift of $\bar{s}$ to $\mathbb{Z}_F^\times$. Let $\Sigma \subset \mathcal{O}^\times$ be a subset such that $\mathrm{nrd}(\Sigma)$ generates $\ker s$. Then $\mathcal{O}^1 \cup \mathbb{Z}_F^\times \cup \Sigma$ generates the group $\mathcal{O}^\times$. □

5. Outlook

Better bounds. As we have seen, our bounds for generators of S-unit groups $\mathcal{O}_S^\times$ apply to sets of places S depending only on F, but the factor g_1 that multiplies $\log\Delta_A$ in our bounds are worse than those of Chinburg and Stover. Both have the best asymptotic behavior: by (iv) of Proposition 2.3.0.29, $d \cdot g_1$ has to be bounded below by a constant depending only on F and S whenever $\mathbb{Z}_{F,S}^\times$ is infinite. It would be interesting to know if we can obtain bounds as good as in [**CS12**] for sets S depending only on F, possibly assuming the Ramanujan conjecture. The current bounds are too large to be practical, improving them could lead to an algorithm worth implementing.

The number of generators. In an algorithmic context, we need to know the size but also the number of generators of the groups $\mathcal{O}_S^1$ that we want to compute. Gelander proved that $\mathcal{O}^1$ has a generating set with at most $O(\Delta_A)$ generators, and we proved that there is a generating set with generators of size $O(\log \Delta_A)$. First, it would be nice to have a generating set satisfying both conditions at the same time, but that would still be exponentially many generators! In general we cannot do better, as the case of Fuchsian groups shows. On the other hand, Sharma and Venkataramana [**SV04**] showed that when A is not a division algebra, $\mathcal{O}^1$ admits a finite index subgroup generated by only three elements. In general it would be very desirable to know what the smallest number of generators for $\mathcal{O}_S^1$ is, and more precisely what the smallest *total size* of a generating set is.

CHAPTER 3

Computing unit groups

In this chapter, we present algorithms for computing unit groups of orders in division algebras. The input will be the maximal order, specified in bits by its multiplication table over $\mathbb{Z}$. By *computing* a group $\Gamma \subset A^\times$, we mean computing a finitely presented group $\mathsf{\Gamma}$ together with computable isomorphisms $\phi : \mathsf{\Gamma} \to \Gamma$ and $\psi : \Gamma \to \mathsf{\Gamma}$ that are inverse of each other, assuming of course that Γ is finitely presented to begin with.

We review some of the literature on this subject. Grunewald and Segal describe a general strategy for computing an arbitrary arithmetic group [**GS80**], but it is not practical and they do not analyse its complexity. Most of the algorithms that have been implemented only consider matrix rings: $\mathcal{M}_d(\mathbb{Z}_F)^\times = \mathrm{GL}_d(\mathbb{Z}_F)$. Over $\mathbb{Q}$, generators for $\mathrm{SL}_d(\mathbb{Z})$ are given by the elementary matrices. Computing a fundamental domain is much harder, see [**AGM11**] and the references therein. For F an imaginary quadratic field, the group $\mathrm{SL}_2(\mathbb{Z}_F)$ is called a *Bianchi group*. Bianchi groups have been intensively studied, going back to Swan [**Swa71**]; the survey [**Şen14**] is a good reference. The case of $\mathrm{GL}_2(\mathbb{Z}_F)$ for some other number fields is studied via Voronoï-type algorithms by Gunnells, Yasaki and Hajir in [**GY08, GHY13, GY13**]. In higher rank ($d \geq 3$), Gunnells et al. treat $\mathrm{SL}_d(\mathbb{Z}_F)$ for imaginary quadratic fields F in [**GGH$^+$13**]. Regarding nonsplit algebras, much less has been done. In the case of totally definite quaternion algebras, the group of units of reduced norm 1 is finite. Voight describes an efficient algorithm computing Dirichlet domains in the Fuchsian case (quaternion algebras A such that $A \otimes \mathbb{R} \cong \mathcal{M}_2(\mathbb{R}) \times \mathbb{H}^r$) in [**Voi09**]. It appears that the only work in the general case is due to Coulangeon and Nebe [**CN13**], again using Voronoï-type methods. Only a few works prove complexity bounds, and there seems to be only two such works. The first one is in Swan's paper [**Swa71**]: at the end of Section 8, he sketches a complexity bound by using explicit diophantine approximation to estimate which elements of the Bianchi group can contribute to the particular fundamental domain he is considering. Working out the details gives an complexity estimate in $\Delta_F^{O(1)}$, the same order of magnitude as our bound. The second one is in [**Jah10**, Section 4]: in the special case of certain unit groups in division quaternion algebras over $\mathbb{Q}$, Jahangiri presents a bound that he attributes to Chalk and that proves a complexity estimate of the form $\exp(O(\Delta_A))$. Our bound is exponentially better.

The chapter is organised as follows. In Section 1 we present an algorithm that computes the group $\mathcal{O}^1$ of units of reduced norm 1 in a a maximal order of a division algebra over $\mathbb{Q}$, and we prove that the algorithm runs in time at

most $\exp(O(d\log\Delta_A)+O_N(\log\log\Delta_A))$. In Section 2, we present an efficient probabilistic algorithm that computes the group $\mathcal{O}^1$ in the Kleinian case: when A is a quaternion algebra such that $A\otimes\mathbb{R}\cong\mathcal{M}_2(\mathbb{C})\times\mathbb{H}^r$. Experimental evidence suggests that it runs in time $(\Delta_A/\Delta_F)^{2+o(1)}$ when the degree of the base field is fixed.

1. Algorithms with proved complexity

The main result of this section is an enumeration algorithm *with proved complexity* for computing unit groups of maximal orders in division algebras over $\mathbb{Q}$. It relies on the results of Chapter 2 giving bounds on the diameter of the Dirichlet domains of such unit groups. In addition, we improve on the naive enumeration algorithm with an enumeration strategy using multiple quadratic forms. This saves a large power in the complexity and could be more suitable for parallelization.

1.1. Enumeration algorithms. In this section we describe a general-purpose algorithm for central simple algebras, that is useful for solving various multiplicative problems. The goal is to use Proposition 2.4.1.11 to compute unit groups, but also to solve the principal ideal problem and norm equations (Section 1). All of these problems reduce to finding elements with a given norm in a given lattice. To solve this problem, we scale the element $x\in A^\times$ that we are looking for so that the new element $p(x)$ has norm 1, and we search in a ball for the quadratic form T_2 with radius determined by the size of the Dirichlet domain for $\mathcal{O}^1$. This quickly provides an algorithm (Algorithm 3.1.1.3), but we also describe a way to improve upon this algorithm as follows. We note that enumerating every vector in a large ball for T_2 and then selecting only the elements having a given norm is wasteful: the level sets of the reduced norm are subvarieties of strictly positive codimension in A. In addition, the elements in A^1 that are close to a given element of $(A\otimes\mathbb{R})^1$ are small for a twisted version of T_2. So we compute a covering of the symmetric space attached to A^1 with small balls, and we enumerate short vectors for the corresponding twisted T_2 quadratic forms. This provides a substantial improvement in the complexity, suppressing a power n, where n is the degree of the base field.

We start by defining the scaling map p that projects onto elements of reduced norm 1. Note that this does not preserve $A^\times$.

Definition 3.1.1.1. Let A be a central simple algebra of degree d over a number field F of degree n. Let $\iota=(\iota_v)_{v\in\mathcal{V}_\infty}$ be a choice of isomorphism $\iota: A\otimes_{\mathbb{Q}}\mathbb{R}\to\prod_{v\in\mathcal{V}_\infty}\mathcal{M}_{d_v}(D_v)$ extending the embeddings $v\in\mathcal{V}_\infty$. For all $v\in\mathcal{V}_\infty$ we define a surjective homomorphism

$$p_v:\mathrm{GL}_{d_v}(D_v)\to\mathrm{SL}_{d_v}(D_v)$$

by $x=d\cdot t\cdot p_v(x)$ where $t>0$ and d is a diagonal matrix $(u,1,\dots,1)$ with $u\in F_v^\times$, $|u|=1$, so that $t=|\mathrm{nrd}(x)|^{1/d}$ and $u\cdot|\mathrm{nrd}(x)|=\mathrm{nrd}(x)$. This defines componentwise a surjective homomorphism

$$p:\prod_{v\in\mathcal{V}_\infty}\mathrm{GL}_{d_v}(D_v)\to\prod_{v\in\mathcal{V}_\infty}\mathrm{SL}_{d_v}(D_v).$$

Recall from Definition 2.3.0.31 that we have defined a symmetric subadditive map

$$\rho : \prod_{v\in\mathcal{V}_\infty} \mathrm{SL}_{d_v}(D_v) \to \mathbb{R}_{>0}$$

such that for all $g = (g_v) \in \prod_{v\in\mathcal{V}_\infty} \mathrm{SL}_{d_v}(D_v)$,

$$\rho(g) = \sum_{v\in\mathcal{V}_\infty} [F_v : \mathbb{R}] \cdot \log \max(\|g_v\|, \|g_v^{-1}\|).$$

We extend ρ to $A^\times$ by letting $\rho(x) = \rho(p(\iota(x)))$ for all $x \in A^\times$. Consider a lattice L in A, an element $\lambda \in F^\times$ and a bound $R > 0$. We define the set

$$L_{\lambda,R} = \{x \in L \mid \mathrm{nrd}(x) = \lambda \text{ and } \rho(x) \leq R\}.$$

LEMMA 3.1.1.2. *Use the same notations as in Definition 3.1.1.1. Then the set $L_{\lambda,R}$ is finite, and for all $x \in L_{\lambda,R}$ we have*

$$\|\iota_v(x)\|_2 \leq \sqrt{d} \cdot |\lambda_v|^{\frac{1}{d}} \exp(R).$$

PROOF. Since L is a lattice, the second assertion implies the first one. Let $v \in \mathcal{V}_\infty$ and $x \in L_{\lambda,R}$, and write $x_v = \iota_v(x)$. We have

$$\|x_v\| = \||\mathrm{nrd}(x_v)|^{1/d} \cdot p_v(x_v)\| \leq |\lambda_v|^{1/d} \exp(\rho(x)),$$

and the lemma follows from Lemma 2.3.0.35: $\|x_v\|_2 \leq \sqrt{d} \cdot \|x_v\|$. □

We are interested in the following task: given a basis of a lattice L in A, an element $\lambda \in F^\times$ and a bound $R > 0$, compute the set $L_{\lambda,R}$. Note that this is a well-defined algorithmic task since the set $L_{\lambda,R}$ is finite. From Lemma 3.1.1.2, we obtain the following straightforward algorithm. We will describe a better algorithm, but we still analyse the complexity of the naive one to compare the better algorithm with the naive one.

ALGORITHM 3.1.1.3 (Naive enumeration).

Input: a lattice L in a central simple algebra A of degree d over a number field F, with a quadratic form T_2 corresponding to an embedding ι, an element $\lambda \in F^\times$ and a bound $R > 0$.

Output: the set $L_{\lambda,R}$.

1: $B \leftarrow \sqrt{d}\exp(R)$
2: $y \leftarrow |\lambda|^{1/d} \in F \otimes_{\mathbb{Q}} \mathbb{R}$
3: $E \leftarrow \emptyset$
4: **for all** $x \in L$ such that $T_2(y^{-1}x) \leq B^2$ **do**
5: **if** $\mathrm{nrd}(x) = \lambda$ and $\rho(x) \leq R$ **then**
6: add x to E
7: **end if**
8: **end for**
9: **return** E

PROPOSITION 3.1.1.4. *Given a lattice L in a central simple algebra A of degree d over a number field F of degree n, an element $\lambda \in F^\times$ and a bound $R > 0$,*

Algorithm 3.1.1.3 returns the set $L_{\lambda,R}$. If A is a division algebra, the algorithm terminates in time at most

$$O_N\left(1+\frac{\exp(NR)|N_{F/\mathbb{Q}}(\lambda)|^d}{N_{A/\mathbb{Q}}(L)}\right)$$

times a polynomial in the size of the input and in R, where $N = nd^2 = \dim_{\mathbb{Q}} A$ and the implicit constant depends only on N.

Proof. If $x \in L_{\lambda,R}$ then

$$T_2(yx) = \sum_{v\in\mathcal{V}_\infty} [F_v : \mathbb{R}]|\lambda_v|^{-2/d}\|\iota_v(x)\|_2^2 \leq B^2$$

by Lemma 3.1.1.2, so x is enumerated in the loop. This proves the correctness of the algorithm. The running time, up to a polynomial in the size of the input and in R, is the time spent in the enumeration. Let x_0 be a shortest vector of the lattice L equipped with the quadratic form $x \mapsto T_2(y^{-1}x)$. If A is a division algebra, by Lemma 2.3.0.34 we have

$$T_2(y^{-1}x_0)^{N/2} \geq (nd)^{N/2}N_{A_\infty/\mathbb{R}}(y^{-1}x_0) \geq (nd)^{N/2}|N_{F/\mathbb{Q}}(\lambda)|^{-d}N_{A/\mathbb{Q}}(L)$$

since $x_0 \in A^\times$, and the proposition follows from Theorem 1.2.1.3. □

Note that the hypothesis that A is a division algebra is necessary here: when A is not a division algebra, there are sequences of lattices with the same norm, but with the length of a shortest nonzero vector tending to 0.

To realize our strategy for the faster algorithm, we need to cover the symmetric space with balls of controlled radius. The natural idea is to use the exponential map. The following lemma gives a control on the size of the image of a ball under exponentiation.

Lemma 3.1.1.5. *Let F be an Archimedean local field, $d \geq 1$ an integer, D is a central division algebra over F and $A = \mathcal{M}_d(D)$. Let $X, Y \in A$. Then*

$$\|\exp(-Y)\exp(X)\| \leq 1 + \exp(\|X\|)\exp(\|Y\|)\|X - Y\|.$$

Proof. First note that since $\|\cdot\|$ is a submultiplicative norm, for all $Z \in A$ we have $\|\exp(Z)\| \leq \exp(\|Z\|)$. Let $f(t) = \exp(-tY)\exp(tX)$, so that $f(0) = 1$ and $f(1) = \exp(-Y)\exp(X)$. Then $f'(t) = \exp(-tY)(X-Y)\exp(tX)$, so $\|f'(t)\| \leq \exp(\|X\|)\exp(\|Y\|)\|X - Y\|$. The result now follows from the mean value theorem. □

This second lemma describes a sufficiently large set in the Lie algebra to cover the portion of the symmetric space that we need.

Lemma 3.1.1.6. *Let F be an Archimedean local field, $d \geq 1$ an integer, D is a central division algebra over F and $A = \mathcal{M}_d(D)$. Let $G = \mathrm{SL}_d(D)$, $K = \mathrm{SU}_d(D)$ and $\mathfrak{P}$ be the space of trace zero hermitian matrices. Let $g \in G$. Let $X \in \mathfrak{P}$ and $k \in K$ be such that $g = \exp(X)k$ and let $g_t = \exp(tX)k$ for all $t \in \mathbb{R}_{\geq 0}$. Then for all $t \geq 0$ we have*

$$\log\max(\|g_t\|, \|g_t^{-1}\|) = t\|X\|.$$

PROOF. The existence of $X \in \mathfrak{P}$ and $k \in K$ such that $g = \exp(X)k$ is the polar decomposition 2.3. Since X is hermitian, there exists $k' \in K$ such that $Y = k'Xk'^{-1}$ is a diagonal matrix with real coefficients $(a_i)_{1\leq i\leq d}$. Then $h_t = \exp(tY) = k'g_t(k'k)^{-1}$ is diagonal with real coefficients $(\exp(ta_i))_{1\leq i\leq d}$. On one hand we have

$$t\|X\| = t\|Y\| = t\max_i |a_i| = \max\Big(\max_i(ta_i), \max_i(-ta_i)\Big),$$

and on the other hand we have $\|g_t\| = \|h_t\| = \max_i \exp(ta_i)$ and similarly we have $\|g_t^{-1}\| = \max_i \exp(-ta_i)$. Comparing these expressions gives the lemma. □

We have all we need to describe an ball covering algorithm in the case of one simple factor.

SUBALGORITHM 3.1.1.7 (Ball covering, one simple factor).

Input: an integer $d \geq 1$, a division algebra D over $\mathbb{R}$, and two strictly positive numbers $R > \alpha$.

Output: a finite subset E of $G = \mathrm{SL}_d(D)$ s.t. $B_R \subset \bigcup_{g\in E} B_\alpha(g)$.

1: Let $\mathfrak{P} \subset \mathcal{M}_d(D)$ be the subspace of trace zero hermitian matrices.
2: $N \leftarrow \dim_{\mathbb{R}} \mathfrak{P}$
3: $b_1, \ldots, b_N \leftarrow$ an orthogonal basis of $\mathfrak{P}$ with respect to $\|\cdot\|_2$
4: $\varepsilon \leftarrow \alpha\exp(-2R-1)$
5: $s \leftarrow 2\varepsilon/\sqrt{N}$
6: $\Lambda \leftarrow$ the lattice $\bigoplus_{i=1}^N \mathbb{Z}sb_i$
7: $E \leftarrow \emptyset$
8: **for all** $X \in \Lambda$ such that $\|X\|_2 \leq \sqrt{d}R + \varepsilon$ **do**
9: **if** $\|X\| \leq R + \varepsilon$ **then**
10: add $\exp(X)$ to E
11: **end if**
12: **end for**
13: **return** E

PROPOSITION 3.1.1.8. *Given an integer $d \geq 1$, a division algebra D over $\mathbb{R}$, and two strictly positive numbers $R > \alpha$, Subalgorithm 3.1.1.7 returns a finite subset E of $G = \mathrm{SL}_d(D)$ such that $B_R \subset \bigcup_{g\in E} B_\alpha(g)$, where balls are expressed with respect to δ. The algorithm terminates in time at most*

$$\exp(2NR - N\log\alpha + O_d(\log R))$$

where $N = \dim_{\mathbb{R}} \mathfrak{P}$ and $\mathfrak{P} \subset \mathcal{M}_d(D)$ is the subspace of trace zero hermitian matrices.

PROOF. Let $h \in B_R$. By Lemma 3.1.1.6, there exists $Y \in \mathfrak{P}$ and $k \in K$ such that $h = \exp(Y)k$ and $\|Y\| \leq R$. By rounding the coordinates, there exists $X \in \Lambda$ such that $\|X - Y\|_2 \leq s\sqrt{N}/2 = \varepsilon$. We have $\|X\| \leq \|Y\| + \|X - Y\| \leq R + \varepsilon$, and $\|X\|_2 \leq \|Y\|_2 + \varepsilon \leq \sqrt{d}R + \varepsilon$, so X is enumerated in Step 8 and $g = \exp(X) \in E$.

By Lemma 3.1.1.5 we have

$$\begin{aligned}\delta(g,h) &= \delta(\exp(X),\exp(Y))\\ &\leq \log\bigl(1+\exp(\|X\|)\exp(\|Y\|)\|X-Y\|\bigr)\\ &\leq \exp(\|X\|)\exp(\|Y\|)\|X-Y\|\\ &\leq \exp(2R+\varepsilon)\varepsilon\\ &\leq \alpha\exp(\varepsilon-1)\\ &\leq \alpha \text{ since } \varepsilon=\exp(\log\alpha-1-2R)\leq\exp(-R)\leq 1.\end{aligned}$$

We obtain $h\in B_\alpha(g)$ with $g\in E$ as claimed.

The running time, up to a polynomial in the size of the input and in R, is the time spent in the enumeration. The shortest vectors of the lattice Λ have norm s, so by Theorem 1.2.1.3, the running time is bounded by

$$O_d\left(1+\left(\frac{\sqrt{d}R+\varepsilon}{s}\right)^N\right)=O_d\left(\left(\frac{R}{s}\right)^N\right),$$

times a polynomial in the size of the input and in R. We have $R/s=e\sqrt{N}/2\exp(2R-\log\alpha+\log R)$, so the running time is bounded by

$$\exp(2NR-N\log\alpha+O_d(\log R))$$

as claimed. □

The general ball covering algorithm applies the previous one on each simple factor.

SUBALGORITHM 3.1.1.9 (Ball covering, general case).

Input: a real semisimple algebra $A=\prod_{i=1}^n\mathcal{M}_{d/e_i}(D_i)$ with D_i a central division algebra of degree $e_i\mid d$ over $F_i\supset\mathbb{R}$ and two strictly positive numbers $R>\alpha$.

Output: a finite subset E of $G=\prod_{i=1}^n\mathrm{SL}_{d/e_i}(D_i)$ s.t. $B_R\subset\bigcup_{g\in E}B_\alpha(g)$.

1: $E\leftarrow\emptyset$
2: **for all** $(t_1,\dots,t_n)\in\mathbb{Z}_{\geq 1}$ such that $t_1+\cdots+t_n\leq R+n$ **do**
3: **for** $i=1$ to n **do**
4: $E_i\leftarrow$ `BallCoverSimple`$(d/e_i,\ D_i,\ t_i/[F_i:\mathbb{R}],\ \alpha/(n[F_i:\mathbb{R}]))$ (Subalgorithm 3.1.1.7)
5: **end for**
6: **for all** $g=(g_1,\dots,g_n)\in E_1\times\cdots\times E_n$ **do**
7: add g to E
8: **end for**
9: **end for**
10: **return** E

PROPOSITION 3.1.1.10. *Given a real semisimple algebra $A=\prod_{i=1}^n\mathcal{M}_{d/e_i}(D_i)$ with D_i a central division algebra of degree $e_i\mid d$ over $F_i\supset\mathbb{R}$ and two strictly positive numbers $R>\alpha$, Subalgorithm 3.1.1.9 returns a finite subset E of $G=\prod_{i=1}^n\mathrm{SL}_{d/e_i}(D_i)$ such that $B_R\subset\bigcup_{g\in E}B_\alpha(g)$. The algorithm terminates in time at*

most

$$\exp(MR - M\log\alpha + O_{n,d}(\log R)),$$

where M is defined as follows:

- *if one of the F_i is real with $e_i = 1$, $M = d^2 + d - 2$;*
- *otherwise, if one of the F_i is complex, $M = d^2 - 1$;*
- *otherwise, $M = d^2 - d - 2$.*

PROOF. Let $h = (h_i) \in B_R \subset G$. For all i, let $t_i = \left\lceil [F_i : \mathbb{R}]\rho(h_i) \right\rceil \leq [F_i : \mathbb{R}]\rho(h_i) + 1$. We have $t_1 + \cdots + t_n \leq \sum_{i=1}^n [F_i : \mathbb{R}]\rho(h_i) + n \leq R + n$, so the n-uple $(t_1, \ldots, t_n)$ is enumerated at some iteration of Step 2. By Proposition 3.1.1.8 and Step 4, since $\rho(g_i) \leq t_i/[F_i : \mathbb{R}]$, for all i there exists $g_i \in E_i$ such that $\delta(g_i, h_i) \leq \alpha/[F_i : \mathbb{R}]$. Let $g = (g_i) \in G$, then we have $g \in E$ and $\delta(g, h) = \sum_{i=1}^n [F_i : \mathbb{R}]\delta(g_i, h_i) \leq \alpha$. We obtain $h \in B_\alpha(g)$ with $g \in E$ as claimed.

For all i, let $M_i = 2\dim_{\mathbb{R}} \mathfrak{P}_i/[F_i : \mathbb{R}]$ where $\mathfrak{P}_i \subset \mathcal{M}_{d/e_i}(D_i)$ is the subspace of trace zero hermitian matrices, so that $M = \max_i M_i$. By Proposition 3.1.1.8, the running time of Step 4 is bounded by

$$\exp(M_i t_i - M_i \log\alpha + O_{n,d}(\log t_i)).$$

As a consequence, $\#E_i$ is bounded by the same quantity, so the total running time of all the loops starting at Step 6 is bounded by

$$\begin{aligned}
\sum_{t_1+\cdots+t_n\leq R+n} \prod_{i=1}^n \#E_i &\leq \sum_{t_1+\cdots+t_n\leq R+n} \prod_{i=1}^n \exp(M_i t_i - M_i\log\alpha + O_{n,d}(\log t_i)) \\
&\leq R^{O_{n,d}(1)} \sum_{t_1+\cdots+t_n\leq R+n} \exp(M\textstyle\sum_{i=1}^n t_i - M\log\alpha) \\
&\leq R^{O_{n,d}(1)} \sum_{t_1+\cdots+t_n\leq R+n} \exp(M(R+n) - M\log\alpha) \\
&\leq \exp(MR - M\log\alpha + O_{n,d}(\log R)) \sum_{t_1+\cdots+t_n\leq R+n} 1 \\
&\leq \exp(MR - M\log\alpha + O_{n,d}(\log R))(R+n)^n \\
&\leq \exp(MR - M\log\alpha + O_{n,d}(\log R)).
\end{aligned}$$

Since the total time of all iterations of Step 4 is also bounded by the same quantity, this proves the Proposition. □

REMARK 3.1.1.11. It suffices to enumerate only the n-uples $(t_1, \ldots, t_n)$ such that $R + n - 1 \leq t_1 + \cdots + t_n \leq R + n$ (otherwise we could increase one of the t_i), but that does not change the complexity of the algorithm.

We can now realize our strategy using multiple twisted T_2 quadratic forms.

ALGORITHM 3.1.1.12 (Multiple quadratic forms enumeration).

Input: a lattice L in a central simple algebra A of degree d over a number field F, with a quadratic form T_2 corresponding to an embedding ι, an element $\lambda \in F^\times$ and a bound $R > 0$.

Output: the set $L_{\lambda,R}$.

