Rapport de stage

Alexandre Roy
Sous la supervision de Jasmin Matz et Morten Riesager

Mars -Juin 2022

Table des matières

1 Déroulement du stage

J'ai effectué un stage à l'université de Copenhague auprès de Jasmin Matz et Morten Riesager. J'ai effectué mon stage du 1er mars au 30 juin. Le stage consistait à l'étude de différents articles et à la présentation orale de ces articles. Je voyais Jasmin et Morten chaque semaine pour discuter des articles et des éventuelles difficultés auxquelles je pouvais être confronté. Je travaillais depuis la bibliothèque de l'université et je mangeais dans la salle de repos du département de mathématiques où c'était l'occasion de manger avec certains chercheurs en mathématiques ou des doctorants. Durant mon stage, j'ai également pu assister à de nombreux séminaires où des chercheurs venus de différentes universités présentaient leurs recherches. J'ai également pu aller à Lund, en Suède, pour assister à la remise du prix Crafoord à Enrico Bombieri. J'ai également fait quelques présentations d'articles à Jasmin et Morten et une fois à un public plus important.

2 Contenu mathématiques

Le sujet du stage était de compter les corps