1: **if** $R \leq 1$ **then**
2: **return** `NaiveEnum`(L, λ, R) (Algorithm 3.1.1.3)
3: **end if**
4: $C \leftarrow$ `BallCoverGeneral`$(\iota(A \otimes_{\mathbb{Q}} \mathbb{R}), R, 1)$ (Subalgorithm 3.1.1.9)
5: $y \leftarrow |\lambda|^{1/d} \in F \otimes_{\mathbb{Q}} \mathbb{R}$
6: $B \leftarrow nd \exp(2)$
7: $E \leftarrow \emptyset$
8: **for all** $g \in C$ **do**
9: **for all** $x \in L$ such that $T_2(xy^{-1}g^{-1}) \leq B$ **do**
10: **if** $\mathrm{nrd}(x) = \lambda$ and $\rho(x) \leq R$ **then**
11: add x to E
12: **end if**
13: **end for**
14: **end for**
15: **return** E

PROPOSITION 3.1.1.13. *Given a lattice L in a central simple algebra A of degree d over a number field F of degree n, with a quadratic form T_2 corresponding to an embedding ι, an element $\lambda \in F^\times$ and a bound $R > 0$, Algorithm 3.1.1.12 returns the set $L_{\lambda,R}$. If A is a division algebra, the algorithm terminates in time at most*

$$\frac{|N_{F/\mathbb{Q}}(\lambda)|^d}{N_{A/\mathbb{Q}}(L)} \exp(MR + O_N(\log R)),$$

times a polynomial in the size of the input, where $N = \dim_{\mathbb{Q}} A = nd^2$, and where M is defined as follows:

- *if F has at least one real place that splits in A, $M = d^2 + d - 2$;*
- *otherwise, if F is not totally real, $M = d^2 - 1$;*
- *otherwise, $M = d^2 - d - 2$.*

PROOF. If $x \in L_{\lambda,R}$, then $p(x) \in B_R$, so by Proposition 3.1.1.10 and Step 4 there exists $g \in E$ such that $\delta(g, p(x)) \leq 1$. By Lemma 2.3.0.32, this implies $\mathrm{H}(p(x)g^{-1}) \leq \exp(1)$, so by Lemma 2.3.0.36 we have $T_2(p(x)g^{-1}) \leq nd \exp(2)$. Since $T_2(p(x)g^{-1}) = T_2(xy^{-1}g^{-1})$ where y is defined is Step 5, the element x is enumerated by some iteration of Step 9, which proves the correctness of the algorithm.

By Proposition 3.1.1.10, Step 4 takes time at most

$$\exp(MR + O_N(\log R)).$$

Therefore, $\#E$ is also bounded by the same quantity. If A is a division algebra, as in the proof of Proposition 3.1.1.4 we have

$$T_2(y^{-1}x_0)^{N/2} \geq (nd)^{N/2} |N_{F/\mathbb{Q}}(\lambda)|^{-d} N_{A/\mathbb{Q}}(L),$$

so by Theorem 1.2.1.3 each iteration of the loop starting at Step 8 takes time at most

$$O_N\left(\frac{|N_{F/\mathbb{Q}}(\lambda)|^d}{N_{A/\mathbb{Q}}(L)}\right).$$

The total running time is therefore bounded by

$$O_N\left(\frac{|N_{F/\mathbb{Q}}(\lambda)|^d}{N_{A/\mathbb{Q}}(L)}\#E\right) \leq \frac{|N_{F/\mathbb{Q}}(\lambda)|^d}{N_{A/\mathbb{Q}}(L)}\exp(MR + O_N(\log R))$$

as claimed. □

This should be compared with the naive Algorithm 3.1.1.3 for which the exponential term in the complexity was $\exp(NR)$. We have $N \sim nd^2$ and $M \sim d^2$, a substantial improvement. However, there are constants hidden in the $O_N(\log R)$, so we do not know in what range Algorithm 3.1.1.12 is faster than Algorithm 3.1.1.3.

1.2. Unit groups. We return to the main subject of this chapter: computation of unit groups. We start with a direct application of Section 1.1 and Chapter 2 providing an algorithm to compute a set of generators for the S-unit group $\mathcal{O}_S^1$.

ALGORITHM 3.1.2.1 (`Norm1SUnitGroup`).

Input: a maximal order $\mathcal{O}$ in a central division algebra A of degree d over a number field F, that is not a totally definite quaternion algebra, and a finite set S of places of F containing $\mathcal{V}_\infty$.

Output: a set of generators for the group $\mathcal{O}_S^1$.

1: Choose an embedding ι and the corresponding quadratic form T_2
2: $R \leftarrow$ the bound of Proposition 2.4.1.11 on the size of generators for $\mathcal{O}^1$
3: $\Sigma \leftarrow$ `MultipleQuadraticFormsEnum`($\mathcal{O}$, 1, R, ι) (Algorithm 3.1.1.12)
4: **for all** $\mathfrak{p} \in S_f$ **do**
5: $\quad I \leftarrow$ integral right $\mathcal{O}$-ideal of norm $\mathfrak{p}$
6: $\quad \mathcal{O}' \leftarrow \mathcal{O}_l(I)$
7: $\quad \Sigma \leftarrow \Sigma \cup$ `MultipleQuadraticFormsEnum`($\mathcal{O}'$, 1, R, ι) (Algorithm 3.1.1.12)
8: **end for**
9: **return** Σ, ι

COROLLARY 3.1.2.2. *Given a maximal order $\mathcal{O}$ in a central division algebra A of degree d over a number field F, that is not a totally definite quaternion algebra, and a finite set S of places of F containing $\mathcal{V}_\infty$, Algorithm 3.1.2.1 returns a set of generators for the group $\mathcal{O}_S^1$. The algorithm terminates in time at most*

$$\exp\Big(O(d\log\Delta_A + \log\#S + \log\log m_S) + O_N(\log\log\Delta_A)\Big),$$

where m_S is the maximum of $N(\mathfrak{p})$ for $\mathfrak{p} \in S$ or $m_S = 1$ if S contains no finite place.

PROOF. The correctness of the algorithm is a direct consequence of Propositions 2.4.2.3, 2.4.1.11 and 3.1.1.13. Since the algorithm consists in at most $\#S$ iterations of Algorithm 3.1.1.12 with size of the input multiplied at most by $\log m_S$, the claim on the running time directly follows from Proposition 3.1.1.13. □

REMARK 3.1.2.3. If we had used the naive enumeration algorithm, directly with the bound of Theorem 2.4.2.4 instead of using Proposition 2.4.2.3, the main term in the complexity would have been

$$\exp\Big(O(nd\log\Delta_A + \log m_S)\Big),$$

instead of

$$\exp\Big(O(d\log\Delta_A+\log\#S+\log\log m_S)\Big).$$

Restricting to units again, we need to construct computable isomorphisms with a finitely presented group. The presentation will be provided by Lemma 1.2.2.3, and the isomorphism from the presentation to $\mathcal{O}^1$ is simply evaluation of words. The other direction is more interesting: given an element $g\in\Gamma$, we need to write it as a word of the generators. Recall the definition of the Dirichlet domain for a subgroup $\Gamma\subset G$ where $G=\prod_{v\in\mathcal{V}_\infty}\mathrm{SL}_{d_v}(D_v)$:

$$D=\{g\in G\mid \delta(g,1)\leq\delta(\gamma g,1)\text{ for all }\gamma\in\Gamma\}$$

By definition a Dirichlet domain gives a simple algorithm to compute the word: repeatedly multiply the element by appropriate generators to reduce the distance to 1. We will describe another algorithm for which we can prove a better complexity, but we will need this greedy algorithm to bootstrap the other one.

Subalgorithm 3.1.2.4 (Greedy reduction algorithm).

Input: an embedding ι and a set Σ of generators of $\mathcal{O}^1$ from Algorithm 3.1.2.1, and an element $g\in G=\prod_{v\in\mathcal{V}_\infty}\mathrm{SL}_{d_v}(D_v)$.

Output: a product γ of elements of Σ such that $\iota(\gamma)g$ is in the Dirichlet domain D for $\Gamma=\iota(\mathcal{O}^1)$.

1: **for** $\gamma\in\Sigma$ **do**
2: $\quad h\leftarrow\iota(\gamma)g$
3: $\quad$ **if** $\delta(h,1)<\delta(g,1)$ **then**
4: $\quad\quad$ **return** $\gamma\cdot$ `GreedyReduce`$(\iota,\ \Sigma,\ h)$
5: $\quad$ **end if**
6: **end for**
7: **return** 1

Proposition 3.1.2.5. *Given an embedding ι and a set Σ of generators of $\mathcal{O}^1$ from Algorithm 3.1.2.1, and an element $g\in G=\prod_{v\in\mathcal{V}_\infty}\mathrm{SL}_{d_v}(D_v)$, Subalgorithm 3.1.2.4 returns a product γ of elements of Σ such that $\iota(\gamma)g$ is in the Dirichlet domain D for $\Gamma=\iota(\mathcal{O}^1)$. The algorithm terminates in time at most*

$$\exp\Big(O(d\log\Delta_A+d^2\delta(g,1))+O_N(\log\log\Delta_A+\log\delta(g,1))\Big).$$

Proof. The cardinality of the set $\#\Sigma$ is bounded by the running time of Algorithm 3.1.2.1, that is

$$\exp\Big(O(d\log\Delta_A)+O_N(\log\log\Delta_A)\Big).$$

During the recursive calls of the algorithm, the distance $\delta(h,1)$ is strictly decreasing, so the elements h are all distinct, so the elements $\gamma\in\mathcal{O}^1$ such that $h=\iota(\gamma)g$ are also all distinct, and we have $\rho(\gamma)\leq\delta(h,1)+\delta(g,1)\leq 2\delta(g,1)$. So the number of recursive calls is bounded by the number of elements $\gamma\in\mathcal{O}^1$ such that $\rho(\gamma)\leq 2\delta(g,1)$. This number is bounded by the running time of Algorithm 3.1.1.12 that enumerates them, which is

$$\exp\Big(O(d^2\delta(g,1))+O_N(\log\delta(g,1))\Big).$$

This proves the claim on the running time. The correctness of the algorithm is clear by tracking the multiplications. □

The running time estimate of Proposition 3.1.2.5 is probably very pessimistic, but it seems hard to obtain a better bound. To get a good complexity bound, we use another algorithm where we have a better control of the reduction steps. It is an algorithmic version of the well-known fact that for a cocompact group, the word metric and the Riemannian metric are Lipschitz-equivalent [**LMR00**, Proposition 3.2].

SUBALGORITHM 3.1.2.6 (Reduction algorithm).

Input: an embedding ι and a set Σ of generators of $\mathcal{O}^1$ from Algorithm 3.1.2.1, and an element $g \in G = \prod_{v\in\mathcal{V}_\infty} \mathrm{SL}_{d_v}(D_v)$.

Output: a product γ of elements of Σ such that $\iota(\gamma)g$ is in the Dirichlet domain D for $\Gamma = \iota(\mathcal{O}^1)$.

1: let $X \in \prod_{v\in\mathcal{V}_\infty} \mathcal{M}_{d_v}(D_v)$ and $k \in \prod_{v\in\mathcal{V}_\infty} \mathrm{SU}_{d_v}(D_v)$ be such that each X_v is Hermitian with trace zero and $g = \exp(X)k$
2: $R \leftarrow$ the bound of Proposition 2.4.1.11 on the size of D
3: $m \leftarrow \lceil \delta(g,1)/R \rceil$
4: **for** $i = 0$ to $m-1$ **do**
5: $\quad t_i \leftarrow Ri/\delta(g,1)$
6: $\quad h_i \leftarrow \exp(t_i X)k$
7: **end for**
8: $t_m \leftarrow 1$
9: $h_m \leftarrow g$
10: $\gamma \leftarrow 1$
11: **for** $i = 1$ to m **do**
12: $\quad \gamma_i \leftarrow$ `GreedyReduce`$(\iota, \Sigma, \iota(\gamma)h_i)$
13: $\quad \gamma \leftarrow \gamma_i\gamma$
14: **end for**
15: **return** γ

PROPOSITION 3.1.2.7. *Given an embedding ι and a set Σ of generators of $\mathcal{O}^1$ from Algorithm 3.1.2.1, and an element $g \in G = \prod_{v\in\mathcal{V}_\infty} \mathrm{SL}_{d_v}(D_v)$, Subalgorithm 3.1.2.4 returns a product γ of elements of Σ such that $\iota(\gamma)g$ is in the Dirichlet domain D for $\Gamma = \iota(\mathcal{O}^1)$. The algorithm terminates in time at most*

$$\delta(g,1)\cdot\exp\Big(O(d\log\Delta_A) + O_N(\log\log\Delta_A)\Big).$$

PROOF. By Lemma 3.1.1.6, for all $t \geq 0$ we have $\delta(\exp(tX)k, 1) = t\delta(g,1)$. We also have $|t_{i+1} - t_i| \leq R/\delta(g,1)$ for all $i \leq m$. By the properties of `GreedyReduce`, after each execution of the loop 11–14 we have $\iota(\gamma)h_{i+1} \in D$. This proves that the algorithm is correct. To bound the running time, we estimate $\delta(\iota(\gamma)h_i, 1)$ and apply

Proposition 3.1.2.5. Since $\iota(\gamma)h_{i-1} \in D$ we have $\delta(\iota(\gamma)h_{i-1}, 1) \leq R$. We compute

$$\begin{aligned}
\delta(\iota(\gamma)h_i, 1) &= \delta(\iota(\gamma)\exp(t_iX)k, 1) \\
&= \delta(\iota(\gamma)\exp(t_iX), 1) \\
&= \delta(\iota(\gamma)\exp(t_{i-1}X)\exp((t_i - t_{i-1})X), 1) \\
&\leq \delta(\iota(\gamma)\exp(t_{i-1}X), 1) + \delta(\iota(\gamma)\exp((t_i - t_{i-1})X), 1) \\
&\leq \delta(\iota(\gamma)h_{i-1}, 1) + |t_i - t_{i-1}|\delta(g, 1) \\
&\leq 2R.
\end{aligned}$$

By Proposition 3.1.2.5 and since $R = O(\log \Delta_A/d) + O_N(1)$, the running time of each iteration of the loop is at most

$$\exp\Big(O(d \log \Delta_A) + O_N(\log\log \Delta_A)\Big).$$

Since $m \leq \delta(g, 1)$, this proves the proposition.

□

Thanks to the better control of the reduction steps, we could prove a complexity bound that is linear in the distance. It is likely that the greedy Subalgorithm 3.1.2.4 has the same complexity, but we do not know how to prove it.

We can finally put the pieces together an describe our algorithm for computing unit groups.

Algorithm 3.1.2.8.

Input: a maximal order $\mathcal{O}$ in a central division algebra A of degree d over a number field F, that is not a totally definite quaternion algebra.

Output: a finitely presented group Γ, and two computable group isomorphisms $\phi : \Gamma \to \mathcal{O}^1$ and $\psi : \mathcal{O}^1 \to \Gamma$, inverse of each other.

1: Σ, $\iota \leftarrow$ `Norm1SUnitGroup`$(\mathcal{O}, \mathcal{V}_\infty)$
2: Choose an arbitrary total order on $\mathcal{O}$
3: $L_1 \leftarrow$ `Sort`(Σ)
4: $L_2 \leftarrow \{gh \ : \ g \in \Sigma, h \in \Sigma\}$
5: $L_2 \leftarrow$ `Sort`(L_2)
6: $\mathsf{R} \leftarrow \emptyset$
7: **for all** $f \in L_1$ and $gh \in L_2$ such that $f = gh$ **do**
8: add $f = gh$ to R
9: **end for**
10: $\Gamma \leftarrow \langle \Sigma \mid \mathsf{R} \rangle$
11: let $\phi : \Gamma \to \mathcal{O}^1$ be the map that evaluates words in the generators
12: $\Sigma_0 \leftarrow \{\gamma \in \Sigma \mid \iota(\gamma) \in K\} \cup \{1\}$
13: **function** $\psi(g)$ **do**
14: $\gamma \leftarrow$ `Reduce`$(\iota, \Sigma, \iota(g))$ (Algorithm 3.1.2.6)
15: $g_1 \leftarrow \gamma g$
16: $\gamma_1 \leftarrow$ element of Σ_0 that equals g_1, as an element of Γ
17: **return** $\gamma^{-1}\gamma_1$
18: **end function**

19: **return** Γ, ϕ, ψ

THEOREM 3.1.2.9. *Given a maximal order $\mathcal{O}$ in a central division algebra A of degree d over a number field F, that is not a totally definite quaternion algebra, Algorithm 3.1.2.8 returns a finitely presented group Γ, and two computable group isomorphisms $\phi : \Gamma \to \mathcal{O}^1$ and $\psi : \mathcal{O}^1 \to \Gamma$, inverse of each other. The algorithm terminates in time at most*

$$\exp\Big(O(d \log \Delta_A) + O_N(\log\log \Delta_A)\Big).$$

Given an element $\gamma \in \mathcal{O}^1$, $\psi(\gamma)$ terminates in time at most

$$\delta(\iota(\gamma), 1) \cdot \exp\Big(O(d \log \Delta_A) + O_N(\log\log \Delta_A)\Big).$$

PROOF. For the correctness, the only claims left to prove are that the presentation is correct and that $\psi(g)$ is an expression of g as a word in the generators. For the presentation, since the symmetric space G/K is simply connected it follows from Lemma 1.2.2.3. Let $g \in \mathcal{O}^1$ and consider the call $\psi(g)$. By the properties of Algorithm 3.1.2.6, at Step 15 we have $\iota(g_1) \in D$ where D is the Dirichlet domain for $\mathcal{O}^1$. Since $g_1 \in \mathcal{O}^1$ we must have $\iota(g_1) \in K$, so g_1 is in Σ_0 and the element γ_1 in Step 16 exists and $\gamma g = \gamma_1$, that is $g = \gamma^{-1}\gamma_1$.

We analyse the running time of the algorithm. By Corollary 3.1.2.2, the call to `Norm1SUnitGroup` takes time at most

$$\exp\Big(O(d \log \Delta_A) + O_N(\log\log \Delta_A)\Big).$$

The computation of the presentation then takes time $\#\Sigma^{2+o(1)}$, which is the same complexity. The claim on the complexity of $\psi(\gamma)$ follows from Proposition 3.1.2.7. □

2. Efficient algorithms for the Kleinian case

The content of this section is the same as [**Pag13**], to be published in Mathematics of Computation. The main results are new deterministic and probabilistic algorithms for constructing fundamental domains for the action of arithmetic Kleinian groups Γ on hyperbolic three-space that produce a finite presentation for Γ. There is a substantial literature concerning such algorithms, some of which we review below. We compare our algorithms to recent ones and discuss numerical evidence suggesting that ours are more efficient.

The problem of computing fundamental domains for such groups is well studied. In the analogous Fuchsian group case, i.e. a subgroup of $\mathrm{PSL}_2(\mathbb{R})$, an algorithm may have been known to Klein, and J. Voight [**Voi09**] has described and implemented an efficient algorithm exploiting reduction theory. In the special case of Bianchi groups, i.e. when the base field is imaginary quadratic and the group is split, R.G. Swan [**Swa71**] has described an algorithm, which was implemented by Riley [**Ril83**] and A. Rahm [**Rah10**]; D. Yasaki [**Yas10**] has described and implemented another algorithm based on Voronoï theory. C. Corrales, E. Jespers, G. Leal and Á. del Río [**CJLdR04**] have described an algorithm for the general Kleinian

group case. They implemented it for one nonsplit group with imaginary quadratic base field. Our algorithm and implementation are more general, and more efficient in practice. We have recently found an unpublished algorithm of K. N. Jones and A. W. Reid, mentioned and briefly described in [**CFJR01**, section 3.1] that solves the same problem.

This section is organized as follows. We describe basic procedures to work in the hyperbolic 3-space, algorithms for computing a Dirichlet domain and a presentation with a computable isomorphism for a cocompact Kleinian group, and how to apply these algorithms to arithmetic Kleinian groups. Finally we show examples produced by our implementation of these algorithms and comment on their running time.

We are going to need the formula for the covolume of arithmetic Kleinian groups. It can be derived from the formula of Prasad by computing the normalization factor to obtain the hyperbolic volume. It takes the following form.

PROPOSITION 3.2.0.10. *Let F be an number field of degree n with exactly one complex place, A a quaternion algebra over F that is ramified at every real place, and $\mathcal{O}$ be an order in F. Let $\iota : A \hookrightarrow \mathcal{M}_2(\mathbb{C})$ be an algebra homomorphism extending a complex embedding of F. Then the group $\Gamma(\mathcal{O}) = \iota(\mathcal{O}^1)/\{\pm 1\} \subset \mathrm{PSL}_2(\mathbb{C})$ is a Kleinian group. It has finite covolume, and it is cocompact if and only if A is a division algebra. Furthermore, if $\mathcal{O}$ is maximal, we have*

$$\mathrm{covol}(\Gamma(\mathcal{O})) = \frac{|\Delta_F|^{3/2}\zeta_F(2)\Phi(\delta_F)}{(4\pi^2)^{n-1}} \tag{3}$$

where Δ_F is the discriminant of F, ζ_F is the Dedekind zeta function of F, δ_A is the reduced discriminant of A and $\Phi(\mathfrak{N}) = N(\mathfrak{N}) \cdot \prod_{\mathfrak{p}|\mathfrak{N}} (1 - N(\mathfrak{p})^{-1})$ for every ideal $\mathfrak{N}$ of F.

For simplicity, we say that a number field F is *almost totally real* (or *ATR*) if it has exactly one complex place. A quaternion algebra over an ATR field is *Kleinian* if it is ramified at every real place.

We describe every algorithm in ideal arithmetic. In section 2.5, we explain how to implement these algorithms using floating-point arithmetic.

2.1. Algorithms for polyhedra in the hyperbolic 3-space. We start with low-level algorithms for dealing with hyperbolic polyhedra. A point in $\mathcal{B}$ is represented by a vector in $\mathbb{C} + \mathbb{R}j$; a geodesic plane not containing 0 is represented by the Euclidean center and radius of the corresponding Euclidean sphere; a geodesic not containing 0 is represented by the Euclidean center and radius of a Euclidean sphere and a basis of a Euclidean plane containing the center of the sphere, such that the geodesic is the intersection of $\mathcal{B}$, this sphere and this plane.

Using these representations, it is an exercise in computational geometry to see that we can compute the faces, edges and vertices of a convex polyhedron given by a finite set of half-spaces containing 0. The details can be found in [**Pag10**, section II.3.3]. A harder task is to compute the volume of such a polyhedron. We describe an algorithm here; it is essentially the same as the one described in [**MR03**, section 1.7] but for the sake of completeness we provide all the details here.

Algorithm 3.2.1.1 computes the volume of a convex polyhedron with finitely many faces.

ALGORITHM 3.2.1.1 (Volume of a convex polyhedron).
Input: A convex polyhedron P with finitely many faces
Output: The hyperbolic volume of P
1: Split every face of P into triangles
2: Split P into tetrahedra
3: Using the map η^{-1}, send every tetrahedron back to $\mathcal{H}^3$
4: Express every tetrahedron as a difference of two tetrahedra, each having a vertex in the sphere at infinity
5: For every tetrahedron having a vertex in the sphere at infinity, apply an isometry to map it to a tetrahedron with one vertex at ∞ and the other vertices on the unit hemisphere
6: Express every such tetrahedron as a sum and difference of tetrahedra of the same type having one vertex at j
7: Express every such tetrahedron as a sum and difference of tetrahedra of the same type with projected Euclidean triangle having a right angle not at 0
8: For every such tetrahedron, compute the angles α and γ and use Proposition 1.2.4.1 to compute the volume
9: $\mathrm{vol}(P) \leftarrow$ sum of every contribution
10: **return** $\mathrm{vol}(P)$

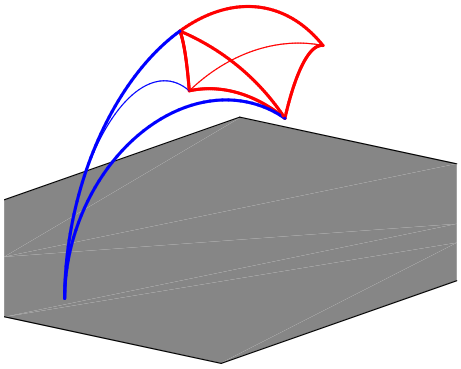

FIGURE 1. Step 4 in Algorithm 3.2.1.1

REMARKS 3.2.1.2.

- For step 1, choose a vertex of the face and link it to every other vertex;
- For step 2, choose a vertex of P and link it to every computed triangle;
- For step 4, choose an edge and consider a geodesic ray containing it, then the tetrahedron appears as the difference between two tetrahedra, each having the geodesic ray as an edge and a face of the initial tetrahedron as a base (see Figure 1);
- In step 6, the signs that appear in the sum are the signs of certain determinants;

- In step 8, the angle α is an angle in a Euclidean triangle and can be computed by elementary trigonometry, and since the upper half-space model is conformal, the angle γ is the Euclidean angle of intersection of the sphere and plane representing the faces of the tetrahedron.

The values of the Lobachevsky function are computed with the following lemma. It may be well-known, but we include it for the sake of completeness.

LEMMA 3.2.1.3. *For all $\theta \in (-\pi, \pi)$ we have the formula*

$$\mathcal{L}(\theta) = \pi \ln\left(\frac{\pi-\theta}{\pi+\theta}\right) + \theta\left(3 - \ln\left[2|\theta|\left(1-\left(\frac{\theta}{\pi}\right)^2\right)\right] + \sum_{n=1}^{\infty} \frac{\zeta(2n)-1}{n(2n+1)}\left(\frac{\theta}{\pi}\right)^{2n}\right)$$

and the bounds

$$\begin{aligned}\sum_{n>r} \frac{\zeta(2n)}{n(2n+1)}\left(\frac{\theta}{\pi}\right)^{2n} &\leq \frac{2}{3}\frac{1}{1-\left(\frac{\theta}{\pi}\right)^2}\left(\frac{\theta}{\pi}\right)^{2r+2}\\ \sum_{n>r} \frac{\zeta(2n)-1}{n(2n+1)}\left(\frac{\theta}{\pi}\right)^{2n} &\leq \frac{1}{1-\left(\frac{\theta}{2\pi}\right)^2}\left(\frac{\theta}{2\pi}\right)^{2r+2}.\end{aligned}$$

PROOF. To derive the first expression we use the previous power series expansion and extract the first term of the series expansion of the zeta function. For all $\theta \in (-\pi, \pi)$ we have

$$\sum_{n=1}^{\infty} \frac{\zeta(2n)}{n(2n+1)}\left(\frac{\theta}{\pi}\right)^{2n} = \sum_{n=1}^{\infty} \frac{1}{n(2n+1)}\left(\frac{\theta}{\pi}\right)^{2n} + \sum_{n=1}^{\infty} \frac{\zeta(2n)-1}{n(2n+1)}\left(\frac{\theta}{\pi}\right)^{2n}$$

since all these series converge. We only need to compute the power series that appears. By taking derivatives twice we find that for all $x \in (-1, 1)$ we have

$$\sum_{n=1}^{\infty} \frac{x^{2n+1}}{n(2n+1)} = 2x - x\ln(1-x^2) + \ln\left(\frac{1-x}{1+x}\right).$$

Letting $x = \frac{\theta}{\pi}$ in this expression gives the first formula.

To prove the inequalities we are going to bound the values $\zeta(2n)$ and $\zeta(2n)-1$ for $n \geq 1$. By series-integral comparison we get

$$\sum_{k=r}^{\infty} k^{-2n} \leq \frac{(r-1)^{1-2n}}{2n-1},$$

giving

$$\zeta(2n) = 1 + \sum_{k=2}^{\infty} k^{-2n} \leq 1 + \frac{1}{2n-1} \leq 2$$

for the first value, and

$$\zeta(2n) - 1 = 2^{-2n} + \sum_{k=3}^{\infty} k^{-2n} \leq \left(1 + \frac{2}{2n-1}\right)2^{-2n} \leq 3 \cdot 2^{-2n}$$

for the second one. Using these inequalities and the bound $\frac{1}{n(2n+1)} \leq \frac{1}{3}$, and computing the geometric sum gives the result. □

REMARKS 3.2.1.4.

- With the same method, for any k we can obtain a formula with remainder term $O\Big((\frac{\theta}{k\pi})^{2r}\Big)$.
- In practice, we precompute the coefficients of the power series we are using. By periodicity and oddness, we can always reduce to the case where $\theta \in [0, \frac{\pi}{2}]$: if the precision is fixed, we know a priori the maximal number of terms needed to evaluate the Lobachevsky function.

2.2. The reduction algorithm. When we have a fundamental domain, it is natural to ask for an algorithm that, given a point in the hyperbolic 3-space, computes an equivalent point in the fundamental domain and an element in the group that sends one point to the other.

DEFINITION 3.2.2.1. Let S be a subset[1] of a Kleinian group Γ. A point $z \in \mathcal{B}$ is *S-reduced* if for all $g \in S$, we have $d(z, 0) \leq d(gz, 0)$, i.e. if $z \in \overline{\mathrm{Ext}(S)}$.

ALGORITHM 3.2.2.2 (Reduction algorithm).

Input: A point $w \in \mathcal{B}$, a finite ordered subset $S \subset \mathrm{PSL}_2(\mathbb{C})$
Output: A point w' and an element $\delta \in \langle S \rangle$ s.t. w' is S-reduced and $w' = \delta w$

1: $w' \leftarrow w$, $\delta \leftarrow 1$
2: $g \leftarrow 1$
3: **repeat**
4: $\quad w' \leftarrow gw'$, $\delta \leftarrow g\delta$
5: $\quad g \leftarrow$ the first $g \in S$ such that $d(gw', 0)$ is minimal
6: **until** $d(gw', 0) \geq d(w', 0)$
7: **return** w', δ

PROPOSITION 3.2.2.3. *Given S a finite subset of a Kleinian group Γ and a point $w \in \mathcal{B}$, Algorithm 3.2.2.2 returns a point w' and $\delta \in \langle S \rangle$ such that w' is S-reduced and $w' = \delta w$.*

PROOF. After step 4, we have $w' = \delta w$ and $\delta \in \langle S \rangle$. Because of the loop condition, while the algorithm runs the distance $d(w', 0)$ decreases. Since w' stays in the orbit of w' under Γ and this orbit is discrete, the algorithm terminates. When it happens, g is an element in S such that $d(gw', 0)$ is minimal and $d(gw', 0) \geq d(w', 0)$, so w' is S-reduced. □

REMARK 3.2.2.4. At step 5, the g achieving the minimal $d(gw', 0)$ may not be unique. We can pick any of these elements. Ordering S gives us a canonical choice.

Reducing points can give interesting information about the elements of the group, because if w has a trivial stabilizer, then the orbit map $\gamma \mapsto \gamma \cdot w$ is a bijection. This is the reason for introducing the following definition:

DEFINITION 3.2.2.5. Let S be a subset of a Kleinian group Γ and $w \in \mathcal{B}$. An element $\gamma \in \mathrm{PSL}_2(\mathbb{C})$ is *(S, w)-reduced* if γw is S-reduced, i.e. if $\gamma w \in \overline{\mathrm{Ext}(S)}$.

[1] In this section, S will always denote a subset of a Kleinian group and never a set of places as in the previous chapter. We hope that this will cause no confusion.

Given a finite S, w and γ, we can now compute an (S,w)-reduced element $\bar{\gamma}$ such that $\bar{\gamma} \equiv \gamma \pmod{S}$ as follows: we reduce γw with respect to S; if $\delta \in \langle S \rangle$ is such that $\delta(\gamma w)$ is S-reduced, then $\bar{\gamma} = \delta\gamma$ is (S,w)-reduced. We also write the reduced element $\bar{\gamma} = \mathrm{Red}_S(\gamma; w)$ and simply $\mathrm{Red}_S(\gamma) = \mathrm{Red}_S(\gamma; 0)$. A priori this reduced element could depend on the chosen ordering in Algorithm 3.2.2.2.

PROPOSITION 3.2.2.6. *Suppose that* $\mathrm{Ext}(S)$ *is a fundamental domain for* $\langle S \rangle$. *Then for* $w \in \mathcal{B}$ *outside of a zero measure, closed subset of* $\mathcal{B}$, *the following holds: for every* $\gamma \in \Gamma$, *there exists a unique* (S,w)*-reduced* $\bar{\gamma} \equiv \gamma \pmod{S}$. *If* $w \in \mathrm{Ext}(S)$ *then* $\bar{\gamma} = 1$ *if and only if* $\gamma \in \langle S \rangle$.

PROOF. Let $w \in \Gamma \cdot \mathrm{Ext}(S)$. The existence follows from Algorithm 3.2.2.2. For uniqueness, suppose $\bar{\gamma}$ and $\bar{\gamma}'$ are (S,w)-reduced and $\bar{\gamma} \equiv \bar{\gamma}' \equiv \gamma \pmod{S}$. Then we have $\bar{\gamma}w, \bar{\gamma}'w \in \overline{\mathrm{Ext}(S)}$, and since w is in the orbit of $\mathrm{Ext}(S)$, they are in fact in $\mathrm{Ext}(S)$. Since these two points are in the same $\langle S \rangle$-orbit, we have $\bar{\gamma} = \bar{\gamma}'$. Now assume $w \in \mathrm{Ext}(S)$. If $\bar{\gamma} = 1$ then $\gamma \equiv \bar{\gamma} \equiv 1 \pmod{S}$, i.e. $\gamma \in \langle S \rangle$. If $\gamma \in \langle S \rangle$ then $\gamma \equiv 1 \pmod{S}$ and 1 is (S,w)-reduced so by uniqueness $\bar{\gamma} = 1$. Moreover the complement of $\Gamma \cdot \mathrm{Ext}(S)$ in $\mathcal{B}$ is a locally finite union of faces of $\mathrm{Ext}(S)$, so it is closed with zero measure. □

Since this provides an algorithm to write an element of the group as a word in the generators and to compute modulo $\langle S \rangle$ with explicit unique representatives, that particular kind of generating set deserves a name.

DEFINITION 3.2.2.7. A subset S of a Kleinian group Γ is a *basis* if $\mathrm{Ext}(S)$ is a fundamental domain for $\langle S \rangle = \Gamma$. If S is also a minimal defining set for $\mathrm{Ext}(S)$, it is called a *normalized basis* for Γ.

2.3. Normalized basis algorithms. Now we describe a general algorithm that computes a normalized basis for a cocompact Kleinian group Γ. We will then apply it to arithmetic groups. First note that, after conjugating the group by a suitable element in $\mathrm{PSL}_2(\mathbb{C})$, we may assume that $0 \in \mathcal{B}$ has a trivial stabilizer in Γ and that every elliptic cycle has length 1.

We will use two blackbox subalgorithms, `Enumerate` and `IsFullGroup`:

- `Enumerate`(Γ, n) takes as an input a positive integer n and returns a finite set of elements in Γ (the integer n is a parameter for iteration, it does not have any mathematical meaning);
- `IsFullGroup`(Γ, S) takes as an input a finite normalized basis S for a subgroup $\langle S \rangle \subset \Gamma$ and returns **true** or **false** according to whether $\langle S \rangle = \Gamma$ or not.

In every algorithm, an exterior domain $\mathrm{Ext}(S)$ with finite S is represented as a polyhedron in $\mathcal{B}$. We begin with a naive algorithm.

ALGORITHM 3.2.3.1 (Naive normalized basis algorithm).

Input: A Kleinian group Γ
Output: A normalized basis S for Γ

1: $S \leftarrow \emptyset,\ n \leftarrow 0$
2: **repeat**
3: **repeat**
4: $n \leftarrow n + 1$
5: add `Enumerate`(Γ, n) to S
6: $S \leftarrow$ minimal defining set of Ext(S)
7: **until** Ext(S) has a face-pairing **and** Ext(S) is complete **and** Ext(S) satisfies the cycle condition
8: **until** `IsFullGroup`(Γ, S)
9: **return** S

We say that `Enumerate` is a *complete enumeration* of Γ if we have

$$\bigcup_{n>0} \texttt{Enumerate}(\Gamma, n) = \Gamma.$$

PROPOSITION 3.2.3.2. *If Γ is geometrically finite and* ***`Enumerate`*** *is a complete enumeration of Γ, then Algorithm 3.2.3.1 terminates after a finite number of steps and the output S is a normalized basis for Γ.*

PROOF. The Dirichlet domain centered at 0 for Γ has finitely many faces by geometric finiteness. Since `Enumerate` is a complete enumeration, a defining set for this Dirichlet domain will be enumerated after a finite number of steps. The algorithm will then terminate as all the conditions are satisfied by Dirichlet domains. The output will then be a normalized basis for Γ by Step 6 and Theorem 1.2.4.4. □

We will now use the reduction algorithm to improve upon Algorithm 3.2.3.1. The main ideas are

- reducing the elements that we have to find smaller ones
- when the face-pairing condition, the cycle condition or the completeness condition fails, using this fact to find elements that make the exterior domain smaller.

For clarity, we divide Algorithm 3.2.3.3 into four routines. Algorithm 3.2.3.3 uses these routines to compute a normalized basis for a geometrically finite Kleinian group Γ.

ALGORITHM 3.2.3.3 (Normalized basis algorithm).

Input: A Kleinian group Γ
Output: A normalized basis S for Γ
1: $S \leftarrow \emptyset,\ n \leftarrow 0$
2: **repeat**
3: **repeat**
4: $n \leftarrow n + 1$
5: add `Enumerate`(Γ, n) to S
6: $S \leftarrow$ `KeepSameGroup`(S)
7: $S \leftarrow$ `CheckPairing`(S)
8: $S \leftarrow$ `CheckCycleCondition`(S)

9: $S \leftarrow$ `CheckComplete`(S)
10: **until** $\mathrm{Ext}(S)$ does not change
11: **until** `IsFullGroup`(Γ, S)
12: **return** S

The first routine, KeepSameGroup, reduces elements as much as possible to eliminate redundant ones and find smaller ones.

Subalgorithm 3.2.3.4 (KeepSameGroup).

Input: A finite subset $S \subset \mathrm{PSL}_2(\mathbb{C})$
Output: A new S generating the same group with smaller elements

1: **repeat**
2: $U \leftarrow$ minimal defining set of $\mathrm{Ext}(S)$
3: **for all** $g \in S$ **do**
4: $\bar{g} \leftarrow \mathrm{Red}_U(g)$
5: **if** $\bar{g} \neq \pm 1$ **then**
6: add $\bar{g}$ to U
7: **end if**
8: **end for**
9: $S \leftarrow U$
10: **until** $\mathrm{Ext}(S)$ does not change
11: **return** S

Proposition 3.2.3.5. *If S is a subset of a Kleinian group, then Algorithm 3.2.3.4 terminates and does not change the group generated by S.*

Proof. We first prove the second claim. Every element added to S belongs to the group generated by S as it is a reduction by $U \subset S$ of an element in S. Moreover, every element that is discarded has $\mathrm{Red}_U(g) = \pm 1$ so at the end of the loop we have $g \in \langle S \rangle$, and every other element $g \in S \smallsetminus U$ is replaced by $\bar{g} = \mathrm{Red}_U(g) \in \langle U \rangle g$, so the group generated by S does not change.

Now we prove that the algorithm terminates. First consider the initial S. Let $M = \max\{d(g \cdot 0, 0) : g \in S\}$ and $X_0 = \{g \in \langle S \rangle : d(g \cdot 0, 0) \leq M\}$. The set X_0 is finite since $\langle S \rangle$ is a Kleinian group, and we have $S \subset X_0$. By definition of reduction, every element added to U is in X_0. Moreover, by Step 2 if an element g is discarded then its isometric sphere $\mathrm{I}(g)$ does not intersect $\overline{\mathrm{Ext}(S)}$, so $g \cdot 0$ is in the complement of $\mathrm{Ext}(S)$: g cannot be the reduction of any element, so it cannot be added again. Similarly if $g \in S \smallsetminus U$ is replaced by $\bar{g} \neq g$, then g is not reduced so it cannot be added again. Hence the algorithm terminates. □

The second routine, CheckPairing, checks whether $\mathrm{Ext}(S)$ has a face-pairing. If it does not, it finds elements that make $\mathrm{Ext}(S)$ smaller.

Subalgorithm 3.2.3.6 (CheckPairing).

Input: A finite subset $S \subset \mathrm{PSL}_2(\mathbb{C})$
Output: A new S such that $\mathrm{Ext}(S)$ is smaller if it did not have a face-pairing

1: $S \leftarrow S \cup S^{-1}$
2: **for all** e edge in $\mathrm{I}(g)$ and $g \in S$, s.t. ge not an edge of $\overline{\mathrm{Ext}(S)}$ **do**
3: $x \leftarrow x \in e$ such that $gx \notin \overline{\mathrm{Ext}(S)}$
4: $\bar{g} \leftarrow \mathrm{Red}_S(g; x)$
5: add $\bar{g}, \bar{g}^{-1}$ to S
6: **end for**
7: **return** S

PROPOSITION 3.2.3.7. *If* $\mathrm{Ext}(S)$ *does not have a face-pairing, then after applying Algorithm 3.2.3.6,* $\mathrm{Ext}(S)$ *is strictly smaller.*

PROOF. If there is a nonpaired edge, at Step 5, since $x \in \mathrm{I}(g)$ we have $d(gx, 0) = d(x, 0)$ and since $gx \notin \overline{\mathrm{Ext}(S)}$ we have $d(gx, 0) > d(\bar{g}x, 0)$. Putting these two together gives $d(\bar{g}x, 0) < d(x, 0)$, i.e. $x \in \mathrm{Int}(\bar{g})$ so finally we have $\mathrm{Ext}(S \cup \{\bar{g}\}) \subsetneq \mathrm{Ext}(S)$. □

We give a second possible algorithm for CheckPairing. It is simpler but less efficient in practice. It uses the fact that if a non-elliptic cycle has length three (which is generically the case), then it is of the form $e \subset \mathrm{I}(g) \cap \mathrm{I}(h)$, $ge \subset \mathrm{I}(g^{-1}) \cap \mathrm{I}(gh^{-1})$, $he \subset \mathrm{I}(hg^{-1}) \cap \mathrm{I}(h^{-1})$.

SUBALGORITHM 3.2.3.8 (CheckPairing').

Input: A finite subset $S \subset \mathrm{PSL}_2(\mathbb{C})$
Output: A new S such that $\mathrm{Ext}(S)$ is smaller if it did not have a face-pairing
1: $S \leftarrow S \cup S^{-1}$
2: **for all** $g, h \in S$ s.t. $\mathrm{I}(g) \cap \mathrm{I}(h) \neq \emptyset$ and $h \neq g^{-1}$ **do**
3: add gh^{-1}, hg^{-1} to S
4: **end for**
5: **return** S

PROPOSITION 3.2.3.9. *If* $\mathrm{Ext}(S)$ *does not have a face-pairing, then after applying Algorithm 3.2.3.8,* $\mathrm{Ext}(S)$ *is strictly smaller.*

PROOF. If there is a nonpaired edge, then there exists elements $g, h \in S$ in the minimal defining set of $\mathrm{Ext}(S)$ and a point $x \in \mathrm{I}(g^{-1}) \cap \overline{\mathrm{Ext}(S)}$ such that $g^{-1}x \in \mathrm{Int}(h)$ (so that $h \neq g^{-1}$). Since we also have $g^{-1}x \in \mathrm{I}(g)$ and $\mathrm{I}(g)$ is not contained in $\mathrm{Int}(h)$, we get $\mathrm{I}(g) \cap \mathrm{I}(h) \neq \emptyset$, so these elements will be considered in the loop. On the other hand we have $d(x, 0) = d(g^{-1}x, 0) > d(g^{-1}hx, 0)$, so $x \in \mathrm{Int}(g^{-1}h)$: we have $\mathrm{Ext}(S \cup \{g^{-1}h\}) \subsetneq \mathrm{Ext}(S)$. □

REMARK 3.2.3.10. Although this algorithm is less efficient than Algorithm 3.2.3.6, it is interesting as it gives a geometric understanding of the method described in [**Lip02**]: *"we consider words that are two-word combinations of those forming the sides of the existing domain to modify the domain. (...) This procedure has proven to be fast and effective in practice."* Proposition 3.2.3.9 explains why taking products of two elements forming the sides of the domain is useful, and in Algorithm 3.2.3.8 we get a geometric description of the the products that we should

form. Actually, the computation in the proof of Proposition 3.2.3.8 also shows that if $\mathrm{I}(g^{-1}h)$ reduces $\mathrm{Ext}(S)$, then $\mathrm{I}(g) \cap \mathrm{I}(h) \neq \emptyset$.

The third routine, CheckCycleCondition, checks whether $\mathrm{Ext}(S)$ satisfies the cycle condition. If it does not, it finds elements that make $\mathrm{Ext}(S)$ smaller.

SUBALGORITHM 3.2.3.11 (CheckCycleCondition).

Input: A finite subset $S \subset \mathrm{PSL}_2(\mathbb{C})$
Output: A new S s.t. $\mathrm{Ext}(S)$ is smaller if it did not satisfy the cycle condition

1: Compute every well-defined edge cycle
2: **for all** g cycle transformation for the edge e **do**
3: **if** $g \neq \pm 1$ fixes at most one point in e **then**
4: $S \leftarrow S \cup \{g, g^{-1}\}$
5: **else if** $g \neq \pm 1$ fixes every point in e **then**
6: $S \leftarrow S \cup \langle g \rangle$
7: **else**
8: $m \leftarrow$ length of the cycle
9: **for all** $0 < i < m$ **do**
10: $h \leftarrow g_i \dots g_1$
11: add h, h^{-1} to S
12: **end for**
13: **end if**
14: **end for**
15: **return** S

REMARKS 3.2.3.12.

- If we assume that every non-elliptic cycle has length three, then the steps 8–12 are unnecessary, as in this case the partial cycle transformations at an edge contained in $\mathrm{I}(g) \cap \mathrm{I}(h)$ are g, $h = (hg^{-1})g$, $1 = h^{-1}(hg^{-1})g$.
- If we know in advance that the group Γ is torsion-free, then we can omit the steps 3–6.
- Assuming both, we can omit CheckCycleCondition completely.

LEMMA 3.2.3.13. *Suppose $S \subset \Gamma$ is a subset of a Kleinian group Γ such that 0 has a trivial stabilizer in Γ, and suppose there is an element $h \in \Gamma \setminus \{\pm 1\}$ and a point $x \in \mathrm{Ext}(S)$ such that $hx \in \mathrm{Ext}(S)$. Then $\mathrm{Ext}(S \cup \{h, h^{-1}\}) \subsetneq \mathrm{Ext}(S)$.*

PROOF. First suppose that $d(x, 0) < d(hx, 0)$. Then writing $x = h^{-1}(hx) = h^{-1}y$ we get $d(h^{-1}y, 0) < d(y, 0)$ i.e. $y \in \mathrm{Int}(h)$. Since we also have $y \in \mathrm{Ext}(S)$, we obtain $\mathrm{Ext}(S \cup \{h\}) \subsetneq \mathrm{Ext}(S)$.

Othewise we have $d(hx, 0) \leq d(x, 0)$. This means that $x \in \overline{\mathrm{Int}(h^{-1})}$, but since $x \in \mathrm{Ext}(S)$ we get $\mathrm{Ext}(S \cup \{h^{-1}\}) \subsetneq \mathrm{Ext}(S)$. □

PROPOSITION 3.2.3.14. *If $\mathrm{Ext}(S)$ does not satisfy the cycle condition, then after applying Algorithm 3.2.3.11, $\mathrm{Ext}(S)$ is strictly smaller.*

PROOF. Since the cycle transformation at an edge stabilizes it, if the edge is not equal to a geodesic then the cycle transformation fixes it pointwise and condition (i)

is automatically satisfied. Suppose that there is a cycle for an edge e equal to a geodesic and that does not satisfy condition (i), and let g be the corresponding cycle transformation. Then the transformation g is either loxodromic, or elliptic of order 2 with exactly one fixed point in e. In both cases, Step 4 is executed. In the first case, since the interior of the isometric sphere of a loxodromic element contains one of its fixed points and the interior of the isometric sphere of its inverse contains the other, we have $\overline{\mathrm{Ext}(\{g, g^{-1}\})} \cap e \subsetneq e$ so $\mathrm{Ext}(S \cup \{g, g^{-1}\}) \subsetneq \mathrm{Ext}(S)$. In the second case, the edge e contains exactly one fixed point of g in $\mathcal{H}^3$, so we again have $\overline{\mathrm{Ext}(\{g\})} \cap e \subsetneq e$ and we get $\mathrm{Ext}(S \cup \{g, g^{-1}\}) \subsetneq \mathrm{Ext}(S)$.

Now suppose some cycle angle for a non-elliptic cycle is larger than 2π. Then considering the images $P = \mathrm{Ext}(S), g_1^{-1}P, \ldots, (g_i \ldots g_1)^{-1}P$ of $P = \mathrm{Ext}(S)$ that glue one after another around e, we see that there is an overlap: there exists a point $x \in P$ such that $hx \in P$ for some h considered in Step 10. In this case after Step 11 we have $\mathrm{Ext}(S \cup \{h, h^{-1}\}) \subsetneq \mathrm{Ext}(S)$ by Lemma 3.2.3.13. Since the cycle transformation is the identity, the angle cannot be smaller than 2π.

Finally suppose some cycle angle for an elliptic cycle at an edge e with cycle transformation g with order ν does not satisfy condition (ii). The cycle has length 1, so $e \subset \mathrm{I}(g) \cap \mathrm{I}(g^{-1})$, and the angle at e is a multiple of $\frac{2\pi}{\nu}$. After running Step 6 the domain $\mathrm{Ext}(\{g, g^{-1}\})$ is replaced by the Dirichlet domain of the finite group $\langle g \rangle$, which satisfies the cycle condition, so the new angle at e is equal to $\frac{2\pi}{\nu}$. □

The fourth routine, CheckComplete, checks whether $\mathrm{Ext}(S)$ is complete. If it is not, it finds elements that make $\mathrm{Ext}(S)$ smaller.

Subalgorithm 3.2.3.15 (CheckComplete).

Input: A finite subset $S \subset \mathrm{PSL}_2(\mathbb{C})$
Output: A new S such that $\mathrm{Ext}(S)$ is smaller if it was not complete

1: Compute every tangency vertex cycle
2: **for all** h tangency vertex transformation **do**
3: **if** $h \neq 1$ is loxodromic **then**
4: add h, h^{-1} to S
5: **end if**
6: **end for**
7: **return** S

Remark 3.2.3.16. If we know in advance that the group Γ is cocompact, we can omit CheckComplete in Algorithm 3.2.3.3 and simply test whether $\mathrm{Ext}(S)$ is bounded.

Proposition 3.2.3.17. *If* $\mathrm{Ext}(S)$ *is not complete, then after applying Algorithm 3.2.3.11,* $\mathrm{Ext}(S)$ *is strictly smaller.*

Proof. If h is a tangency vertex transformation at $z = \mathrm{I}(g) \cap \mathrm{I}(g') \in \partial\mathcal{B}$, then it fixes z. By looking at the successive images of the polyhedron along the cycle we see that $\mathrm{I}(g')$ separates $\mathrm{I}(g)$ from $h\mathrm{I}(g)$, so h has infinite order. If $\mathrm{Ext}(S)$ is not

complete, then h is loxodromic. Being a fixed point of h, the point z is contained in $\mathrm{Int}(h) \cup \mathrm{Int}(h^{-1})$, so we get $\mathrm{Ext}(S \cup \{h, h^{-1}\}) \subsetneq \mathrm{Ext}(S)$. □

PROPOSITION 3.2.3.18. *Let Γ be a Kleinian group. The following holds for Algorithm 3.2.3.3 applied to Γ:*

(i) Suppose the algorithm terminates. Then the output is a normalized basis for Γ.
(ii) Suppose that Γ is geometrically finite and `Enumerate` *is a complete enumeration of Γ. Then the algorithm terminates.*

REMARK 3.2.3.19. In practice Algorithm 3.2.3.3 runs much faster that the naive Algorithm 3.2.3.1 (see section 3.1), but unfortunately we could not prove it. What we believe is that in Algorithm 3.2.3.3 the blackbox `Enumerate` only needs to find a set of generators for the group, and then the other routines find the elements of the normalized basis; in Algorithm 3.2.3.1 the blackbox `Enumerate` needs to find directly the elements of the normalized basis, which is harder. The natural idea would be to put the routines in a loop that would not contain `Enumerate` in Algorithm 3.2.3.3, but then it is not clear whether this internal loop would terminate; actually in general it is false, since Γ can admit finitely generated subgroups that are not geometrically finite.

PROOF.

(i) If the algorithm terminates, then by Theorem 1.2.4.4, since $\mathrm{Ext}(S)$ is complete, has a face-pairing and satisfies the cycle condition, the set S is a normalized basis for $\langle S \rangle$. It is then valid to use `IsFullGroup` to check that $\langle S \rangle = \Gamma$.
(ii) The closure of the Dirichlet domain centered at 0 for Γ has finitely many faces by geometric finiteness. Since `Enumerate` is a complete enumeration, a defining set for this Dirichlet domain will be enumerated after a finite number of steps. The algorithm will then terminate as all the conditions are satisfied by the Dirichlet domain.

□

2.4. Instantiation of the blackboxes.

`Enumerate` and `IsFullGroup` for a group given by generators. Suppose the group Γ is given by a finite set of generators G. We can take for `Enumerate` the algorithm that writes every word of length n in the generators, and we can take for `IsFullGroup` the algorithm that reduces every element in G with respect to the given normalized basis S and returns whether every generator reduces to ± 1: by Proposition 3.2.2.6, this is equivalent to $\Gamma \subset \langle S \rangle$.

`Enumerate` and `IsFullGroup` for an arithmetic group. We provide a possible instantiation of the blackboxes `Enumerate` and `IsFullGroup` for an arithmetic group $\Gamma(\mathcal{O})$ attached to a maximal order $\mathcal{O}$ in a Kleinian quaternion algebra A with base field F of degree n.

We describe `IsFullGroup` first. A subgroup is proper if and only if its covolume is infinite or at least twice the covolume of Γ, the quotient of the covolumes being the index of the subgroup. Since Γ comes from a maximal order, the covolume

of Γ is given by (3), which we can compute, and the covolume of a subgroup can be computed with Algorithm 3.2.1.1 once we have a normalized basis. We take for `IsFullGroup` the algorithm that computes the covolume $\mathrm{covol}(\Gamma)$ by the formula and the volume V of $\mathrm{Ext}(S)$ for the given normalized basis S, and returns whether $\frac{V}{\mathrm{covol}(\Gamma)} < 2$. Since S is a normalized basis for $\langle S\rangle$, the polyhedron $\mathrm{Ext}(S)$ is a fundamental domain for $\langle S\rangle$ so the volume V equals the covolume of $\langle S\rangle$.

We now describe an instantiation of the blackbox `Enumerate` for the Kleinian group associated with an order $\mathcal{O}$ in A. Under the natural embedding $\mathcal{O} \subset A \hookrightarrow A \otimes_{\mathbb{Q}} \mathbb{R}$, the order $\mathcal{O}$ is discrete. Now suppose that we have a positive definite quadratic form $Q : A \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{R}$. Then $\mathcal{O}$ becomes a full lattice in a real vector space of dimension $4n$. We can use lattice enumeration algorithms such as the Kannan-Fincke-Pohst algorithm [**FP85, Kan83**] to enumerate elements in $\mathcal{O}$ that are short with respect to Q. We can then select the elements having reduced norm 1. As we increase the bound on the values of Q, we will get every element in $\mathcal{O}^1$. A priori any such quadratic form would work, but here we describe one that has a geometric meaning.

Recall we can embed A in $M_2(\mathbb{C})$ in such a way that $\mathcal{O}^1$ becomes discrete in $\mathrm{SL}_2(\mathbb{C})$. This embedding is only defined up to conjugation by $\mathrm{PSL}_2(\mathbb{C})$. Let ι be such an embedding. If $A = \left(\frac{a,b}{F}\right)$ we can take for example

$$\iota : x + yi + zj + tij \mapsto \begin{pmatrix} x + y\alpha & z + t\alpha \\ (z - t\alpha)\beta & x - y\alpha \end{pmatrix}$$

where σ is a complex embedding of F, $\beta = \sigma(b)$ and α is a square root of $\sigma(a)$.

For $m = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathcal{M}_2(\mathbb{C})$, we define $\mathrm{invrad}(m) = \left|(c + \bar{b}) + (d - \bar{a})j\right|^2$.

PROPOSITION 3.2.4.1. *The quadratic form $Q : A \otimes \mathbb{R} \to \mathbb{R}$ defined by*

$$Q(x) = \mathrm{invrad}(\iota(x)) + \mathrm{Tr}_{F/\mathbb{Q}}(\mathrm{nrd}(x)) \text{ for all } x \in A$$

is positive definite and satisfies

$$Q(x) = \frac{4}{\mathrm{rad}(\iota(x))^2} + n \text{ for all } x \in \mathcal{O}^1$$

where $\mathrm{rad}(g)$ *denotes the Euclidean radius of the isometric sphere of $g \in \mathrm{SL}_2(\mathbb{C})$ if $g \cdot 0 \neq 0$, and ∞ otherwise.*

PROOF. We show first that Q is positive definite. For a matrix $m \in \mathcal{M}_2(\mathbb{C})$ we have $\mathrm{invrad}(m) = |c + \bar{b}|^2 + |d - \bar{a}|^2 = \|m\|^2 - 2\,\Re(\det m)$ where $\|\cdot\|$ is the usual L^2 norm on $\mathcal{M}_2(\mathbb{C})$, so that $\|\cdot\|^2$ is a positive definite quadratic form on $\mathcal{M}_2(\mathbb{C})$. Since nrd is a positive definite quadratic form on $\mathbb{H}$ and we have the decomposition $A \otimes \mathbb{R} \cong \mathcal{M}_2(\mathbb{C}) \oplus \mathbb{H}^{n-2}$, we can construct a positive definite quadratic form on $A \otimes \mathbb{R}$ by letting for all $x \in A \otimes \mathbb{R}$

$$Q(x) = \|m\|^2 + \mathrm{nrd}(h_1) + \cdots + \mathrm{nrd}(h_{n-2}) = \mathrm{invrad}(m) + \mathrm{Tr}_{F\otimes\mathbb{R}/\mathbb{R}}(\mathrm{nrd}(x))$$

where

$$x = m + h_1 + \cdots + h_{n-2} \in \mathcal{M}_2(\mathbb{C}) \oplus \mathbb{H}^{n-2},$$

since $2\,\Re(\det m) + \mathrm{nrd}(h_1) + \cdots + \mathrm{nrd}(h_{n-2}) = \mathrm{Tr}_{F\otimes\mathbb{R}/\mathbb{R}}(\mathrm{nrd}(x))$. This gives the positive definiteness.

For the formula on $\mathcal{O}^1$, note that according to (2), it is

$$\mathrm{invrad}(g) = \left|(c+\bar{b}) + (d-\bar{a})j\right|^2 = \frac{4}{\mathrm{rad}(g)^2}$$

for $g \in \mathrm{SL}_2(\mathbb{C})$ not fixing 0 in $\mathcal{B}$, and if g fixes 0 then $\mathrm{invrad}(g) = 0$. □

We obtain the following enumeration algorithm. It is a complete enumeration of $\Gamma(\mathcal{O})$, and depends on a parameter: a sequence of bounds $A_n \to \infty$.

Subalgorithm 3.2.4.2 (`Enumerate`).

Input: A positive integer n
Output: A finite subset $L \subset \Gamma(\mathcal{O})$

```
L ← ∅
for all x ∈ O such that Q(x) ≤ A_n do
    if nrd(x) = 1 then
        Add ι(x) to L
    end if
end for
return L
```

We are now going to present a probabilistic enumeration algorithm. It is not a complete enumeration, but performs better in pratice (see section 3.1). It uses variants of the former quadratic form.

Definition 3.2.4.3. Let $z_1, z_2 \in \mathcal{H}^3$. Let $h_1, h_2 \in \mathrm{SL}_2(\mathbb{C})$ be such that $z_1 = h_1 \cdot j$ and $z_2 = h_2 \cdot j$. We then define the quadratic form Q_{z_1,z_2} by

$$Q_{z_1,z_2}(x) = \mathrm{invrad}(h_2^{-1}\iota(x)h_1) + \mathrm{Tr}_{F/\mathbb{Q}}(\mathrm{nrd}(x))$$

for all $x \in A$.

This family of quadratic forms has the following properties.

Proposition 3.2.4.4. *Let $z_1, z_2 \in \mathcal{H}^3$. Then Q_{z_1,z_2} does not depend on the choice of $h_1, h_2 \in \mathrm{SL}_2(\mathbb{C})$ such that $z_1 = h_1 \cdot j$ and $z_2 = h_2 \cdot j$. It is positive definite, and for all $g \in \mathcal{O}^1$ we have*

$$Q_{z_1,z_2}(g) = 2\cosh d(gz_1, z_2) - 2 + n.$$

Proof. The matrices h_1 and h_2 are defined up to right multiplication by $\mathrm{SU}_2(\mathbb{C})$, the stabilizer of the point j. For all matrices $m \in \mathcal{M}_2(\mathbb{C})$ we have $\mathrm{invrad}(m) = \|m\|^2 - 2\,\Re(\det m)$, which is not changed by left and right multiplication of m by elements of $\mathrm{SU}_2(\mathbb{C})$, so that Q_{z_1,z_2} does not depend on the choice of h_1 and h_2.

For $z_1 = z_2 = j$ the formula reads $\|g\|^2 = 2\cosh d(gj, j)$ for all $g \in \mathrm{SL}_2(\mathbb{C})$, which is well-known (and is a direct consequence of the explicit formulas for the hyperbolic distance). Then for arbitrary $z_1, z_2 \in \mathcal{H}^3$ we have

$$\|h_2^{-1}gh_1\|^2 = 2\cosh d(h_2^{-1}gh_1 j, j) = 2\cosh d(gh_1 j, h_2 j) = 2\cosh d(gz_1, z_2).$$

□

This family of quadratic forms is very useful, as it enables us to determine the elements $g \in \Gamma(\mathcal{O})$ such that gz_1 is close to z_2. We propose the following probabilistic algorithm for enumerating elements in $\Gamma(\mathcal{O})$. It depends on a choice of some parameters: an increasing sequence of positive numbers $R_n \to \infty$ representing the radius of the search space, a sequence of positive integers $N_n \in \mathbb{Z}_{>0}$ representing the number of enumerations in small balls, and a positive number A being a bound on the quadratic form. For $w_1, w_2 \in \mathcal{B}$, we write $Q_{w_1,w_2} = Q_{\eta^{-1}(w_1),\eta^{-1}(w_2)}$.

SUBALGORITHM 3.2.4.5 (`Enumerate'`).

Input: An positive integer n
Output: A finite subset $L \subset \Gamma(\mathcal{O})$

$L \leftarrow \emptyset$
for $i = 1$ to N_n **do**
  Draw a point $w \in \mathcal{B}$ such that $d(0, w) \leq R_n$ randomly, uniformly w.r.t. the hyperbolic volume
  for all $x \in \mathcal{O}$ such that $Q_{0,w}(x) \leq A$ **do**
    if $\mathrm{nrd}(x) = 1$ **then**
      Add $\iota(x)$ to L
    end if
  end for
end for
return L

REMARKS 3.2.4.6.

- We can also use these quadratic forms differently: if we miss an element of the group to "close off" the exterior domain around a point at infinity ξ, we can look for elements of small $Q_{j,z}$ where $z \to \xi$. This is a similar idea as in Remark 4.9 in [**Voi09**], but the quadratic form that was used there is the analogue of $Q_{z,z}$. If g is the element that we are looking for, $d(gz, z)$ is bounded by below by a positive constant if g is loxodromic, which is the generic case. On the contrary we have $d(gj, z) \to 0$ as $z \to gj$.
- The efficiency of this algorithm depends on the choice of the parameters N_n, R_n and A. Heuristics led us to the following choice, which works well in practice:
  - we use a small bound $A = \alpha \cdot |\Delta_F N(\delta_A)|^{\frac{1}{4[F:\mathbb{Q}]}}$ so that the number of $x \in \mathcal{O}$ such that $Q_{0,w}(x) \leq A$ is approximately constant by Gaussian heuristic;
  - experimental evidence and Gelander's Theorem 2.2.0.15 suggest that a number of random elements of Γ proportional to $\mathrm{covol}(\Gamma)$ has a good probability to generate Γ, and by Gaussian heuristic we need on average $O(\mathrm{covol}(\Gamma))$ random centers to obtain one element of the group, so we choose $N_0 = \beta \cdot \mathrm{covol}(\Gamma)^2$, and we increase it exponentially fast: $N_n = (1 + \eta)^n N_0$;

– the radius R_n has to be large enough to ensure good randomness of the elements of Γ, so we choose R_0 such that $\mathrm{vol}(B(w, R_0)) = \mathrm{covol}(\Gamma)^\gamma$ and we increase it in arithmetic progression (so the volume increases exponentially fast): $R_n = R_0 + \epsilon \cdot n$. Because of our choice of N_n we take $\gamma > 2$.

Now we explain how we draw points at random in the ball $B(0, R)$ of radius R. Since the hyperbolic volume is invariant by rotation around 0, it is equivalent to draw a random point uniformly on the sphere, and then multiply it by an appropriate random scalar independent from the point on the sphere. Thus we only have to determine the distribution of the distance from 0 of the points in the ball of radius R. Let X be a random variable with uniform distribution in $B(0, R)$. The cumulative distribution function of the distance to 0 is

$$f_R(r) = \mathcal{P}_X(d(X, 0) \leq r) = \frac{\mathrm{vol}(B(0, r))}{\mathrm{vol}(B(0, R))}.$$

Recall that the volume $v(r)$ of the ball of radius r is $v(r) = \pi(\sinh(2r) - 2r)$. It is clear that the function $f_R : [0, R] \to [0, 1]$ is a continuous bijection. It implies that $d(0, X) = f_R^{-1}(U)$ where U is a uniform random variable in $[0, 1]$. We rewrite that expression as $d(0, X) = v^{-1}(U')$ where U' is a uniform variable in $[0, v(R)]$. It is well-known how to draw a uniform variable in an interval and on a sphere, and v^{-1} can be computed by Newton iteration.

2.5. Floating-point implementation. Here we describe a floating-point implementation of the above algorithms. We start with a lemma giving us control on the error made when having an element of the group act on a point. We only study the stability of the algorithm, so we do not take into account the error made by rounding in elementary operations.

LEMMA 3.2.5.1. *Let $g \in \mathrm{SL}_2(\mathbb{C})$, $\tilde{g} \in \mathcal{M}_2(\mathbb{C})$ and $w, \tilde{w} \in \mathcal{B}$. Let $\epsilon = |w - \tilde{w}|$, $\eta = \|g - \tilde{g}\|$ and $\delta = \frac{1}{1-|w|^2}$. Suppose that $(\|g\|\epsilon + 2\eta)^2 \leq \frac{1}{3\delta}$. Then the quantity $\widetilde{gw}$ obtained by applying Formula (1) to $\tilde{g}$ and $\tilde{w}$ is well-defined, and we have*

$$|g \cdot w - \widetilde{gw}| \leq 68\, \delta^{\frac{3}{2}} \|g\|^3 \epsilon + 136\, \delta^{\frac{3}{2}} \|g\|^2 \eta.$$

PROOF. By direct computation we have $|A - \tilde{A}| \leq \sqrt{2}\eta$ and $|A| \leq \sqrt{2}\|g\|$, and the same inequalities for B, C, D. We write

$$g \cdot w = (Aw + B)(Cw + D)^{-1} = \frac{1}{|Cw + D|^2}(Aw + B)(\overline{w}\overline{C} + \overline{D})$$

and similarly for $\tilde{g}, \tilde{w}$. Another direct computation gives

$$|w|^2 - |g \cdot w|^2 = \left(1 - \frac{4}{|Cw + D|^2}\right)(|w|^2 - 1), \tag{4}$$

showing that

$$\frac{1}{|Cw + D|^2} \leq \frac{1}{4}(1 + 2\delta) \leq \frac{3}{4}\delta \quad \text{and} \quad \frac{4}{3\delta} \leq |Cw + D|^2.$$

By the triangle inequality, adding and substracting $A\tilde{w}$ gives

$$|Aw - \tilde{A}\tilde{w}| \leq \sqrt{2}\|g\|\epsilon + \sqrt{2}\eta$$

and the same inequality for Cw. We get

$$|(Cw + D) - (\tilde{C}\tilde{w} + \tilde{D})|^2 \leq 2(\|g\|\epsilon + 2\eta)^2 \leq \frac{|Cw + D|^2}{2}$$

since by hypothesis we have $(\|g\|\epsilon + 2\eta)^2 \leq \frac{1}{3\delta}$. In particular $\tilde{C}\tilde{w} + \tilde{D} \neq 0$ and $\widetilde{gw}$ is well-defined. By the mean value theorem this gives

$$||Cw + D|^{-2} - |\tilde{C}\tilde{w} + \tilde{D}|^{-2}| \leq (6\delta)^{\frac{3}{2}}(\|g\|\epsilon + 2\eta)$$

We also get

$$\begin{aligned} & |(Aw + B)(\overline{w}\overline{C} + \overline{D}) - (\tilde{A}\tilde{w} + \tilde{B})(\overline{\tilde{w}}\overline{\tilde{C}} + \overline{\tilde{D}})| \\ \leq\ & |Aw + B|(\sqrt{2}\|g\|\epsilon + 2\sqrt{2}\eta) + 2|Cw + D|(\sqrt{2}\|g\|\epsilon + 2\sqrt{2}\eta) \\ \leq\ & (2\sqrt{2}\|g\|)(\sqrt{2}\|g\|\epsilon + 2\sqrt{2}\eta) + (2\sqrt{2}\|g\|)(2\sqrt{2}\|g\|\epsilon + 4\sqrt{2}\eta) \\ =\ & 12\|g\|^2\epsilon + 24\|g\|\eta. \end{aligned}$$

Finally we have

$$\begin{aligned} & |(Aw + B)(Cw + D)^{-1} - (\tilde{A}\tilde{w} + \tilde{B})(\tilde{C}\tilde{w} + \tilde{D})^{-1}| \\ \leq\ & |g \cdot w||Cw + D|^2(6\delta)^{\frac{3}{2}}(\|g\|\epsilon + 2\eta) + \tfrac{2}{|Cw+D|^2}(12\|g\|^2\epsilon + 24\|g\|\eta) \\ \leq\ & (24\sqrt{6} + 9)\delta^{\frac{3}{2}}\|g\|^3\epsilon + (48\sqrt{6} + 18)\delta^{\frac{3}{2}}\|g\|^2\eta \\ \leq\ & 68\,\delta^{\frac{3}{2}}\|g\|^3\epsilon + 136\,\delta^{\frac{3}{2}}\|g\|^2\eta \end{aligned}$$

as claimed. □

In the following, we want to maintain the property $(\|g\|\epsilon + 2\eta)^2 \leq \frac{1}{3\delta}$ for every element g and every point w considered, where ϵ is the imprecision on the points in $\mathcal{B}$, η the imprecision on the elements g considered, and $\eta = \frac{8}{3}\epsilon$.

We now describe the modification of the algorithms for the floating-point version. In the reduction algorithm (Algorithm 3.2.2.2), we choose $\alpha > 0$ and in Step 6 we replace the inequality $d(gw', 0) \geq d(w', 0)$ by $\frac{4}{|Cw'+D|^2} \leq 1 + \alpha$. Since we have $w' \in \mathrm{Ext}(g)$ if and only if $|Cw' + D|^2 \geq 4$, the modified condition is indeed an approximation of the exact condition.

PROPOSITION 3.2.5.2. *Let $\beta = \alpha - 68\,\delta^{\frac{5}{2}}M^3\epsilon - 136\,\delta^{\frac{5}{2}}M^2\eta$ where $\delta = \frac{1}{1-|w|^2}$ and $M = \max_{g\in S}\|g\|$. If $\beta > 0$, then the floating-point version of the reduction algorithm terminates.*

PROOF. Formula (4) can be rewritten

$$1 - |g \cdot w|^2 = \frac{4}{|Cw + D|^2}(1 - |w|^2),$$

which gives, if the modified condition of Step 6 is not satisfied

$$1 - |g \cdot w'|^2 \geq (1 + \alpha)(1 - |w'|^2).$$

Lemma 3.2.5.1 gives

$$1 - |\widetilde{gw'}|^2 \geq (1+\beta)(1-|w'|^2),$$

so $1-|w'|^2$ is multiplied by $1+\beta$ at each step of the algorithm. Since we also have $1-|w'|^2 \leq 1$, the algorithm terminates. □

We want to use a uniform α that tends to 0 as $\epsilon \to 0$. For this, we assume that we only consider points w such that $1-|w|^2 \geq 2\epsilon^{\frac{2}{9}}$ and elements g such that $\|g\| \leq \epsilon^{-\frac{1}{9}}$. Assuming that $\epsilon < 10^{-9}$ we can then take $\alpha = 18\epsilon^{\frac{1}{9}}$. These assumptions also ensure that $(\|g\|\epsilon + 2\eta)^2 \leq \frac{1}{3\delta}$, and are compatible since the points $g \cdot 0$ that we have to consider satisfy $1-|g\cdot 0|^2 = \frac{4}{\|g\|^2+2} \geq \frac{2}{\|g\|^2} \geq 2\epsilon^{\frac{2}{9}}$.

There is no change in KeepSameGroup (Algorithm 3.2.3.4): the same argument shows that the algorithm terminates, regardless of finite precision in the computations.

The routine CheckPairing (Algorithm 3.2.3.6) should only consider an edge e contained in $\mathrm{I}(g)$ as not being paired if there is $x \in e$ and we have the stronger inequality $|C\widetilde{gx}+D|^2 < \frac{4}{1+\alpha}$ and C, D correspond to h for some $h \in S$. This ensures that the floating-point reduction will yield a non-trivial element, since at least one step of reduction will be performed.

The routines CheckCycleCondition (Algorithm 3.2.3.11) and CheckComplete (Algorithm 3.2.3.15) contain only finite loops regardless of the use of finite precision, so there is no change in them.

Proposition 3.2.5.3. *The floating-point version of the Normalized basis algorithm (Algorithm 3.2.3.3) terminates.*

Proof. By the arguments above, each of the routines terminates. Moreover, because of precision restriction we impose $\|g\| \leq \epsilon^{-\frac{1}{9}}$ for every element g of the group considered in the algorithm, so that only finitely many g can be used, so the algorithm terminates. □

Of course if the precision chosen is insufficient, the algorithm can terminate with an error or a wrong answer, but with Riley's methods [**Ril83**], we can use Poincaré's theorem with the approximate fundamental domain to prove that the computed presentation is correct. Alternatively, we could check the fundamental domain algebraically, but this is likely to be time-consuming.

2.6. Master algorithm. As a summary, this is our master algorithm for computing an arithmetic Kleinian group associated with a maximal order.

Algorithm 3.2.6.1 (Master algorithm).

Input: A maximal order $\mathcal{O}$ in a Kleinian quaternion algebra A

Output: A finitely presented group Γ, and two computable group homomorphism $\phi : \Gamma \to \Gamma(\mathcal{O})$ and $\psi : \Gamma(\mathcal{O}) \to \Gamma$, inverse of each other

1: Choose an embedding $\iota : A \hookrightarrow \mathcal{M}_2(\mathbb{C})$ s.t. the point 0 has trivial stabilizer in the group $\Gamma(\mathcal{O}) = \iota(\mathcal{O}^1)/\{\pm 1\}$

2: $V \leftarrow \mathrm{covol}(\Gamma(\mathcal{O}))$ computed with Formula (3)

3: **function** `IsFullGroup`(S) **do**
4: compute $V' = \mathrm{vol}(\mathrm{Ext}(S))$ with Algorithm 3.2.1.1
5: **return** $V' < 2V$
6: **end function**
7: `Enumerate` $\leftarrow$ Algorithm 3.2.4.2 or Algorithm 3.2.4.5
8: $\Sigma \leftarrow$ output of the Normalized Basis Algorithm 3.2.3.3
9: $\mathsf{R} \leftarrow$ inverse, cycle and reflection relations from Theorem 1.2.4.2
10: $\Gamma \leftarrow \langle \Sigma \mid \mathsf{R} \rangle$
11: Let $\phi : \Gamma \to \Gamma(\mathcal{O})$ be the map that evaluates words in the generators
12: Let $\psi : \Gamma(\mathcal{O}) \to \Gamma$ be the map that writes elements as words in the generators using Algorithm 3.2.2.2
13: **return** Γ, ϕ, ψ

Remarks 3.2.6.2.

- If we want to compute the group that is the image of a smaller order, or more generally a finite index subgroup Γ' of the group $\Gamma(\mathcal{O})$ given by a maximal order $\mathcal{O}$, we can compute first a normalized basis for the larger group $\Gamma(\mathcal{O})$, and then compute the index by standard coset enumeration techniques. This gives the covolume of the smaller group, and even a set of generators for it, so we can then apply the same algorithm we described.
- We may also want to compute a maximal group in the commensurability class of $\Gamma(\mathcal{O})$. There are infinitely many conjugacy classes of such maximal groups. They were originally described in [**Bor81**] but the reader can also refer to [**MR03**, Section 11.4]. They can be obtained as follows. Let $\mathcal{O}'$ be a maximal order in A, and S a finite set of primes of F that split in A. Let $\mathcal{O}'' \subset \mathcal{O}'$ be an Eichler order of level $\mathfrak{N}$ where $\mathfrak{N}$ is the product of the primes in S, and define $\Gamma_{S,\mathcal{O}'}$ to be the normalizer of $\mathcal{O}''$ in $A^\times$. Then every maximal group in the commensurability class of $\Gamma(\mathcal{O})$ is conjugate to a group $\Gamma_{S,\mathcal{O}'}$ for some set S and some maximal order $\mathcal{O}'$, which can be taken from a set of representatives of the conjugacy classes of maximal orders in A. Note however that some of the groups $\Gamma_{S,\mathcal{O}'}$ may not be maximal. Since each of these groups is the image in $\mathrm{PSL}_2(\mathbb{C})$ of the normalizer of an order in A, we can use the same enumeration techniques. The index is given in terms of a class group and a finite quotient of units in $\mathbb{Z}_F$, which can be computed, so again we get the covolume of this larger group, and can apply the same technique.

3. Examples

The author has implemented the algorithm described in the previous section in the computer system Magma [**BCP97**]. Our package `KleinianGroups` is available at `http://www.normalesup.org/~page/software.html`. Here we show some examples of the output of this code. In sections 3.1 and 3.2, the computations are

performed on a 1.73 GHz Intel i7 processor with Magma v2.18-4. The more extensive computations of sections 3.3 and 3.4 are run on a 2.5 GHz Intel Xeon E5420 processor from the PLAFRIM experimental testbed with Magma v2.17-12.

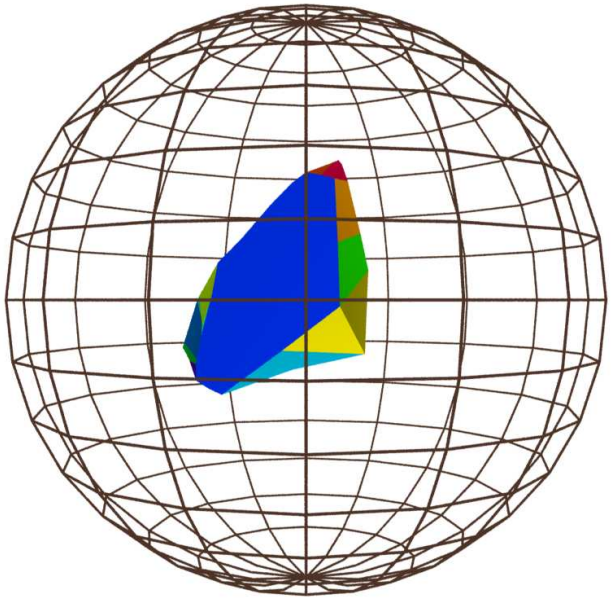

FIGURE 2. Dirichlet domain of a Kleinian group over a sextic field

3.1. Comparison between subalgorithms.

Comparison between the normalized basis algorithms. Consider the ATR sextic field F of discriminant -92779 generated by an element t such that $t^6 - t^5 - 2t^4 + 3t^3 - t^2 - 2t + 1 = 0$, and let $\mathbb{Z}_F$ be its ring of integers. Let $A = \left(\frac{-1,-1}{F}\right)$ be the quaternion algebra ramified only at the real places of F. Let $\mathcal{O}$ be a maximal order in A; the choice does not matter as they are all conjugate. The Kleinian group $\Gamma(\mathcal{O})$ has covolume $0.3007\ldots$. We compare our algorithm with the naive Algorithm 3.2.3.1. Both need a precomputation of 3 seconds for the computation of the coefficients of the Lobachevsky power series and 4 seconds for the evaluation of the Dedekind zeta function at 2. Our algorithm then computes a Dirichlet domain in 2 seconds, and enumerates 37 elements of $\mathcal{O}$, yielding 21 elements of $\Gamma(\mathcal{O})$. The naive algorithm (actually we only removed the routine CheckPairing) computes the same Dirichlet domain in 48 seconds and has to enumerate 16 246 elements of $\mathcal{O}$, yielding 1713 elements of $\Gamma(\mathcal{O})$. The fundamental domain (Figure 2) has 18 faces and 42 edges.

Comparison between the enumeration algorithms. Consider the ATR number field F of degree 8 and discriminant -407793664, generated by an element t such that $t^8 - 4t^7 + 4t^6 + 2t^5 - 8t^4 + 4t^3 + 5t^2 - 2t - 1 = 0$, and let $\mathbb{Z}_F$ be its ring of integers. Let $A = \left(\frac{-1,-1}{F}\right)$ be the quaternion algebra ramified only at the real places of F. Let $\mathcal{O}$ be a maximal order in A; the choice does not matter as they are all conjugate.

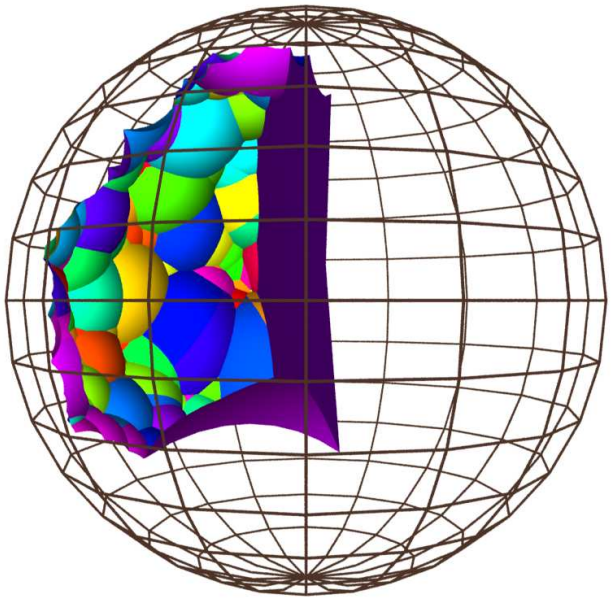

FIGURE 3. Dirichlet domain of a Kleinian group over an octic field

The Kleinian group $\Gamma(\mathcal{O})$ has covolume $56.509\ldots$. We compare the performance of our algorithm when using the enumeration algorithms 3.2.4.2 or 3.2.4.5. With the deterministic enumeration algorithm 3.2.4.2, our code computes a fundamental domain in 12 hours and 45 minutes (45943 seconds, most of which is enumeration), and enumerates 84 159 799 vectors, yielding 1600 group elements. With the probabilistic enumeration algorithm 3.2.4.5, our code computes the same Dirichlet domain in 71 seconds, and only needs to enumerate 3511 vectors, yielding 164 group elements. It spends 2 seconds for computing the value of the zeta function, 16 seconds for enumeration, 3 seconds for the routine KeepSameGroup, 40 for CheckPairing and 10 for computing the volume of the polyhedron. The fundamental domain (Figure 3) has 202 faces and 582 edges.

3.2. Relation to previous work. In this section we show how to recover examples covered by earlier work with our algorithm. When available, we provide a comparison of running times between public implementations and our Magma code. The reader should keep in mind that these are only comparisons between implementations since the complexity of the algorithms is usually unknown.

Bianchi groups. Let F be an imaginary quadratic field with ring of integers $\mathbb{Z}_F$. Consider the quaternion algebra $A = \mathcal{M}_2(F)$ and the maximal order $\mathcal{O} = \mathcal{M}_2(\mathbb{Z}_F)$. Then the group $\Gamma(\mathcal{O}) = \mathrm{PSL}_2(\mathbb{Z}_F)$ is called a *Bianchi group*. There exists already several programs computing fundamental domains for these groups [**Rah10, Yas10**] but they only work for Bianchi groups while ours deals with general arithmetic Kleinian groups. Table 1 gives the running time (in seconds) of our Magma package and other public implementations. The first three columns correspond to the discriminant of the field, its class number and the covolume of $\mathrm{PSL}_2(\mathbb{Z}_F)$. The

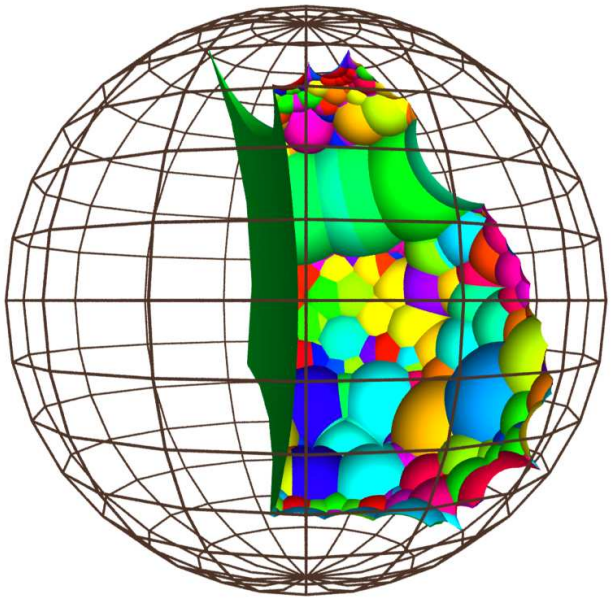

FIGURE 4. Dirichlet domain of the Bianchi group $\mathrm{PGL}_2\left(\mathbb{Z}\left[\frac{1+\sqrt{-199}}{2}\right]\right)$

last four columns display running times in seconds: `Bianchi.gp` [**Rah10**] written in GP [**PAR14**] implementing Swan's algorithm for $\mathrm{PSL}_2(\mathbb{Z}_F)$, our Magma package `KleinianGroups` computing $\mathrm{PSL}_2(\mathbb{Z}_F)$, the code provided by Magma implementing the algorithm of [**Yas10**] using Voronoï theory for $\mathrm{PGL}_2(\mathbb{Z}_F)$, and our code for $\mathrm{PGL}_2(\mathbb{Z}_F)$. Note that it is not surprising that computing $\mathrm{PGL}_2(\mathbb{Z}_F)$ is faster: the group is larger by an index 2, so the covolume is twice smaller and our computation is 4 times shorter (see also section 3.4). The numerical data suggest that the complexity of the Voronoï method is the same as ours, with a factor of 2 in the running time coming from the implementation. On the other hand, the implementation of Swan's algorithm seems to have larger complexity than our algorithm, maybe a larger exponent.

Arithmetic Fuchsian groups. Let F be a totally real field and A a quaternion algebra ramified at every infinite place but one. Let $\mathcal{O}$ be an order in A. Then the group $\Gamma(\mathcal{O}) = \mathcal{O}^1/\{\pm 1\}$ embeds into $\mathrm{PSL}_2(\mathbb{R})$, in which it is discrete with finite covolume: it is an *arithmetic Fuchsian group*. Using the action of $\mathrm{PSL}_2(\mathbb{R})$ on the upper half-plane Voight [**Voi09**] was able to compute fundamental domains for these groups. Since we have $\mathrm{PSL}_2(\mathbb{R}) \subset \mathrm{PSL}_2(\mathbb{C})$, a Fuchsian group can be seen as a Kleinian group leaving a geodesic plane stable. Using this we can also compute arithmetic Fuchsian groups with our code. Our probabilistic enumeration Algorithm 3.2.4.5 leads to an improvement in high degree. As an example, consider the totally real field F with discriminant 9685993193, generated by an element t such that $t^9 - 2t^8 - 7t^7 + 11t^6 + 15t^5 - 15t^4 - 10t^3 + 7t^2 + 2t - 1 = 0$. Let $A = \left(\frac{a,b}{F}\right)$ with $a = -3t^8 + 2t^7 + 30t^6 - 8t^5 - 93t^4 + 90t^2 + 2t - 26$ and $b = -1$. It is ramified at

Δ_F	h_F	volume	`Bianchi`	`KG`, PSL_2	Magma	`KG`, PGL_2
-3	1	0.169	0.015	0.93	0.43	0.83
-15	2	3.139	0.152	0.92	0.8	2.32
-23	3	6.449	0.176	1.22	1.11	2.06
-39	4	13.80	2.37	9.44	3.05	4.36
-47	5	19.43	3.83	19.9	5.33	6.96
-71	7	37.53	21.6	36.6	17.8	13.2
-87	6	44.72	25.7	45.1	17.3	16.4
-95	8	57.06	41.4	43.8	33.9	19.3
-119	10	82.93	7080.	137.	99.5	25.6
-167	11	132.3	1545.	391.	188.	80.9
-199	9	148.5	3840.	393.	224.	92.7

TABLE 1. Running times for Bianchi groups

every real place but one. Let $\mathcal{O}$ be a maximal order in A. The Fuchsian group $\Gamma(\mathcal{O})$ has coarea $103.67\ldots$; our code computes a fundamental domain for this group in 13 minutes (735 seconds). The code provided by Magma and implementing the algorithm of [**Voi09**] computes a fundamental domain for $\Gamma(\mathcal{O})$ in 1 hour and 10 minutes (4204 seconds).

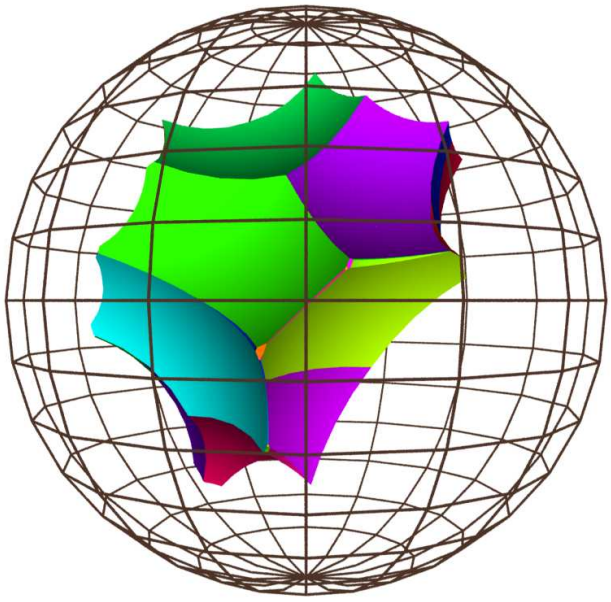

FIGURE 5. Dirichlet domain of $\mathbb{H}\Big/\Big(\mathbb{Z}\Big[\frac{1+\sqrt{-7}}{2}\Big]\Big)^1$

The Hamiltonians over $\mathbb{Z}\Big[\frac{1+\sqrt{-7}}{2}\Big]$. Consider the field $F = \mathbb{Q}(\sqrt{-7})$ and the quaternion division algebra $A = \Big(\frac{-1,-1}{F}\Big)$. Then $\mathcal{O} = \mathbb{Z}_F + \mathbb{Z}_F i + \mathbb{Z}_F j + \mathbb{Z}_F ij$ is a non-maximal order in A. A fundamental domain for this group was computed by

C. Corrales, E. Jespers, G. Leal and Á. del Río in [**CJLdR04**]. Using the method of Remark 3.2.6.2, our code can compute a fundamental domain for the group $\Gamma(\mathcal{O})$. It computes first a maximal order $\mathcal{O}' \supset \mathcal{O}$, and a fundamental domain for $\Gamma(\mathcal{O}')$ (having covolume $0.8889\ldots$). By coset enumeration, it finds that $\Gamma(\mathcal{O})$ has index 9 in the larger group, and computes a fundamental domain (Figure 5) for the initial group $\Gamma(\mathcal{O})$. The overall computation takes 15 seconds.

3.3. A larger example. Consider the ATR field F generated by an element t such that $t^{10} + 4t^9 - 18t^7 - 27t^6 + 26t^5 + 57t^4 - 2t^3 - 33t^2 - 10t + 1 = 0$, having discriminant $-546829505431 \simeq -5.5 \cdot 10^{11}$. Let A be the quaternion algebra $\left(\frac{a,b}{F}\right)$ where $a = \frac{1}{2}(-25t^9 - 82t^8 + 61t^7 + 404t^6 + 376t^5 - 932t^4 - 718t^3 + 590t^2 + 368t - 33)$ and $b = -1$. It is ramified exactly at the real places of F. Let $\mathcal{O}$ be a maximal order in A. The group $\Gamma(\mathcal{O})$ has covolume $1783.7\ldots$. Our code computes a fundamental domain for this group in 23 hours and 39 minutes (85150 seconds). It spends 5.3% of the time for enumeration, 5.8% for the routine KeepSameGroup, 87.7% for CheckPairing and 1.3% for computing the volume of the polyhedron. The fundamental domain has 5434 faces and 16252 edges.

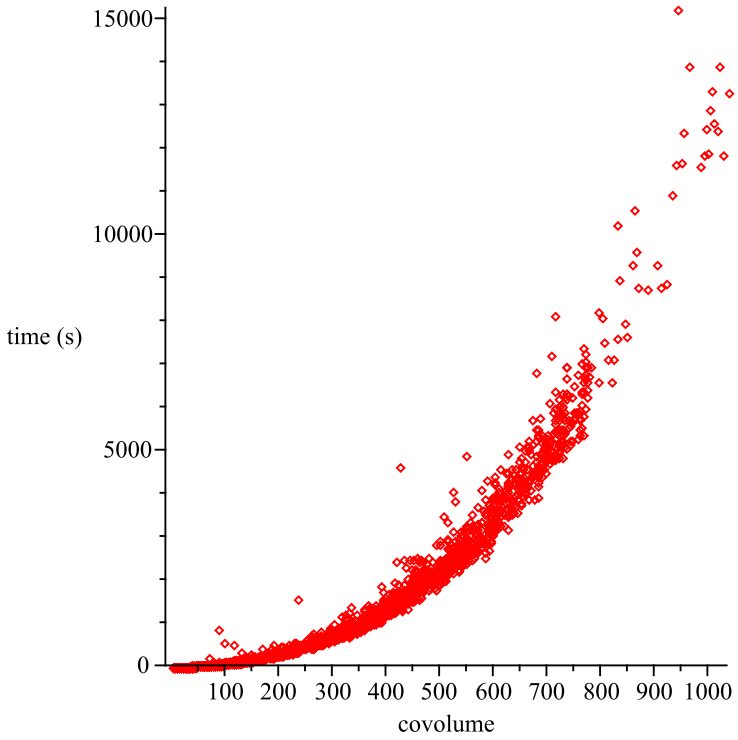

FIGURE 6. Running time of the algorithm

3.4. Efficiency of the algorithm. According to geometers, the parameter encoding the complexity of an arithmetic Kleinian group is the covolume. In practice it is simpler to vary the discriminant of the base field (and hence the degree) and

the norm of the discriminant of the quaternion algebra. It seems hard to estimate the running time of the algorithm in terms of these parameters. First, we do not know any bound on the radii of the isometric spheres containing the faces of the closure of the Dirichlet domain, or of generators of the group, so we do not know how many elements we have to enumerate. Then, even if we have generators of the group, we do not know how long the normalized basis algorithm could run before terminating (see also Remark 3.2.3.19).

We present numerical data obtained in a family. Since the running time increases very quickly with the discriminant of the field (since the volume increases like $|\Delta_F|^{3/2}$), we fixed the base field and varied the discriminant of the algebra. The field we chose is the ATR cubic field of discriminant -23. We computed groups $\Gamma(\mathcal{O})$ for every algebra with discriminant less than 10 000, and one algebra every ten with discriminant less than 15 000.

Analysis of this data shows that the running time is approximately proportional to the square of the covolume, with a few exceptionnally slow computations. We explain this as follows: in almost all cases, the enumeration appears to take negligible time, and the longest part is the computation of the fundamental domain itself; moreover the data (Figure 7) seem to indicate that the number of faces is proportional to the covolume (we have such a lower bound since the volume of a hyperbolic tetrahedron is bounded by $3\mathcal{L}(\frac{\pi}{3})$), and we know that our algorithm to compute the domain given the faces is quadratic.

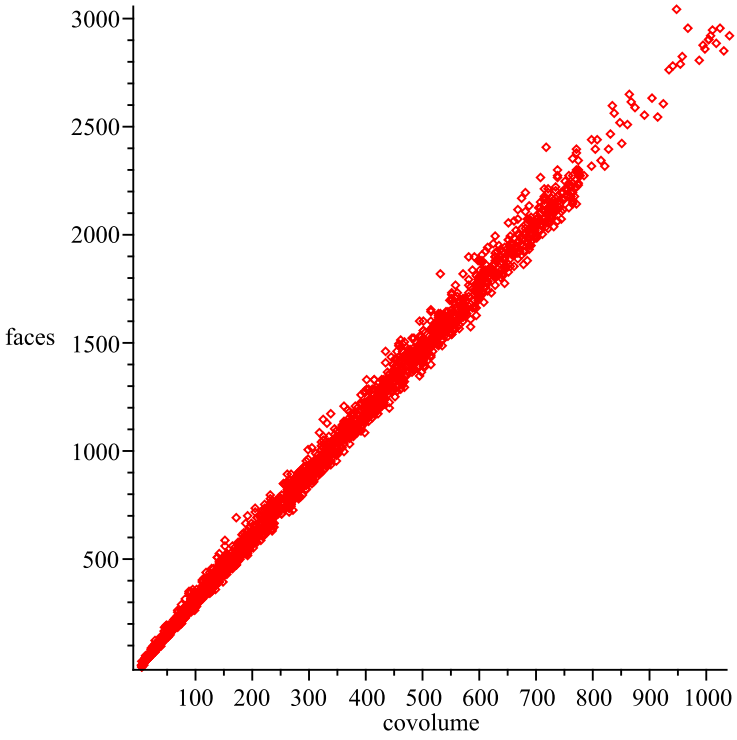

FIGURE 7. Number of faces of the closure of the Dirichlet domains

CHAPTER 4

The principal ideal problem

Automorphic forms and their Hecke eigenvalues are of tremendous importance in number theory. These eigenvalues carry a lot of interesting arithmetic information, such as the number of points on elliptic curves or traces of Frobenius in Galois representations. One of the most successful methods for computing automorphic forms for GL_2 over number fields uses the Jacquet-Langlands correspondence. This result transfers the problem to a quaternion algebra, in which it is often easier to solve. This approach has its roots in the theory of Brandt matrices and has been successfully used by Dembélé-Donnelly and Greenberg-Voight [**DV13**] to compute Hecke eigenvalues of Hilbert modular forms. In both methods, a crucial step is to test whether an ideal is principal and to produce a generator in this case: this is the *principal ideal problem* that we are considering in this chapter.

The principal ideal problem naturally splits into two cases: definite and indefinite algebras. In the definite case, Dembélé and Donnelly described an algorithm and Kirschmer and Voight proved that this algorithm runs in polynomial time when the base field is *fixed*, so we focus on the remaining indefinite case. In that case, testing whether an ideal is principal reduces to the same problem over the base field by Eichler's theorem (Theorem 1.1.2.4), but finding a generator is difficult. Kirschmer and Voight [**KV10**] provide an algorithm for quaternion algebras, that improves on naive enumeration[1], without analysing its complexity.

We present two algorithms for the principal ideal problem. The first one applies to any division algebra over $\mathbb{Q}$ and relies on the results of the last two chapters, and we can prove that it runs in time at most

$$\exp(O(d \log \Delta_A) + O_N(\log \log \Delta_A)).$$

The second one is an adaptation of Buchmann's algorithm [**Buc90**], and is heuristically subexponential.

1. Enumeration algorithms

Our first algorithm relies on the enumeration algorithms presented in Chapter 3. As with previous enumeration algorithms such as that of Kirschmer and Voight, it is based on the following simple observation.

LEMMA 4.1.0.1. *Let A be a central simple algebra over the number field F, let $\mathcal{O}$ be an order in A, let I be a right $\mathcal{O}$-ideal, and let $x \in I$. Then x is a generator of I if and only if* $\mathrm{nrd}(I) = \mathrm{nrd}(x)\mathbb{Z}_F$.

[1]Trying every linear combination of the basis elements until we find a generator.

PROOF. It is a necessary condition since $\mathrm{nrd}(x\mathcal{O}) = \mathrm{nrd}(x)\mathbb{Z}_F$. Conversely, if $\mathrm{nrd}(I) = \mathrm{nrd}(x)\mathbb{Z}_F$, let $J \subset I$. By the theory of projective modules over Dedekind rings, there exists $e_1, \dots, e_N$ an F basis of A, there exists $\mathfrak{a}_1, \dots, \mathfrak{a}_N$ and $\mathfrak{b}_1, \dots, \mathfrak{b}_n$ integral ideals of $\mathbb{Z}_F$ such that $I = \mathfrak{a}_1 e_1 + \dots + \mathfrak{a}_N e_N$ and $J = \mathfrak{a}_1\mathfrak{b}_1 e_1 + \dots + \mathfrak{a}_N\mathfrak{b}_N e_N$. Then $\mathrm{nrd}(I) = \mathrm{nrd}(J) = \mathfrak{b}_1 \dots \mathfrak{b}_N \mathrm{nrd}(I)$, so that $\mathfrak{b}_1 \dots \mathfrak{b}_N = \mathbb{Z}_F$, which implies $\mathfrak{b}_1 = \dots = \mathfrak{b}_N = \mathbb{Z}_F$ and finally $I = J$ as claimed. □

Given a generator λ of $\mathrm{nrd}(I)$, this lemma reduces the principal ideal problem to a norm equation, and it suffices to enumerate every element in I intersected with a fundamental domain for the action of $\mathcal{O}^1$ on the set of elements of norm λ. Again, we can estimate this set with Proposition 2.4.1.11. This leads to the following algorithm.

ALGORITHM 4.1.0.2 (`FindGenerator`).

Input: a right $\mathcal{O}$-ideal I for some maximal order $\mathcal{O}$ of a division algebra over $\mathbb{Q}$, and a generator λ of $\mathrm{nrd}(I)$ that is positive at every ramified real place.

Output: a generator x of I.

1: $R \leftarrow$ the bound of Proposition 2.4.1.11
2: choose an embedding ι
3: $X \leftarrow$ `MultipleQuadraticFormsEnum`(I, λ, R, ι) (Algorithm 3.1.1.12)
4: let $x \in X$
5: **return** x

REMARK 4.1.0.3. For the sake of simplicity we expressed the algorithm directly with Algorithm 3.1.1.12 that enumerates every element of norm λ, but we should really stop when we find the first element with norm λ.

THEOREM 4.1.0.4. *Given a right $\mathcal{O}$-ideal I for some maximal order $\mathcal{O}$ of a division algebra over $\mathbb{Q}$, and a generator λ of* $\mathrm{nrd}(I)$ *that is positive at every ramified real place, Algorithm 4.1.0.2 returns a generator x of I. It terminates in time at most*

$$\exp(O(d \log \Delta_A) + O_N(\log\log \Delta_A))$$

times a polynomial in the size of the input.

PROOF. By Eichler's theorem, the existence of λ implies that I is principal: $I = y\mathcal{O}$ for some $y \in I$. By Lemma 4.1.0.1, we have $\mathrm{nrd}(I) = \lambda\mathbb{Z}_F = \mathrm{nrd}(y)\mathbb{Z}_F$, so there exists $u \in \mathbb{Z}_F^\times$ such that $\lambda = \mathrm{nrd}(y)u$. Since $\mathrm{nrd}(y)$ and λ are positive at every real place that ramifies in A, so is u. By Eichler's theorem there exists $z \in \mathcal{O}^\times$ such that $\mathrm{nrd}(z) = u$. This gives $\mathrm{nrd}(yz) = \lambda$ and $yz \in I$, so by Proposition 2.4.1.11 at Step 4 the set X is nonempty and the instruction is valid. By Lemma 4.1.0.1 the output x is a generator of I.

Since we have

$$R \leq O(\log \Delta_A/d) + O_N(1)$$

and $|N_{F/\mathbb{Q}}(\lambda)|^d = N_{F/\mathbb{Q}}(\mathrm{nrd}(I))^d = N_{A/\mathbb{Q}}(I)$, the result follows from Proposition 3.1.1.13. □

We formulated the algorithm with λ given as an input so we could prove a complexity result without assuming anything on the complexity of the principal ideal problem in the base field. To get a complete algorithm, we first test whether $\mathrm{nrd}(I)$ is trivial in the class group $\mathrm{Cl}_A(F)(F)$ an compute a corresponding generator if it is, and then apply Algorithm 4.1.0.2.

2. Factor base algorithm

In this section, we present a probabilistic algorithm using a factor base and an auxiliary data structure to solve the principal ideal problem in indefinite quaterion algebras. Our algorithm is inspired by Buchmann's algorithm [**Buc90**] for computing the class group of a number field. However, it is not easy to adapt this technique to quaternion algebras. Indeed, the set of right ideals of an order does not form a group under multiplication. In fact, for most pairs of ideals, multiplication is not well-defined. We are able to salvage the factor base technique in the case of indefinite quaternion algebras by algorithmically realizing the strong approximation property (Theorem 1.1.2.2). The main point is that if every ideal were two-sided, Buchmann's method would work unchanged. Our algorithm is divided in two parts. Because the algebra is indefinite, every ideal is equivalent to an "almost two-sided" ideal: a local algorithm (Algorithm 4.2.1.9) makes this equivalence effective. The global algorithm (Algorithm 4.2.1.12) uses a factor base: by linear algebra it cancels out the valuations of the *norm* of the ideal and then corrects the ideal locally at every prime to make it two-sided. We implemented our algorithm in Magma. It performs well in practice, compared to the built-in Magma function implementing Kirschmer and Voight's algorithm.

The section is organized as follows. We first describe our algorithms in Section 2.1. In Section 2.1, we define local and global reduction structures and Algorithm 4.2.1.14, solving the principal ideal problem. In Section 2.1, Algorithm 4.2.1.19 constructs the needed local and global reduction structures: the first one uses units constructed from commutative suborders, and the second one is inspired by Buchmann's algorithm. In Section 2.1, we introduce a compact representation for quaternions to prevent coefficient explosion in the previous algorithms. Section 2.2 provides a complexity analysis of our algorithms: assuming suitable heuristics, we prove a subexponential running time. Section 3 presents examples.

2.1. Algorithms. We want to adapt the classical subexponential algorithms for computing the class group of a number field due to Hafner and McCurley [**HM89**] in the quadratic case and Buchmann [**Buc90**] in the general case to indefinite quaternion algebras by using a factor base: a fixed finite set of primes of $\mathbb{Z}_F$. To simplify the notations, we set $\Delta = \Delta_A$.

Definition 4.2.1.1. A *factor base* for A is a finite set $\mathcal{B}$ of primes of $\mathbb{Z}_F$ that generates the group $\mathrm{Cl}_A(F)$.

We say that a fractional ideal $\mathfrak{a}$ of F is $\mathcal{B}$-*smooth* or simply *smooth* if it is a product of the primes in $\mathcal{B}$. Let I be a right $\mathcal{O}$-ideal I. When I is integral, we say

that I is *smooth* if its reduced norm is. When I is arbitrary, it is *smooth* if it can be written $I = J\mathfrak{a}$ with $\mathfrak{a}$ a smooth fractional ideal of F and J an integral smooth right $\mathcal{O}$-ideal. Equivalently, the ideal I is smooth if and only if $I_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$ for all $\mathfrak{p} \notin \mathcal{B}$. An element $x \in A^\times$ is *smooth* if the ideal $x\mathcal{O}$ is smooth, or equivalently if $x \in \mathcal{O}_S^\times$ with $S = \mathcal{B}$.

We equip $\mathcal{M}_2(\mathbb{R})$ and $\mathcal{M}_2(\mathbb{C})$ with the usual positive definite quadratic form Q given by the sum of the squares of the absolute values of the coefficients, and we equip the Hamiltonian quaternion algebra $\mathbb{H}$ with the positive definite quadratic form $Q = \mathrm{nrd}$. For each infinite place of F represented by a complex embedding σ, we fix an isomorphism $\sigma' : A \otimes_F F_\sigma \cong M$ extending σ, where M is one of $\mathcal{M}_2(\mathbb{R})$, $\mathcal{M}_2(\mathbb{C})$ or $\mathbb{H}$. This defines a positive definite quadratic form $T_2 : A \otimes_\mathbb{Q} \mathbb{R} \to \mathbb{R}$ by setting $T_2(x) = \sum_\sigma [F_\sigma : \mathbb{R}] \cdot Q(\sigma'(x))$ for all $x \in A \otimes_\mathbb{Q} \mathbb{R}$, giving covolume $\Delta^{1/2}$ to the lattice $\mathcal{O}$. We represent a lattice in A by a $\mathbb{Z}_F$-pseudobasis (see [**KV10**]). When L is a lattice in A, we can enumerate its elements by increasing value of T_2 with the Kannan–Fincke–Pohst algorithm [**FP85, Kan83**]. We represent this enumeration with a routine `NextElement` that outputs a new element of L every time we call `NextElement`(L), ordering them by increasing value of T_2.

The reduction algorithms. In this section, we describe the reduction structures and the corresponding reduction algorithms. We start with the local reduction, which is an effective version of the fact that every integral right $\mathcal{O}$-ideal of norm $\mathfrak{p}^2$ is equivalent to the two-sided ideal $\mathfrak{p}\mathcal{O}$ (Theorem 1.1.2.4). We perform this reduction by making algorithmic the reduction theory of $\mathrm{SL}_2(F_\mathfrak{p})$ on the Bruhat-Tits tree $\mathcal{T}_\mathfrak{p}$ (Section 2.5). The connection between the Bruhat-Tits tree and ideals is the following: a right $\mathcal{M}_2(R)$-ideal is always principal, generated by an element of $\mathrm{GL}_2(F)$. Such an ideal is two-sided if and only if it is generated by an element of $F^\times \mathrm{GL}_2(R)$. So there is a $\mathrm{GL}_2(F)$-equivariant bijection between set of the vertices of the Bruhat-Tits tree and the quotient of the set of right $\mathcal{M}_2(R)$-ideals modulo the action of the group of two-sided $\mathcal{M}_2(R)$-ideals. The point is that the reduction procedure in $\mathcal{T}_\mathfrak{p}$ needs only a small number of units: this leads to the definition of the $\mathfrak{p}$-reduction structure.

Definition 4.2.1.2. Let $\mathfrak{p}$ be a prime that splits in A, let $\mathcal{O}_0 = \mathcal{O}$ and let P_0 be the fixed point of $\mathcal{O}_0^\times$ in the Bruhat-Tits tree $\mathcal{T}_\mathfrak{p}$. A $\mathfrak{p}$-*reduction structure* is given by the following data:

(i) the left order $\mathcal{O}_1$ of an integral right $\mathcal{O}$-ideal of norm $\mathfrak{p}$, and the fixed point P_1 of $\mathcal{O}_1^\times$ in $\mathcal{T}_\mathfrak{p}$;
(ii) for each $b \in \{0, 1\}$ and for each $P \in \mathcal{T}_\mathfrak{p}$ at distance 1 from P_b, an element $g \in \mathcal{O}_b^\times$ such that $g \cdot P = P_{1-b}$.

Such a structure exists by strong approximation (Theorem 1.1.2.2). Note that if I is an integral right $\mathcal{O}$-ideal of norm $\mathfrak{p}$ such that $\mathcal{O}_1 = \mathcal{O}_l(I)$, we have $I_\mathfrak{p} = x\mathcal{O}_\mathfrak{p}$ for some $x \in A^\times$, and $P_1 = x \cdot P_0$. We represent the points at distance 1 from P_b by elements of $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ and we compute the action on these points via explicit splitting maps $\iota_b : \mathcal{O}_b/\mathfrak{p}\mathcal{O}_b \to \mathcal{M}_2(\mathbb{F}_\mathfrak{p})$.

This structure provides everything we need to perform reduction in the Bruhat-Tits tree. The following algorithm corresponds to the standard reduction procedure (Theorem 1.2.5.1), which is illustrated in Figure 1. The idea is to use successive "rotations" (elements in $\mathrm{SL}_2(F_\mathfrak{p})$ having a fixed point in the tree) around the adjacent vertices P_0 and P_1 to send an arbitrary vertex to one of the vertices P_b: every rotation around a vertex decreases the distance to the other one.

To realize this procedure, we need to perform the following subtask: given a right $\mathcal{O}$-ideal I, find $x \in I$ such that $I_\mathfrak{p} = x\mathcal{O}_\mathfrak{p}$. A simple idea is to let $e = v_\mathfrak{p}(\mathrm{nrd}(J))$ and to draw elements $x \in J/\mathfrak{p}\mathcal{O}$ uniformly at random until $v_\mathfrak{p}(\mathrm{nrd}(x)) = e$. To obtain a deterministic algorithm, we can adapt Euclid's algorithm in the matrix ring $\mathcal{M}_2(\mathcal{R})$ with $\mathcal{R} = \mathbb{Z}_F/\mathfrak{p}^{e+1}$. This is done in [**San67**], except that the base ring $\mathcal{R}$ is assumed to be a domain. We adapt the argument to our case. First note that we have a well-defined $\mathfrak{p}$-adic valuation $v = v_\mathfrak{p}$ in the ring $\mathcal{R}$. Let $a, b \in \mathcal{R}$. We have $v(ab) \leq v(a) + v(b)$ whenever $ab \neq 0$, and $a \mid b$ if and only if $v(b) \geq v(a)$. If $a \neq 0$, there is a Euclidean division taking the following simple form: if $a \mid b$ then $b = a \cdot (b/a) + 0$, and otherwise $b = a \cdot 0 + b$. In every case we have written $b = aq + r$ with $r = 0$ or $v(r) < v(a)$. Adapting this in the matrix ring leads to the following Euclidean division algorithm, where for convenience we write $w = v \circ \det$. The idea is to work with A in Smith normal form, and if A is a diagonal matrix, dividing by A is almost the same as dividing by the diagonal coefficients. The difference is that we have to ensure that $\det(R) \neq 0$ unless $R = 0$.

Subalgorithm 4.2.1.3 (`DivideMatrix`).

Input: two matrices $A, B \in \mathcal{M}_2(\mathcal{R})$ with $\det A \neq 0$, where $\mathcal{R} = \mathbb{Z}_F/\mathfrak{p}^i$.

Output: two matrices $Q, R \in \mathcal{M}_2(\mathcal{R})$ such that $B = AQ + R$, and ($R = 0$ or $w(R) < w(A)$).

1: let $A' = UAV$ be the Smith form of A with $U, V \in \mathrm{SL}_2(\mathcal{R})$ and $A = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$
2: $B' \leftarrow UB$
3: let $B'' = B'W$ be the Hermite form of B' with $W \in \mathrm{SL}_2(\mathcal{R})$ and $B'' = \left(\begin{smallmatrix} c & 0 \\ e & f \end{smallmatrix}\right)$
4: **if** $a \mid c$ **then**
5: **if** $b \mid f$ **then**
6: **if** $b \mid e$ **then**
7: $Q \leftarrow \left(\begin{smallmatrix} c/a & 0 \\ e/b & f/b \end{smallmatrix}\right)$, $R \leftarrow \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$
8: **else**
9: $Q \leftarrow \left(\begin{smallmatrix} c/a & 1 \\ 0 & f/b \end{smallmatrix}\right)$, $R \leftarrow \left(\begin{smallmatrix} 0 & -a \\ e & 0 \end{smallmatrix}\right)$
10: **end if**
11: **else**
12: $Q \leftarrow \left(\begin{smallmatrix} c/a-1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $R \leftarrow \left(\begin{smallmatrix} a & 0 \\ e & f \end{smallmatrix}\right)$
13: **end if**
14: **else**
15: **if** $b \mid f$ **then**
16: $Q \leftarrow \left(\begin{smallmatrix} 0 & 0 \\ 0 & f/b-1 \end{smallmatrix}\right)$, $R \leftarrow \left(\begin{smallmatrix} c & 0 \\ e & b \end{smallmatrix}\right)$
17: **else**

18: $Q \leftarrow \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $R \leftarrow \left(\begin{smallmatrix} c & 0 \\ e & b \end{smallmatrix}\right)$
19: **end if**
20: **end if**
21: **return** VQW^{-1}, $U^{-1}RW^{-1}$

PROPOSITION 4.2.1.4. *Subalgorithm 4.2.1.3 is correct.*

PROOF. By case-by-case analysis, we have $B'' = A'Q + R$, and either $R = 0$ (Step 7) or $\det(R) \neq 0$ and $w(R) < w(A')$. Let $Q' = VQW^{-1}$ and $R' = U^{-1}RW^{-1}$ be the matrices returned by the algorithm. We have $B = U^{-1}B' = U^{-1}B''W^{-1} = U^{-1}(A'Q + R)W^{-1} = U^{-1}A'V^{-1}Q' + R' = AQ' + R'$. Since U, V and W have determinant 1, we have $R = 0$ if and only if $R' = 0$, and $w(R') = w(R) < w(A') = w(A)$, proving the correctness of the algorithm. □

SUBALGORITHM 4.2.1.5 (`GCDMatrix`).

Input: two matrices $A, B \in \mathcal{M}_2(\mathcal{R})$ with $\det A \neq 0$, where $\mathcal{R} = \mathbb{Z}_F/\mathfrak{p}^i$.
Output: a matrix D such that $A\mathcal{M}_2(\mathcal{R}) + B\mathcal{M}_2(\mathcal{R}) = D\mathcal{M}_2(\mathcal{R})$.
1: $Q, R \leftarrow$ `DivideMatrix`(A, B)
2: **if** $R = 0$ **then**
3: **return** A
4: **else**
5: **return** `GCDMatrix`(R, A)
6: **end if**

PROPOSITION 4.2.1.6. *Subalgorithm 4.2.1.5 is correct.*

PROOF. In Step 5 we have $\det(R) \neq 0$ by the properties of Subalgorithm 4.2.1.3, so the recursive call to `GCDMatrix` is valid. The rest of the proof is the same as with the usual Euclidean algorithm. □

SUBALGORITHM 4.2.1.7 (`LocalGenerator`).

Input: an integral right $\mathcal{O}$-ideal I and a prime $\mathfrak{p}$, for some maximal order $\mathcal{O}$.
Output: an element $x \in I$ such that $I_{\mathfrak{p}} = x\mathcal{O}_{\mathfrak{p}}$.
1: $b_1, \ldots, b_n \leftarrow$ an LLL-reduced $\mathbb{Z}$-basis of I
2: $e \leftarrow v_{\mathfrak{p}}(\mathrm{nrd}(b_1))$
3: $\mathcal{R} \leftarrow \mathbb{Z}_F/\mathfrak{p}^{e+1}$
4: $B_1, \ldots, B_n \leftarrow$ images of $b_1, \ldots, b_n$ in $\mathcal{M}_2(\mathcal{R})$
5: $D \leftarrow B_1$
6: **for** $i = 1$ to n **do**
7: $D \leftarrow$ `GCDMatrix`(D, B_i)
8: **end for**
9: let $\mu_1, \ldots, \mu_n \in \mathbb{Z}$ be such that $\sum \mu_i B_i = D$
10: **return** $\sum \mu_i b_i$

PROPOSITION 4.2.1.8. *Subalgorithm 4.2.1.7 is correct.*

PROOF. By definition of the norm of an ideal, we have $v_{\mathfrak{p}}(\mathrm{nrd}(I)) \leq v_{\mathfrak{p}}(\mathrm{nrd}(b_1)) = e$. Because of the choice of $\mathcal{R}$, at Step 5 we have $\det(D) \neq 0$, so the calls to

`GCDMatrix` are valid. By the properties of Subalgorithm 4.2.1.5, at Step 9 we have the relation $D\mathcal{M}_2(\mathcal{R}) = B_1\mathcal{M}_2(\mathcal{R}) + \cdots + B_1\mathcal{M}_2(\mathcal{R})$ so the integers $\mu_1, \ldots, \mu_n$ exist. Now let $x = \sum \mu_i b_i \in I$ be the output of the algorithm, so that $v_\mathfrak{p}(\mathrm{nrd}(x)) \leq e$, hence $\mathfrak{p}^{e+1}\mathcal{O}_\mathfrak{p} \subset x\mathcal{O}_\mathfrak{p}$. Let $y \in I_\mathfrak{p}$. By reduction modulo $\mathfrak{p}^{e+1}$ there exists $a \in \mathcal{O}_\mathfrak{p}$ and $b \in \mathfrak{p}^{e+1}\mathcal{O}$ such that $y = xa + b \in x\mathcal{O}_\mathfrak{p}$, proving the result. □

Now we can present the local reduction algorithm.

Subalgorithm 4.2.1.9 (`PReduce`).

Input: an integral right $\mathcal{O}$-ideal I, a prime $\mathfrak{p}$ and a $\mathfrak{p}$-reduction structure.

Output: an integer r, an element $c \in A^\times$ and an integral $\mathcal{O}$-ideal J such that $cI = J\mathfrak{p}^r$ and $v_\mathfrak{p}(\mathrm{nrd}(J)) \in \{0, 1\}$.

1: $r \leftarrow$ largest integer such that $I \subset \mathcal{O}\mathfrak{p}^r$, $J \leftarrow I\mathfrak{p}^{-r}$
2: $k \leftarrow v_\mathfrak{p}(\mathrm{nrd}(J))$
3: $c \leftarrow 1$, $b \leftarrow 0$
4: $x \leftarrow$ `LocalGenerator`$(I, \mathfrak{p})$
5: $Q \leftarrow x \cdot P_0$
6: **repeat**
7: $\quad P \leftarrow$ point at distance 1 from P_b in the segment P_bQ
8: $\quad (c, J, Q) \leftarrow g \cdot (c, J, Q)$ where $g \in \mathcal{O}_b^\times$ is such that $g \cdot P = P_{1-b}$
9: $\quad$ **if** $b = 1$ **then** $J \leftarrow J\mathfrak{p}^{-1}$, $r \leftarrow r + 1$, $k \leftarrow k - 2$ **end if**
10: $\quad b \leftarrow 1 - b$
11: **until** $k < 2$
12: **return** J, c, r

In Step 1, we have $2r = v_\mathfrak{p}(\mathrm{nrd}(\mathfrak{I}))$ where $\mathfrak{I}$ is the two-sided $\mathcal{O}$-ideal generated by I. We can compute $\mathfrak{I}$ as follows: if $w_1, \ldots, w_n$ is a $\mathbb{Z}$-basis of $\mathcal{O}$ and $b_1, \ldots, b_n$ is a $\mathbb{Z}$-basis of I, then $\mathfrak{I} = \sum_{i,j} \mathbb{Z} w_i b_j$.

Proposition 4.2.1.10. *Subalgorithm 4.2.1.9 is correct.*

Proof. Since k decreases by 2 every two iterations and is positive by the loop condition, the algorithm terminates. We now prove that the output is correct.

First, the distance $d(P_b, Q)$ decreases by 1 during each execution of the loop: before Step 8, we have $d(P_{1-b}, gQ) = d(gP, gQ) = d(P, Q) = d(P_b, Q) - 1$ since P is at distance 1 from P_b on the segment P_bQ. We claim that before or after a complete execution of the loop, we have $d(P_0, Q) = k$ (see Figure 1). The claim is true before the first iteration: we have $x \in \mathcal{O} \smallsetminus \mathfrak{p}\mathcal{O}$ so $d(P_0, Q) = d(P_0, xP_0) = v_\mathfrak{p}(\mathrm{nrd}(x)) = v_\mathfrak{p}(\mathrm{nrd}(J)) = k$. We only need to prove that the equality $d(P_0, Q) = k$ is preserved when $b = 1$. In that case, P_1 is in the segment P_0Q because of the previous iteration, so that $d(P_0, Q) = 1 + d(P_1, Q) = k$.

We now prove that before or after a complete execution of the loop, the $\mathcal{O}$-ideal J is integral and $v_\mathfrak{p}(\mathrm{nrd}(J)) = k$. This property clearly holds before the first iteration. Before Step 9, after two iterations $b = 0$ and $b = 1$, J and Q have been multiplied by an element h such that $v_\mathfrak{p}(\mathrm{nrd}(h)) = 0$ and $d(P_0, hQ) = d(P_0, Q) - 2$, so hJ is divisible by $\mathfrak{p}$. Step 9 hence preserves integrality and updates k according to the valuation of $\mathrm{nrd}(J)$.

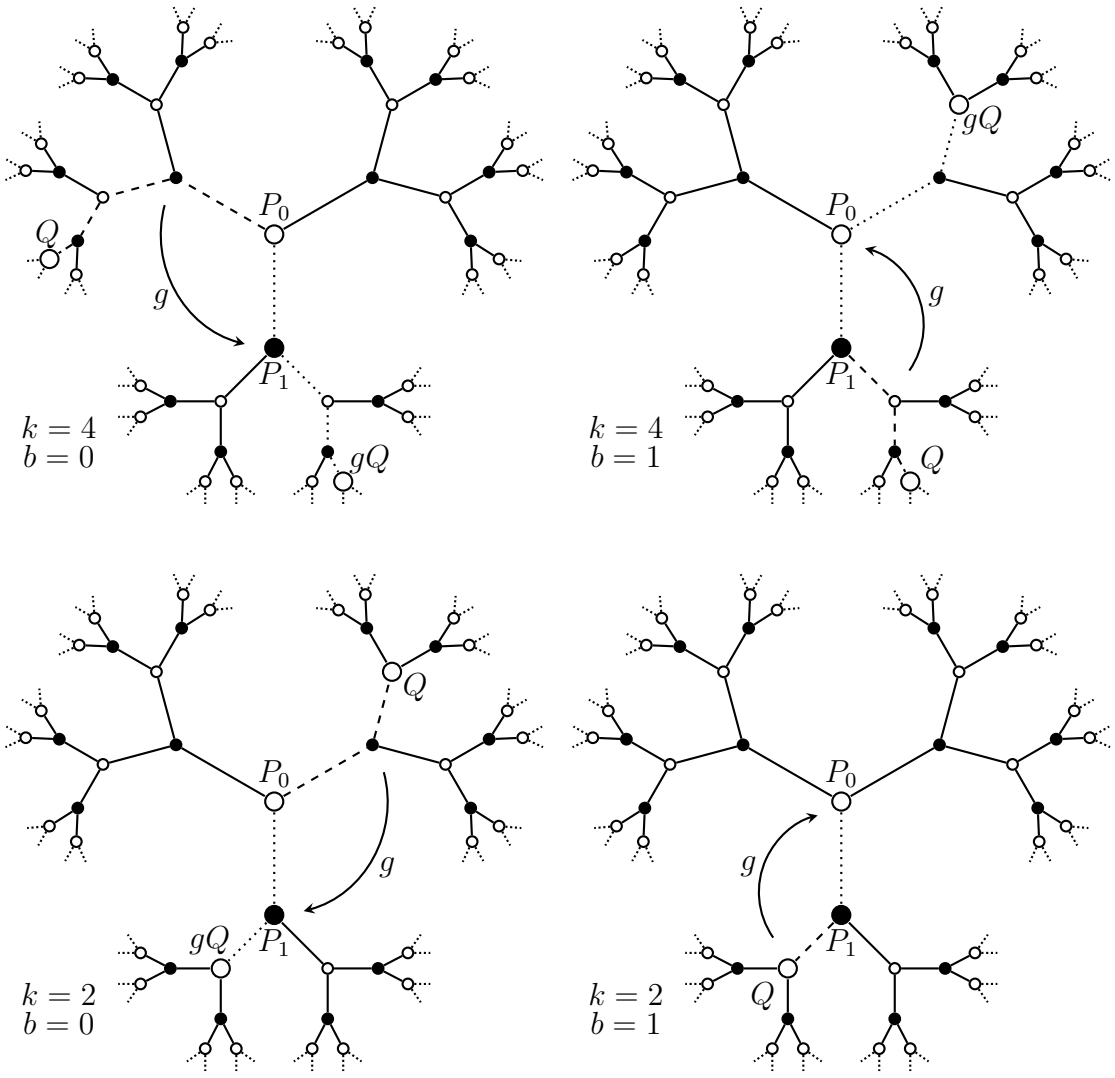

FIGURE 1. `PReduce` (Subalgorithm 4.2.1.9)

We now prove the proposition. The element c is a product of elements of $\mathcal{O}_0^\times$ and $\mathcal{O}_1^\times$ so c is a $\mathfrak{p}$-unit with $\mathrm{nrd}(c) \in \mathbb{Z}_F^\times$. We have just proved that J is integral, and by Step 9 the value of r is such that $cI = J\mathfrak{p}^r$. Because of the loop condition, after the algorithm terminates we have $v_\mathfrak{p}(\mathrm{nrd}(J)) = k \in \{0, 1\}$. □

We now explain how to perform global reduction. We use linear algebra to control the valuations of a smooth ideal and then perform local reduction at every prime to get an "almost two-sided ideal". The first step is similar to its commutative analogue: we need sufficiently many "relations" (smooth elements in $A^\times$) so that the quotient of the factor base by the norms of the relations is the ray class group $\mathrm{Cl}_A(F)$. This leads to the definition of a G-reduction structure.

DEFINITION 4.2.1.11. A *G-reduction structure* is given by the following data:

(i) a $\mathfrak{p}$-reduction structure for each $\mathfrak{p} \in \mathcal{B}$ that splits in A;
(ii) a finite set of elements $X \subset \mathcal{O} \cap A^\times$ and a map $\phi : \mathrm{Cl}_A(F) \to \langle \mathcal{B} \rangle$ that is a lift of an isomorphism $\mathrm{Cl}_A(F) \xrightarrow{\sim} \langle \mathcal{B} \rangle / \langle \mathrm{nrd}(X) \rangle$ and such that $\phi(1) = \mathbb{Z}_F$.

The following algorithm performs global reduction. In order to avoid explosion of the size of the ideal in the local reduction, we extract the two-sided part, allowing us to reduce all exponents modulo 2. The remaining part stays small and gets $\mathfrak{p}$-reduced, while the two-sided part is only multiplied by powers of primes.

Subalgorithm 4.2.1.12 (`GReduce`).

Input: a smooth integral right $\mathcal{O}$-ideal I and a G-reduction structure.
Output: an integral ideal J, an element $c \in A^\times$ and a two-sided ideal $\mathfrak{I}$ such that $cI = J\mathfrak{I}$ and I is principal if and only if $J = \mathcal{O}$ and $\mathfrak{I} = \mathcal{O}$.

1: $\mathfrak{a} \leftarrow \mathrm{nrd}(I)$
2: $\mathfrak{b} \leftarrow \phi(\mathfrak{a})$ where $\mathfrak{a}$ is seen as an element of $\mathrm{Cl}_A(F)$
3: let $e \in \mathbb{Z}^X$ be such that $\mathrm{nrd}(y)\mathfrak{a} = \mathfrak{b}$ where $y = \prod_{x \in X} x^{e_x}$.
4: $c \leftarrow \prod_{x \in X} x^{e_x \bmod 2}$, $f \leftarrow \prod_{x \in X} \mathrm{nrd}(x)^{\lfloor e_x/2 \rfloor}$ {Extract two-sided part}
5: $J \leftarrow cI$
6: $\mathfrak{I} \leftarrow$ two-sided ideal generated by J
7: $J \leftarrow J\mathfrak{I}^{-1}$ {Extract two-sided part}
8: $\mathfrak{I} \leftarrow f\mathfrak{I}$
9: **for** $\mathfrak{p} \in \mathcal{B}$ dividing $\mathrm{nrd}(J)$ and splitting in A **do**
10: $\quad J, c', r \leftarrow$ `PReduce`$(J, \mathfrak{p})$
11: $\quad c \leftarrow c'c$, $\mathfrak{I} \leftarrow \mathfrak{p}^r\mathfrak{I}$
12: **end for**
13: **return** $J, cf, \mathfrak{I}$

Proposition 4.2.1.13. *Subalgorithm 4.2.1.12 is correct.*

Proof. Since Step 7 and `PReduce` preserve integrality (Proposition 4.2.1.10), the output J is integral. The relation $cI = J\mathfrak{I}$ is clear by tracking the multiplications. If the output is such that $J = \mathcal{O}$ and $\mathfrak{I} = \mathcal{O}$, then $I = c^{-1}\mathcal{O}$ is principal. Conversely, if I is principal, then $\mathfrak{a} = \mathrm{nrd}(I)$ is trivial in the class group $\mathrm{Cl}_A(F)$ so $\mathfrak{b} = \phi(\mathrm{cl}(\mathfrak{a})) = \mathbb{Z}_F$. After Step 5, we have $\mathrm{nrd}(J) = f^{-2}\mathbb{Z}_F$. After Step 7, we have multiplied J by a two-sided ideal, so $v_\mathfrak{p}(\mathrm{nrd}(J))$ is even for all primes $\mathfrak{p}$ splitting in A. Since J is not divisible by a two-sided ideal, $\mathrm{nrd}(J)$ is not divisible by primes that ramify in A. We obtain $J = \mathcal{O}$ at the end of the loop by the properties of `PReduce` so $\mathrm{nrd}(\mathfrak{I}) = \mathbb{Z}_F$. Since $\mathfrak{I}$ is two-sided, it is entirely determined by its norm so $\mathfrak{I} = \mathcal{O}$. □

Finally, we reduce the general case to the smooth case by the noncommutative analogue of standard randomizing techniques. We generate a random smooth $\mathcal{O}$-ideal by the following procedure, to which we refer as `RandomLeftIdeal`$(\mathcal{O})$. For each $\mathfrak{p} \in \mathcal{B}$, pick a nonnegative integer k. Let $\iota : \mathcal{O} \to \mathcal{M}_2(\mathbb{Z}_F/\mathfrak{p}^k)$ be a splitting map. Let $M \in \mathcal{M}_2(\mathbb{Z}_F/\mathfrak{p}^k)$ be a random upper-triangular matrix with zero determinant and compute $R_\mathfrak{p} = \mathcal{O}\iota^{-1}(M) + \mathfrak{p}^k\mathcal{O}$. Finally, return $\bigcap_\mathfrak{p} R_\mathfrak{p}$. Choose the exponents k such that $\mathcal{N}(R) \approx \Delta$.

It not clear at the moment what the best distribution for the exponents is. A simpler idea would be to use random products $\prod_{\mathfrak{p}} \mathfrak{p}^{k_{\mathfrak{p}}}$. In our experience, this leads to poorly randomized ideals. This is clear in the case $F = \mathbb{Q}$: the randomized ideals are simply integer multiples of $\mathcal{O}$.

ALGORITHM 4.2.1.14 (`IsPrincipal`).
Input: an integral right $\mathcal{O}$-ideal I and a G-reduction structure.
Output: an integral ideal J, an element $c \in A^\times$ and a two-sided ideal $\mathfrak{I}$ such that $cfI = J\mathfrak{I}$ and I is principal if and only if $J = \mathcal{O}$ and $\mathfrak{I} = \mathcal{O}$.
1: $R \leftarrow$ `RandomLeftIdeal`$(\mathcal{O})$
2: $x \leftarrow$ `NextElement`$(I^{-1} \cap R)$
3: **if** xI is not smooth **then return FAIL end if**
4: $J, c, \mathfrak{I} \leftarrow$ `GReduce`(xI)
5: **return** $J, cx, \mathfrak{I}$

By Proposition 4.2.1.13, if Algorithm 4.2.1.14 does not return FAIL, its output is correct. In practice, we repeat Algorithm 4.2.1.14 until it returns the result.

Building the reduction structures. Now we explain how to build the previous reduction structures. The local reduction structure needs units in $\mathcal{O}$. In general it is difficult to compute the whole unit group $\mathcal{O}^\times$: for instance in the Fuchsian case, the minimal number of generators is at least $\Delta^{3/8+o(1)}$ (this follows from the theory of signatures of Fuchsian groups [**Kat92**, Section 4.3] and a volume formula [**MR03**, Theorem 11.1.1]), which makes it hopeless to find a subexponential method. However, we can find some units in $\mathcal{O}$ by considering commutative suborders and computing generators of their unit group with Buchmann's algorithm. Heuristically, these units are sufficiently random for our purpose. This strategy is implemented by the following algorithms.

SUBALGORITHM 4.2.1.15 (`P1Search`).
Input: a maximal order $\mathcal{O}$ and a prime $\mathfrak{p}$.
Output: a set of elements $X \subset \mathcal{O}^\times$ acting transitively on $\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$.
1: $X \leftarrow \emptyset$
2: **repeat**
3: $\quad x \leftarrow$ `NextElement`$(\mathcal{O})$
4: $\quad L \leftarrow F(x)$
5: $\quad$ **if** L/F has positive relative unit rank **then**
6: $\quad\quad \mathcal{R} \leftarrow \mathbb{Z}_L \cap \mathcal{O}$
7: $\quad\quad X \leftarrow X \cup$ a set of generators of $\mathcal{R}^\times$
8: $\quad$ **end if**
9: **until** X acts transitively on $\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$
10: **return** X

In Step 7, we can compute the unit group $\mathcal{R}^\times$ with the algorithms of Klüners and Pauli [**KP05**]. Note that we actually do not need the full group $\mathcal{R}^\times$: a subgroup of finite index is sufficient.

PROPOSITION 4.2.1.16. *Subalgorithm 4.2.1.15 is correct.*

PROOF. By strong approximation (Theorem 1.1.2.2), the group $\mathcal{O}^\times$ acts transitively on $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$. This group is finitely generated, so after finitely many iterations we will have enumerated a set of generators and the algorithm will terminate. By the loop condition, the output is correct. □

SUBALGORITHM 4.2.1.17 (`PBuild`).

Input: a maximal order $\mathcal{O}$ and a prime $\mathfrak{p}$.
Output: a $\mathfrak{p}$-reduction structure.

1: $I \leftarrow$ an integral right $\mathcal{O}$-ideal of norm $\mathfrak{p}$
2: $\mathcal{O}_1 \leftarrow \mathcal{O}_l(I)$
3: $X \leftarrow \texttt{P1Search}(\mathcal{O}, \mathfrak{p})$
4: from X, for each P at distance 1 from P_0 compute an element $g \in \mathcal{O}^\times$ such that $g \cdot P = P_1$
5: $X \leftarrow \texttt{P1Search}(\mathcal{O}_1, \mathfrak{p})$
6: from X, for each P at distance 1 from P_1 compute an element $g \in \mathcal{O}_1^\times$ such that $g \cdot P = P_0$
7: **return** the $\mathfrak{p}$-reduction structure

REMARK 4.2.1.18. Let $g, g' \in \mathcal{O}^\times$ be such that $g \cdot P_1 = g' \cdot P_1$ and let $h = g^{-1}g'$. Then $h \cdot P_1 = P_1$ so $h \in \mathcal{O}^\times \cap \mathcal{O}_1^\times$. This allows us to construct many elements in $\mathcal{O}_1^\times$ before Step 5. If we have sufficiently many such units, which often happens in practice, they will act transitively on the points $P \neq P_0$ at distance 1 from P_1. In this case, in Step 5 we will only need to find one element $g \in \mathcal{O}_1^\times$ such that $g \cdot P_0 \neq P_0$.

We build the global reduction structure in a way similar to the commutative case: we look for small relations in smooth ideals. In addition, we have a good starting point thanks to the inclusion $\mathbb{Z}_F \subset \mathcal{O}$: the units $\mathbb{Z}_{F,\mathcal{B}}^\times$ provide all the relations up to a 2-elementary Abelian group.

ALGORITHM 4.2.1.19 (`GBuild`).

Input: a maximal order $\mathcal{O}$ and a factor base $\mathcal{B}$.
Output: a G-reduction structure.

1: **for** $\mathfrak{p} \in \mathcal{B}$ that splits in A **do**
2: $\quad \texttt{PBuild}(\mathcal{O}, \mathfrak{p})$
3: **end for**
4: $X \leftarrow$ integral generators of $\mathbb{Z}_{F,\mathcal{B}}^\times$
5: **for** $\mathfrak{p} \in \mathcal{B}$ **do**
6: $\quad I \leftarrow$ integral $\mathcal{O}$-ideal of norm $\mathfrak{p}$
7: $\quad$ **repeat**
8: $\quad\quad x \leftarrow \texttt{NextElement}(I)$
9: $\quad$ **until** x is smooth
10: $\quad X \leftarrow X \cup \{x\}$
11: **end for**
12: **function** $\langle \mathcal{B} \rangle / \langle \mathrm{nrd}(X) \rangle \ncong \mathrm{Cl}_A(F)$ **do**
13: $\quad x \leftarrow \texttt{NextElement}(\mathcal{O})$

14: **if** x is smooth **then** $X \leftarrow X \cup \{x\}$ **end if**
15: **end function**
16: **return** the G-reduction structure

REMARK 4.2.1.20. The various calls to `PBuild` in Step 2 are not completely independent: we can keep the elements in $\mathcal{O}^\times$ from one call for other ones.

PROPOSITION 4.2.1.21. *Algorithm 4.2.1.19 is correct.*

PROOF. Let I be the ideal in Step 6. There exists a smooth ideal J equivalent to I, let $x \in A^\times$ be such that $I = xJ$. Then $x\mathcal{O} = IJ^{-1}$, so $\mathrm{nrd}(J)x \in I\bar{J} \subset I$ is smooth. It will be enumerated at some point, so the loop starting at Step 7 terminates. Since $\mathcal{B}$ generates the class group $\mathrm{Cl}_A(F)$, by Eichler's theorem (Theorem 1.1.2.4) we have $\langle\mathcal{B}\rangle/\mathrm{nrd}(A^\times) \cong \mathrm{Cl}_A(F)$, so there exists a finite set of $\mathcal{B}$-smooth elements $X \subset \mathcal{O}$ such that $\langle\mathcal{B}\rangle/\langle\mathrm{nrd}(X)\rangle \cong \mathrm{Cl}_A(F)$. We will enumerate this set at some point, so the loop starting at Step 12 terminates. So Algorithm 4.2.1.19 terminates, and by Proposition 4.2.1.16 and Step 12 it returns a correct G-reduction structure. □

REMARK 4.2.1.22. We have restricted to maximal orders to simplify the exposition, but this restriction can be weakened as follows. Let $\mathcal{O}$ be an arbitrary order, and let S be the set of primes $\mathfrak{p}$ of $\mathbb{Z}_F$ such that $\mathcal{O}$ is not $\mathfrak{p}$-maximal. The set S is finite, so we can choose a factor basis disjoint from S. Then our algorithms work unchanged for right $\mathcal{O}$-ideals except for one point: Theorem 1.1.2.4 characterizing principal ideals might no longer hold. If we restrict to Eichler orders, that is intersections of two maximal orders, Theorem 1.1.2.4 still holds. Otherwise we need to find the suitable class group and change Definition 4.2.1.11 ii accordingly.

Compact representations. In the previous algorithms, the cost of elementary operations is important. Representing units as linear combinations of basis elements of $\mathcal{O}$ could be catastrophic: the classical example of real quadratic fields suggests that fundamental units in commutative orders, such as those produced by Subalgorithm 4.2.1.15, can have exponential size. This problem is classically circumvented by representing units in *compact form*: a product of small S-units with possibly large exponents. The problem is reduced to computing efficiently with those compact representations. A natural notion of compact representation in $\mathcal{O}$ would be to take ordered products of S-units in $\mathcal{O}$ but we do not know how to compute efficiently with such a general representation. Instead we use a more restrictive notion: we group the units belonging to a common commutative suborder, in which we can compute efficiently. This leads to the following definition.

DEFINITION 4.2.1.23. A *compact representation* in $\mathcal{O}$ is:

(i) an element $x \in \mathcal{O}$, or
(ii) a product $y = \prod_{i=1}^{r} y_i^{e_i}$ where the exponents are signed integers, the elements y_i all lie in a single ring $\mathcal{R} \subset \mathcal{O}$ containing $\mathbb{Z}_F$ and such that $y \in \mathcal{R}^\times$, together with a $\mathbb{Z}$-basis of the integral closure of $\mathcal{R}$ and a factorization of its conductor, or

(iii) an ordered product of compact representations.

A product y as in ii will be called a *representation of type ii*.

We describe the algorithms for representations of type ii, and they naturally extend by multiplicativity to arbitrary compact representations. We first explain the algorithm for local evaluation of compact representations. Since the product represents a unit, we can replace it with a product of local units, avoiding loss of precision despite the large exponents.

SUBALGORITHM 4.2.1.24 (`EvalCR`).

Input: a representation $y = \prod_{i=1}^{r} y_i^{e_i} \in \mathcal{R}$ of type ii, an ideal $\mathfrak{a} \subset \mathbb{Z}_F$.
Output: an element $z \in \mathcal{O}$ such that $z = y \pmod{\mathfrak{a}\mathcal{O}}$.

1: $L \leftarrow$ field of fractions of $\mathcal{R}$
2: $\mathfrak{f} \leftarrow$ conductor of $\mathcal{R}$ inside $\mathbb{Z}_L$
3: $\prod_{j=1}^{k} \mathfrak{P}_j^{w_j} \leftarrow$ factorization of $\mathfrak{a}\mathfrak{f}\mathbb{Z}_L$
4: **for** $j = 1$ to k **do**
5: $\quad \phi \leftarrow$ reduction map onto $\mathbb{Z}_L/\mathfrak{P}_j^{w_j}$
6: $\quad \pi \leftarrow$ uniformizer in $\mathfrak{P}_j$, $v \leftarrow v_{\mathfrak{P}_j}$
7: $\quad z_j \leftarrow \prod_{i=1}^{r} \phi(y_i \pi^{-v(y_i)})^{e_i}$
8: **end for**
9: $z \leftarrow$ element in $\mathbb{Z}_L$ such that $z = z_j \pmod{\mathfrak{P}_j^{w_j}}$
10: **return** z

PROPOSITION 4.2.1.25. *Subalgorithm 4.2.1.24 is correct.*

PROOF. First, we claim that for all $j \leq k$, we have $z_j = y \pmod{\mathfrak{P}_j^{w_j}}$. Since the norm $\mathrm{nrd}(y)$ is in $\mathbb{Z}_F^\times$, we have $\sum_{i=1}^{r} v(y_i)e_i = 0$ so we get

$$\prod_{i=1}^{r} (y_i \pi^{-v(y_i)})^{e_i} = \prod_{i=1}^{r} \pi^{-v(y_i)e_i} \prod_{i=1}^{r} y_i^{e_i} = y.$$

Since $y_i \pi^{-v(y_i)}$ is integral at $\mathfrak{P}_j$, we can apply ϕ to it and the claim follows. This implies that the output z of the algorithm satisfies $z = y \pmod{\mathfrak{a}\mathfrak{f}\mathbb{Z}_L}$. In particular, we have $z = y \pmod{\mathfrak{f}\mathbb{Z}_L}$ so $z - y \in \mathcal{R}$. Since $y \in \mathcal{R}$ we get $z \in \mathcal{R} \subset \mathcal{O}$. The relation $\mathfrak{a}\mathfrak{f}\mathbb{Z}_L \subset \mathfrak{a}\mathcal{R} \subset \mathfrak{a}\mathcal{O}$ shows that $z = y \pmod{\mathfrak{a}\mathcal{O}}$. □

We can now explain how to multiply an ideal by a compact representation. To know an ideal, it suffices to know it up to large enough precision: we reduce the problem to local evaluation.

SUBALGORITHM 4.2.1.26 (`MulCR`).

Input: a representation $y = \prod_{i=1}^{r} y_i^{e_i} \in \mathcal{R}$ of type ii, an integral right $\mathcal{O}$-ideal I.
Output: the ideal yI.

1: $\mathfrak{a} \leftarrow \mathrm{nrd}(I)$
2: $z \leftarrow \mathtt{EvalCR}(y, \mathfrak{a})$
3: **return** $zI + \mathfrak{a}\mathcal{O}$

PROPOSITION 4.2.1.27. *Subalgorithm 4.2.1.26 is correct.*

PROOF. By Proposition 4.2.1.25, we have $z = y \pmod{\mathfrak{a}\mathcal{O}}$ so $(z-y)I \subset (z-y)\mathcal{O} \subset \mathfrak{a}\mathcal{O}$, which gives $zI + \mathfrak{a}\mathcal{O} = yI + \mathfrak{a}\mathcal{O}$. Since $y \in \mathcal{O}^\times$, we have $\mathrm{nrd}(yI) = \mathrm{nrd}(I) = \mathfrak{a}$, so $\mathfrak{a}\mathcal{O} \subset yI$ and finally $yI + \mathfrak{a}\mathcal{O} = yI$. Therefore the output of the algorithm is correct. □

2.2. Complexity analysis. We perform a complete complexity analysis of our algorithms, assuming suitable heuristics. To simplify the notations, we set $L(x) = \exp(\sqrt{\log x \log\log x})$. In every complexity estimate, the degree of the base field F is fixed. When we mention a complexity of the form $L(\Delta)^{O(1)}$, we always implicitly mean $L(\Delta)^{O(1)}$ times a polynomial in the size of the input. We fix a parameter $\alpha > 0$. We will analyse our algorithm using the general paradigm that with a factor base of subexponential size, elements have a subexponential probability of being smooth. However, recall from Definition 4.2.1.1 that the factor base $\mathcal{B}$ is assumed to generate the ray class group $\mathrm{Cl}_A(F)$, so we need the following heuristic.

HEURISTIC 4.2.2.1. There exists a constant $c = c_\alpha$ such that for every quaternion algebra A with absolute discriminant Δ, the set of primes having norm less than $c \cdot L(\Delta)^\alpha$ generates the class group $\mathrm{Cl}_A(F)$.

This heuristic is a theorem under the Generalized Riemann Hypothesis [**Bac90**]. By Minkowski's bound, Heuristic 4.2.2.1 is also true unconditionnally with the restriction that $\log\Delta \gg_\alpha (\log|\Delta_F|)^2$. From now on, we assume Heuristic 4.2.2.1 and we assume that the factor base $\mathcal{B}$ is the set of primes having norm less than $c \cdot L(\Delta)^\alpha$. Note that this implies the bound $\#\mathcal{B} \leq L(\Delta)^{\alpha+o(1)}$.

We start by analysing the complexity of elementary operations: Subalgorithm 4.2.1.7 and the algorithms of Section 2.1.

LEMMA 4.2.2.2. *Subalgorithm 4.2.1.7 terminates in time polynomial in the size of the input.*

PROOF. Subalgorithm 4.2.1.3 (`DivideMatrix`) is made of a constant number of elementary operations, so it is polynomial. In Subalgorithm 4.2.1.5 (`GCDMatrix`) with $\mathcal{R} = \mathbb{Z}_F/\mathfrak{p}^i$, since the valuation of the determinant decreases at every recursive call, there are at most i such calls. When Subalgorithm 4.2.1.7 (`LocalGenerator`) calls Subalgorithm 4.2.1.5, we have $i = e + 1 = v_\mathfrak{p}(\mathrm{nrd}(b_1)) + 1 = O(\log\mathcal{N}(I))$ by lattice reduction. So the algorithm is polynomial in the size of the input. □

LEMMA 4.2.2.3. *Given the factorization of $\mathfrak{a}$, Subalgorithm 4.2.1.24 terminates in time polynomial in the size of the input. Given the factorization of $\mathrm{nrd}(I)$, Subalgorithm 4.2.1.24 terminates in time polynomial in the size of the input.*

PROOF. In Subalgorithm 4.2.1.24, the number of iterations of the loop is polynomial in the size of the input. The only operations that could possibly not be polynomial in the size of the input are the computation of $\mathbb{Z}_L$ and the factorization of $\mathfrak{a}\mathfrak{f}\mathbb{Z}_L$, but $\mathbb{Z}_L$ and the factorization of $\mathfrak{f}$ are contained in the compact representation, and the factorization of $\mathfrak{a}$ is assumed to be given. So the algorithm is polynomial in the size of its input. Since the HNF of the output can be computed in polynomial time [**BF12**], Subalgorithm 4.2.1.24 is also polynomial. □

The restriction on the factorization is not a problem in our application: every ideal on which we call these algorithms is smooth.

Since our algorithms use their commutative counterparts, we have to make assumptions on the algorithms used to compute commutative unit groups.

HEURISTIC 4.2.2.4. There is an explicit algorithm that, given a number field K with discriminant Δ_K, an order $\mathcal{R}$ in K and a bound $b = L(\Delta_K)^{O(1)}$, computes a set U of integral generators for the S-unit group of $\mathbb{Z}_K$, where S is the set of primes of norm less than b, and generators for the unit group $\mathcal{R}^\times$ expressed as products of elements in U, in expected time $L(\Delta_K)^{O(1)}$.

This is a strong hypothesis. However, under the Generalized Riemann Hypothesis it is a theorem for quadratic number fields [**HM89, Vol02**] and experience has shown that it is not an unreasonable assumption[2].

Since the reduction algorithms depend on the structures that are given as input, we analyse the algorithms building the reduction structures before the reduction algorithms. We start with Subalgorithm 4.2.1.15, for which we need some heuristic assumptions.

HEURISTICS 4.2.2.5. In Subalgorithm 4.2.1.15, we assume the following.

(i) If F is totally real, a positive proportion of x satisfies the condition of Step 5 that $F(x)/F$ has positive relative unit rank.
(ii) The images in $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{p})$ of the units produced at Step 7 are uniformly distributed in the image of $\mathcal{O}^\times$ in $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{p})$.

PROPOSITION 4.2.2.6. *Assuming Heuristics 4.2.2.4 and 4.2.2.5, the expected running time of Subalgorithm 4.2.1.15 is at most* $L(\Delta)^{O(1)}$.

PROOF. We first prove that the expected number of iterations of the loop is $O(1)$. If F is not totally real, the relative unit rank condition is always satisfied, so by Heuristic 4.2.2.5 (i) a positive proportion of the iterations of the loop produce a unit. By strong approximation, the image of $\mathcal{O}^\times$ in $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{p})$ contains $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$, and the index is at most 2. By Heuristic 4.2.2.5 (ii), with probability at least $1/2$ the image of the unit produced at Step 7 is in $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$, and the corresponding images are equidistributed in $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$. By [**KL90**], the probability that two random elements of $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$ generate this group is bounded below by a constant. Therefore, after an expected number of iterations $O(1)$, the image of X generates $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$ and hence acts transitively on $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$.

Each computation of a unit group in Step 7 takes expected time $L(\Delta)^{O(1)}$ by Heuristic 4.2.2.4 since the discriminant of $\mathbb{Z}_F[x]$ is $\Delta^{O(1)}$. The units are stored in

[2]The PARI developers experimented extensively with this algorithm in the past twenty years, as implemented in the PARI/GP function `bnfinit`, while building and checking tables of number fields of small degree [Ref: `http://pari.math.u-bordeaux1.fr/pub/pari/packages/nftables/`], as well as with number fields of much larger degree. E.g. the class group and unit group of $F = \mathbb{Q}[t]/(t^{90} - t^2 - 1)$, $d_F > 10^{175}$ can be computed in a few hours (Karim Belabas, personal communication).

compact representation and we use Subalgorithm 4.2.1.24 (`EvalCR`) to compute the action on $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$, so by Lemma 4.2.2.3 this takes total time $L(\Delta)^{O(1)}$. □

HEURISTICS 4.2.2.7. Let $\mathbb{Z}_{F,\mathcal{B},A}^\times$ be the group of $\mathcal{B}$-units in $\mathbb{Z}_F$ that are positive at every real place ramified in A. In Algorithm 4.2.1.19, we assume the following.

(i) There exists a constant $\beta > 0$ such that the elements x produced in Steps 8 and 13 are smooth with probability at least $L(\Delta)^{-\beta+o(1)}$.
(ii) The norms of the smooth elements produced in Step 13 are equidistributed in $\mathbb{Z}_{F,\mathcal{B},A}^\times/\mathbb{Z}_{F,\mathcal{B}}^{\times 2}$.

By comparison with the case of integers [**Gra08**, Equation (1.16) and Section 1.3], $\beta = 1/(2\alpha)$ could be a reasonable value.

THEOREM 4.2.2.8. *Assume Heuristics 4.2.2.4, 4.2.2.5, 4.2.2.1 and 4.2.2.7. Then, given a maximal order $\mathcal{O}$ in an indefinite quaternion algebra A, Algorithm 4.2.1.19 (`GBuild`) terminates in expected time $L(\Delta)^{O(1)}$.*

PROOF. There are $2 \cdot \#\mathcal{B} = L(\Delta)^{O(1)}$ calls to Subalgorithm 4.2.1.15 (`P1Search`). By Proposition 4.2.2.6, these calls take total time $L(\Delta)^{O(1)}$. The computation of the group $\mathbb{Z}_{F,\mathcal{B}}^\times$ takes time $L(\Delta_F)^{O(1)} = L(\Delta)^{O(1)}$ by Heuristic 4.2.2.4. By Heuristic 4.2.2.7 (i), the expected number of iterations in the loop starting at Step 7 is at most $L(\Delta)^{O(1)}$ for each $\mathfrak{p} \in \mathcal{B}$, so the total expected number of iterations of this loop is at most $\#\mathcal{B} \cdot L(\Delta)^{O(1)} = L(\Delta)^{O(1)}$.

We study the loop starting at Step 12. After Step 4, we have $\langle\mathcal{B}\rangle/\langle\mathrm{nrd}(X)\rangle = \langle\mathcal{B}\rangle/\mathbb{Z}_{F,\mathcal{B}}^{\times 2}$. Let C be the group $\mathbb{Z}_{F,\mathcal{B},A}^\times/\mathbb{Z}_{F,\mathcal{B}}^{\times 2}$. There is an exact sequence

$$1 \longrightarrow C \longrightarrow \langle\mathcal{B}\rangle/\mathbb{Z}_{F,\mathcal{B}}^{\times 2} \longrightarrow \mathrm{Cl}_A(F) \longrightarrow 1,$$

so that the loop terminates if and only if the image of $\mathrm{nrd}(X)$ generates the group C. We have $\#C = 2^{\#\mathcal{B}+O(1)}$, so by Heuristic 4.2.2.7 (ii) this happens after we find an expected number of $\#\mathcal{B} + O(1)$ smooth elements. By Heuristic 4.2.2.7 (i), the total expected number of iterations of this loop is at most $\#\mathcal{B} \cdot L(\Delta)^{O(1)} = L(\Delta)^{O(1)}$. Checking the loop condition $\langle\mathcal{B}\rangle/\langle\mathrm{nrd}(X)\rangle \ncong \mathrm{Cl}_A(F)$ amounts to linear algebra, so it also takes time $L(\Delta)^{O(1)}$. This proves the theorem. □

THEOREM 4.2.2.9. *Assume Heuristics 4.2.2.4, 4.2.2.5, 4.2.2.1 and 4.2.2.7. Then, given the G-reduction structure computed by Algorithm 4.2.1.19 and a smooth integral right $\mathcal{O}$-ideal I, Algorithm 4.2.1.12 (`GReduce`) terminates in expected time $L(\Delta)^{O(1)}$.*

PROOF. First, since by Theorem 4.2.2.8, Algorithm 4.2.1.19 terminates in expected time $L(\Delta)^{O(1)}$. In particular the expected size of its output is also at most $L(\Delta)^{O(1)}$. In Subalgorithm 4.2.1.12 (`GReduce`), the first part is linear algebra, which is polynomial in the size of the input, so it takes time $L(\Delta)^{O(1)}$. By Lemma 4.2.2.3, all the elementary operations can be performed in time polynomial in the size of their input.

We analyse the calls to Subalgorithm 4.2.1.9 (`PReduce`). In this subalgorithm, the variable k decreases by 2 every two iterations and the initial value of k is bounded by $v_\mathfrak{p}(\mathrm{nrd}(J))$, so the algorithm terminates after at most $v_\mathfrak{p}(\mathrm{nrd}(J))$ iterations by the

loop condition. So the total number of iterations in the calls to Subalgorithm 4.2.1.9 is bounded by $\sum_{\mathfrak{p}\in\mathcal{B}} v_{\mathfrak{p}}(\mathrm{nrd}(J)) \leq \log_2 \mathcal{N}(J) \leq \log_2(N_X \cdot \mathcal{N}(I))$ by Step 5 of Subalgorithm 4.2.1.12, where $N_X = \prod_{x\in X} \mathcal{N}(x)$. But $\log \mathcal{N}(I)$ is polynomial in the size of the input and $\log N_X$ is polynomial in the size of the G-reduction structure, which is $L(\Delta)^{O(1)}$. This proves the theorem. □

Finally, for a general integral right $\mathcal{O}$-ideal, repeated attempts with Algorithm 4.2.1.14 (`IsPrincipal`) takes total expected time $L(\Delta)^{O(1)}$ if we assume the following heuristic.

Heuristic 4.2.2.10. There exists a constant $\gamma > 0$ such that in Step 3 of Algorithm 4.2.1.14, the element x is smooth with probability at least $L(\Delta)^{-\gamma+o(1)}$.

Again, by comparison with the case of integers [**Gra08**], $\gamma = 1/(\sqrt{2}\alpha)$ could be a reasonable value.

3. Examples

We have implemented the above algorithms in the computer algebra system Magma [**BCP97**]. In this section, we demonstrate how our algorithms work and perform in practice. Every computation was performed on a 2.5 GHz Intel Xeon E5420 processor with Magma v2.20-5 from the PLAFRIM experimental testbed.

Example 1. Let A be the quaternion algebra over $\mathbb{Q}$ generated by two elements i, j such that $i^2 = 3$, $j^2 = -1$ and $ij = -ji$. The algebra A is ramified at 2 and 3 and unramified at every other place: A is indefinite and our method applies. Let $\mathcal{O}$ be the maximal order $\mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\omega$ where $\omega = (1+i+j+ij)/2$. We construct a reduction structure with Algorithm 4.2.1.19 (`GBuild`) and factor base $\mathcal{B} = \{2, 3, 5, 7, 11, 13, 17\}$. Let $I = 19\mathcal{O} + a\mathcal{O}$ where $a = -3 - 4i + j$, so that $\mathrm{nrd}(I) = 19\mathbb{Z}$. We use Algorithm 4.2.1.14 (`IsPrincipal`) to compute a generator of I. It finds an element $x = (7+i-9j-3\omega)/19 \in I^{-1}$ such that $\mathrm{nrd}(xI) = 7\mathbb{Z}$, so that xI is smooth. The linear algebra phase in Subalgorithm 4.2.1.12 (`GReduce`) computes $c = -1-2i-j+\omega$ having norm -7 and $f = 1/7$. We obtain $J = 49\mathcal{O}+b\mathcal{O}$ with $b = -17 - 8i + j$ and $\mathfrak{I} = 7^{-1}\mathcal{O}$ before the local reduction. We reduce the ideal J at 7. In Subalgorithm 4.2.1.9 (`PReduce`), at the first iteration we have $P = P_1$ so $c = 1$. In the second iteration we have $c = (-9 - 5i - 7j - 3\omega)/7$: the element c has norm 1 and $r = 1$. After multiplying every element, we obtain the output $c = 7/19 \cdot (8 + 4i + 3j - 11\omega)$, $f = 1/7$ and $x = (cf)^{-1} = 3 + 4i - 3j - 11\omega$ has norm -19: x is a generator of the ideal I.

Example 2. Let F be the complex cubic field of discriminant -23, which is generated by an element t such that $t^3 - t + 1 = 0$. Let A be the quaternion algebra over F generated by two elements i, j such that $i^2 = 2t^2 + t - 3$, $j^2 = -5$ and $ij = -ji$. The algebra A is ramified at the real place of F and the discriminant δ_A has norm 5. All the maximal orders in A are conjugate and we compute one of them with Magma. Algorithm 4.2.1.19 (`GBuild`) constructs the reduction structure in 4 seconds. We then compute the 22 primes of F coprime to δ_A and having norm less than 100. For every such prime $\mathfrak{p}$, we construct a random integral right

$\mathcal{O}$-ideal I with norm $\mathfrak{p}$. Since $\mathrm{Cl}_A(F)$ is trivial, they are all principal. We apply Algorithm 4.2.1.14 (`IsPrincipal`) to compute a generator of each of these ideals. This computation takes 0.3 seconds per ideal on average with a maximum of 0.9 seconds. As a comparison, we compute generators for the same ideals with the function provided by Magma. This computation takes 4 hours per ideal on average with a maximum of 69h, and 5 of the 23 ideals take less that 0.1 seconds.

Example 3. When the base field is totally real and the algebra is ramified at every real place except one, there is an algorithm of Voight [**Voi09**] for computing the unit group of an order. In [**DV13**, p. 25], Dembélé and Voight mention but do not describe an unpublished algorithm using this computation to speedup ideal principalization. This algorithm is provided in Magma[3] and improves on the algorithm of [**KV10**]. Let F be the real cubic field of discriminant $3132 = 2^2 \cdot 3^3 \cdot 29$, which is generated by an element t such that $t^3 - 15t + 6 = 0$. Let A be the quaternion algebra over F generated by two elements i, j such that $i^2 = -1$, $j^2 = (141t^2 + 57t - 2092)/2$ and $ij = -ji$. The algebra A is ramified at two of the three real places of F and no finite place. We compute a maximal order in A and then construct the reduction structure in 14 seconds. We produce a random integral ideal of norm $\mathfrak{p}$ for each prime $\mathfrak{p}$ having norm less than 100 and compute a generator for each of them with our algorithm. The computation takes 1.5 seconds per ideal on average with a maximum of 4.6 seconds. With Magma we compute the unit group $\mathcal{O}^\times$ in 8 minutes and then compute generators for the same ideals with the units-assisted algorithm [**DV13**, p. 25] provided by Magma. The computation takes 1 hour per ideal on average with a maximum of 17h, and 10 of the 23 ideals take less that 0.5 seconds. Magma tends to return smaller generators than our algorithm. Magma is fast whenever there exists a small generator and our algorithm is faster when this is not the case.

Example 4. In order to understand the practical behaviour of the algorithms, we conduct the following experiment. We draw algebras A and ideals I at random[4]. In every random test case, we compute our reduction structure with Algorithm 4.2.1.19 (`GBuild`), and we compute a generator of the ideal I with Algorithm 4.2.1.14 (`IsPrincipal`). We also compute a generator of I with the function provided by Magma. In every case, we interrupt any algorithm that takes more than 1000 seconds to terminate. The result of 15 000 such test cases is plotted in

[3] `IsPrincipal(<Any> I, <GrpPSL2> Gamma) -> BoolElt, AlgQuatElt`

[4] Let x be uniformly distributed in $[0, 70]$. This value controls the size of the discriminant. Let k be 1 or 2, each with probability $1/2$. This is the number of prime factors of the discriminant of the algebra. Let t be uniformly distributed in $[0, 1]$. This value controls the part of the size of the discriminant coming from the base field or from the algebra. Let d be the smallest fundamental discriminant larger that $\exp(tx/4)$, and let $F = \mathbb{Q}(\sqrt{d})$. Let $\mathfrak{p}_1$ be the prime of $\mathbb{Z}_F$ with smallest norm larger than $\exp((1-t)x/2k)$, and if $k = 2$ let $\mathfrak{p}_2$ be the prime with smallest norm larger than $N(\mathfrak{p}_1)$. Let A be the quaternion algebra ramified exactly at $\mathfrak{p}_i$ for $i \leq k$ and at $k \bmod 2$ real places of F, and let $\mathcal{O}$ be a maximal order in A. Let $\Delta = d^4 N(\delta_A)^2$ be the absolute discriminant of A. Let y be uniformly distributed in $[0, 1]$, and let $\mathfrak{p}$ be the prime of $\mathbb{Z}_F$ of smallest norm larger than $y\Delta^{1/2}$, coprime to δ_A and such that the class of $\mathfrak{p}$ in $\mathrm{Cl}_A(F)$ is trivial. Finally, let I be a random integral right $\mathcal{O}$-ideal of norm $\mathfrak{p}$.

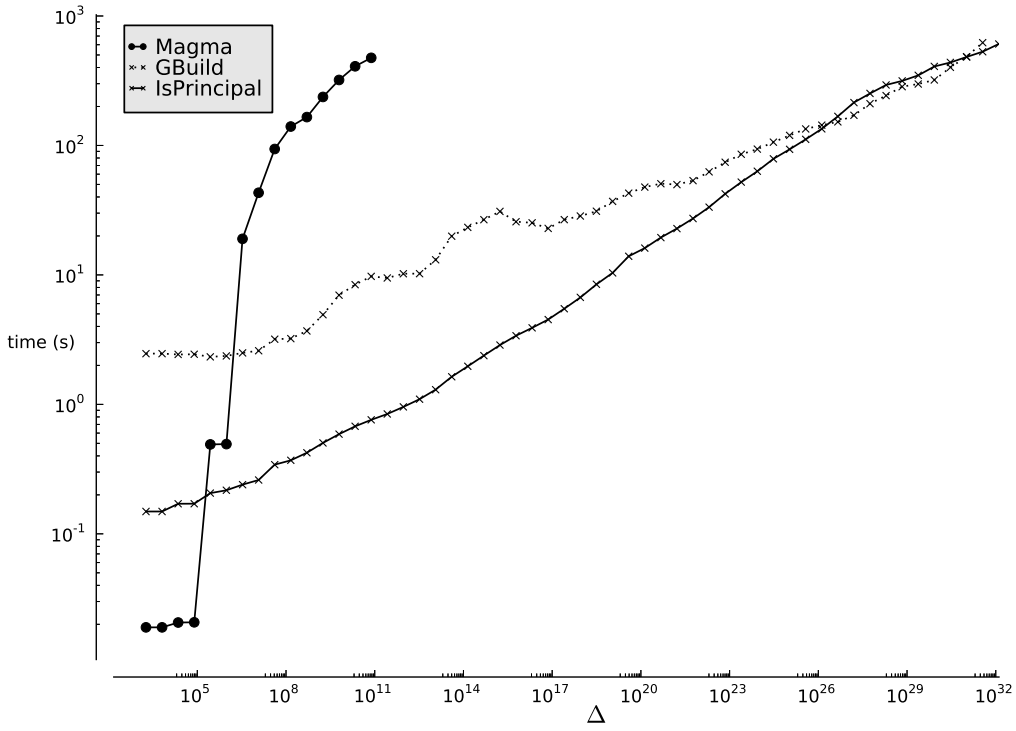

FIGURE 2. Running time of the algorithms

Figure 2: the discriminant Δ and the time are both in logarithmic scale, and each plot (D, T) is such that T is the average of the running time of the algorithm over the discriminants $\Delta \in [D/10, 10D]$. We do not plot the running time when more than 50% of the executions were interrupted, since the corresponding value is no longer meaningful.

Bibliography

[AGM11] Avner Ash, Paul E. Gunnells, and Mark McConnell. Torsion in the cohomology of congruence subgroups of $\mathrm{SL}(4,\mathbb{Z})$ and Galois representations. *J. Algebra*, 325:404–415, 2011.

[Bac90] Eric Bach. Explicit bounds for primality testing and related problems. *Math. Comp.*, 55(191):355–380, 1990.

[BB11] Valentin Blomer and Farrell Brumley. On the Ramanujan conjecture over number fields. *Ann. of Math. (2)*, 174(1):581–605, 2011.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BdlHV08] Bachir Bekka, Pierre de la Harpe, and Alain Valette. *Kazhdan's property (T)*, volume 11 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2008.

[Bel04] Karim Belabas. Topics in computational algebraic number theory. *J. Théor. Nombres Bordeaux*, 16(1):19–63, 2004.

[Bel05] Karim Belabas. L'algorithmique de la théorie algébrique des nombres. In *Théorie algorithmique des nombres et équations diophantiennes*, pages 85–155. Ed. Éc. Polytech., Palaiseau, 2005.

[BF12] Jean-François Biasse and Claus Fieker. A polynomial time algorithm for computing the HNF of a module over the integers of a number field. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, pages 75–82. ACM, 2012.

[BH96] Yuri Bilu and Guillaume Hanrot. Solving Thue equations of high degree. *J. Number Theory*, 60(2):373–392, 1996.

[Bla06] Don Blasius. Hilbert modular forms and the Ramanujan conjecture. In *Noncommutative geometry and number theory*, Aspects Math., E37, pages 35–56. Vieweg, Wiesbaden, 2006.

[Bor81] A. Borel. Commensurability classes and volumes of hyperbolic 3-manifolds. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 8(1):1–33, 1981.

[BR13] Ethan Berkove and Alexander Rahm. The mod 2 cohomology rings of SL_2 of the imaginary quadratic integers. July 2013.

[Bro92] Robert Brooks. Some relations between spectral geometry and number theory. In *Topology '90 (Columbus, OH, 1990)*, volume 1 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 61–75. de Gruyter, Berlin, 1992.

[BS91] M. Burger and P. Sarnak. Ramanujan duals. II. *Invent. Math.*, 106(1):1–11, 1991.

[Buc90] Johannes Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. In *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, pages 27–41. Birkhäuser Boston, Boston, MA, 1990.

[CE75] Jeff Cheeger and David G. Ebin. *Comparison theorems in Riemannian geometry*. North-Holland Publishing Co., Amsterdam-Oxford; American Elsevier Publishing Co., Inc., New York, 1975. North-Holland Mathematical Library, Vol. 9.

[CFJR01] Ted Chinburg, Eduardo Friedman, Kerry N. Jones, and Alan W. Reid. The arithmetic hyperbolic 3-manifold of smallest volume. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 30(1):1–40, 2001.

[CFO+11] John Cremona, Tom Fisher, Cathy O'Neil, Denis Simon, and Michael Stoll. Explicit n-descent on elliptic curves. iii. algorithms. *arXiv preprint arXiv:1107.3516*, 2011.

[CGY97] F. R. K. Chung, A. Grigor′yan, and S.-T. Yau. Eigenvalues and diameters for manifolds and graphs. In *Tsing Hua lectures on geometry & analysis (Hsinchu, 1990–1991)*, pages 79–105. Int. Press, Cambridge, MA, 1997.

[CJLdR04] Capi Corrales, Eric Jespers, Guilherme Leal, and Angel del Río. Presentations of the unit group of an order in a non-split quaternion algebra. *Adv. Math.*, 186(2):498–524, 2004.

[Clo03] Laurent Clozel. Démonstration de la conjecture τ. *Invent. Math.*, 151(2):297–328, 2003.

[CN13] Renaud Coulangeon and Gabriele Nebe. Maximal finite subgroups and minimal classes. *arXiv preprint arXiv:1304.2597*, 2013.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[Coh00] Henri Cohen. *Advanced topics in computational number theory*, volume 193. Springer, 2000.

[CS12] Ted Chinburg and Matthew Stover. Small generators for S-unit groups of division algebras. *arXiv preprint arXiv:1204.5968*, 2012.

[CV12] Frank Calegari and Akshay Venkatesh. A torsion Jacquet–Langlands correspondence. *arXiv preprint arXiv:1212.3847*, 2012.

[DV13] Lassina Dembélé and John Voight. Explicit methods for Hilbert modular forms. In *Elliptic curves, Hilbert modular forms and Galois deformations*, Adv. Courses Math. CRM Barcelona, pages 135–198. Birkhäuser/Springer, Basel, 2013.

[Ebe96] Patrick B. Eberlein. *Geometry of nonpositively curved manifolds*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1996.

[FP85] U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Math. Comp.*, 44(170):463–471, 1985.

[Gel11] Tsachik Gelander. Volume versus rank of lattices. *J. Reine Angew. Math.*, 661:237–248, 2011.

[GGH+13] Herbert Gangl, Paul E Gunnells, Jonathan Hanke, Achill Schürmann, Mathieu Dutour Sikiric, and Dan Yasaki. On the cohomology of linear groups over imaginary quadratic fields. *arXiv preprint arXiv:1307.1165*, 2013.

[GHY13] Paul E. Gunnells, Farshid Hajir, and Dan Yasaki. Modular forms and elliptic curves over the field of fifth roots of unity. *Exp. Math.*, 22(2):203–216, 2013. With an appendix by Mark Watkins.

[GMcS14] Xavier Guitart, Marc Masdeu, and Mehmet Haluk ¸Sengün. Darmon points on elliptic curves over number fields of arbitrary signature. *arXiv preprint arXiv:1404.6650*, 2014.

[Gra08] Andrew Granville. Smooth numbers: computational number theory and beyond. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 267–323. Cambridge Univ. Press, Cambridge, 2008.

[GS80] F. Grunewald and D. Segal. Some general algorithms. I: Arithmetic groups. *Annals of Mathematics*, 112(3):531–583, 1980.

[GS85] Fritz Grunewald and Daniel Segal. Decision problems concerning S-arithmetic groups. *J. Symbolic Logic*, 50(3):743–772, 1985.

[Gün60] Paul Günther. Einige Sätze über das Volumenelement eines Riemannschen Raumes. *Publ. Math. Debrecen*, 7:78–93, 1960.

[GY08] Paul E. Gunnells and Dan Yasaki. Hecke operators and Hilbert modular forms. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 387–401. Springer, Berlin, 2008.

[GY13] Paul E. Gunnells and Dan Yasaki. Modular forms and elliptic curves over the cubic field of discriminant -23. *Int. J. Number Theory*, 9(1):53–76, 2013.

[Hid81] Haruzo Hida. On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves. *Amer. J. Math.*, 103(4):727–776, 1981.

[HM89] James L. Hafner and Kevin S. McCurley. A rigorous subexponential algorithm for computation of class groups. *J. Amer. Math. Soc.*, 2(4):837–850, 1989.

[HS00] Marc Hindry and Joseph H Silverman. *Diophantine geometry: an introduction*, volume 201. Springer, 2000.

[HS07] Guillaume Hanrot and Damien Stehlé. Improved analysis of Kannan's shortest lattice vector algorithm (extended abstract). In *Advances in cryptology—CRYPTO 2007*, volume 4622 of *Lecture Notes in Comput. Sci.*, pages 170–186. Springer, Berlin, 2007.

[Jah10] Majid Jahangiri. Generators of arithmetic quaternion groups and a Diophantine problem. *Int. J. Number Theory*, 6(6):1311–1328, 2010.

[JL70] H. Jacquet and R. P. Langlands. *Automorphic forms on* GL(2). Lecture Notes in Mathematics, Vol. 114. Springer-Verlag, Berlin-New York, 1970.

[Kan83] Ravi Kannan. Improved algorithms for integer programming and related lattice problems. In *Proceedings of the fifteenth annual ACM symposium on Theory of computing*, STOC '83, pages 193–206, New York, NY, USA, 1983. ACM.

[Kat92] Svetlana Katok. *Fuchsian groups*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1992.

[KL90] William M. Kantor and Alexander Lubotzky. The probability of generating a finite classical group. *Geom. Dedicata*, 36(1):67–87, 1990.

[Kna01] Anthony W. Knapp. *Representation theory of semisimple groups*. Princeton Landmarks in Mathematics. Princeton University Press, Princeton, NJ, 2001. An overview based on examples, Reprint of the 1986 original.

[KP05] Jürgen Klüners and Sebastian Pauli. Computing residue class rings and Picard groups of orders. *J. Algebra*, 292(1):47–64, 2005.

[KV10] Markus Kirschmer and John Voight. Algorithmic enumeration of ideal classes for quaternion orders. *SIAM J. Comput.*, 39(5):1714–1747, 2010.

[Len92] H. W. Lenstra, Jr. Algorithms in algebraic number theory. *Bull. Amer. Math. Soc. (N.S.)*, 26(2):211–244, 1992.

[Lip02] M. Lipyanskiy. A computer-assisted application of Poincaré's fundamental polyhedron theorem. Preprint available at `http://www.math.columbia.edu/~ums/Archive.html`, 2002.

[LMR00] Alexander Lubotzky, Shahar Mozes, and M. S. Raghunathan. The word and Riemannian metrics on lattices of semisimple groups. *Inst. Hautes Études Sci. Publ. Math.*, (91):5–53 (2001), 2000.

[LOB12] Laura Luzzi, Ghaya Rekaya-Ben Othman, and Jean-Claude Belfiore. Algebraic reduction for the golden code. *Adv. Math. Commun.*, 6(1):1–26, 2012.

[LPS88] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[Lub10] Alexander Lubotzky. *Discrete groups, expanding graphs and invariant measures*. Modern Birkhäuser Classics. Birkhäuser Verlag, Basel, 2010. With an appendix by Jonathan D. Rogawski, Reprint of the 1994 edition.

[Mas71] Bernard Maskit. On Poincaré's theorem for fundamental polygons. *Advances in Math.*, 7:219–230, 1971.

[MR03] Colin Maclachlan and Alan W. Reid. *The arithmetic of hyperbolic 3-manifolds*, volume 219 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2003.

[Oh02] Hee Oh. Uniform pointwise bounds for matrix coefficients of unitary representations and applications to Kazhdan constants. *Duke Math. J.*, 113(1):133–192, 2002.

[Pag10] A. Page. Computing fundamental domains for arithmetic Kleinian groups. Master's thesis, Université Paris 7, Aug 2010.

[Pag13] A. Page. Computing arithmetic kleinian groups. *Math. Comp.*, 2013. In press, preprint available at the url `http://arxiv.org/abs/1206.0087`.

[Pag14] Aurel Page. An algorithm for the principal ideal problem in indefinite quaternion algebras. *arXiv preprint arXiv:1405.6674*, 2014.

[PAR14] The PARI Group, Bordeaux. *PARI/GP, version `2.7.0`*, 2014. available from `http://pari.math.u-bordeaux.fr/`.

[PR94] Vladimir Platonov and Andrei Rapinchuk. *Algebraic groups and number theory*, volume 139 of *Pure and Applied Mathematics*. Academic Press Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen.

[Pra89] Gopal Prasad. Volumes of S-arithmetic quotients of semi-simple groups. *Inst. Hautes Études Sci. Publ. Math.*, (69):91–117, 1989. With an appendix by Moshe Jarden and the author.

[Rah10] Alexander Rahm. *(Co)homologies et K-théorie de groupes de Bianchi par des modèles géométriques calculatoires*. Phd thesis, Université Joseph-Fourier - Grenoble I, October 2010.

[Rah13] Alexander D. Rahm. Higher torsion in the Abelianization of the full Bianchi groups. *LMS J. Comput. Math.*, 16:344–365, 2013.

[Rat06] John G. Ratcliffe. *Foundations of hyperbolic manifolds*, volume 149 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2006.

[Rei03] I. Reiner. *Maximal orders*, volume 28 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, With a foreword by M. J. Taylor.

[Ril83] Robert Riley. Applications of a computer implementation of Poincaré's theorem on fundamental polyhedra. *Math. Comp.*, 40(162):607–632, 1983.

[Riv12] Igor Rivin. Generic phenomena in groups–some answers and many questions. *arXiv preprint arXiv:1211.6509*, 2012.

[Riv13] Igor Rivin. How to pick a random integer matrix?(and other questions). *arXiv preprint arXiv:1312.4607*, 2013.

[RŞ13] Alexander D. Rahm and Mehmet Haluk Şengün. On level one cuspidal Bianchi modular forms. *LMS J. Comput. Math.*, 16:187–199, 2013.

[San67] I. N. Sanov. Euclid's algorithm and one-sided prime factorizations for matrix rings. *Sibirsk. Mat. Ž.*, 8:846–852, 1967.

[Seh90] Sudarshan K. Sehgal. Units of integral group rings—a survey. In *Algebraic structures and number theory (Hong Kong, 1988)*, pages 255–268. World Sci. Publ., Teaneck, NJ, 1990.

[Şen14] Mehmet Haluk Şengün. Arithmetic aspects of Bianchi groups. In *Computations with modular forms, proceedings of a Summer School and Conference, Heidelberg, August/September 2011*, Contributions in Mathematical and Computational Sciences, pages 279–315. Springer-Verlag, Berlin, 2014.

[Ser62] Jean-Pierre Serre. *Corps locaux*, volume 3. Hermann Paris, 1962.

[Ser80] Jean-Pierre Serre. *Trees*. Springer-Verlag, Berlin-New York, 1980. Translated from the French by John Stillwell.

[Sha00] Yehuda Shalom. Explicit Kazhdan constants for representations of semisimple and arithmetic groups. *Ann. Inst. Fourier (Grenoble)*, 50(3):833–863, 2000.

[Smy08] Chris Smyth. The Mahler measure of algebraic numbers: a survey. In *Number theory and polynomials*, volume 352 of *London Math. Soc. Lecture Note Ser.*, pages 322–349. Cambridge Univ. Press, Cambridge, 2008.

[SV04] R. Sharma and T. N. Venkataramana. Generators for arithmetic groups. *arXiv preprint arXiv:0409345*, 2004.

[Swa71] Richard G. Swan. Generators and relations for certain special linear groups. *Advances in Math.*, 6:1–77 (1971), 1971.

[Vig80] Marie-France Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[Voi06] John Voight. Computing CM points on Shimura curves arising from cocompact arithmetic triangle groups. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 406–420. Springer, Berlin, 2006.

[Voi09] John Voight. Computing fundamental domains for Fuchsian groups. *J. Théor. Nombres Bordeaux*, 21(2):469–491, 2009.

[Vol02] Ulrich Vollmer. An accelerated Buchmann algorithm for regulator computation in real quadratic fields. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 148–162. Springer, Berlin, 2002.

[Wan69] Hsien-chung Wang. Discrete nilpotent subgroups of Lie groups. *J. Differential Geometry*, 3:481–492, 1969.

[Weh07] B. A. F. Wehrfritz. Nilpotent subgroups of finite-dimensional division algebras. *Bull. Lond. Math. Soc.*, 39(3):359–365, 2007.

[Yas10] Dan Yasaki. Hyperbolic tessellations associated to Bianchi groups. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 385–396. Springer, Berlin, 2010.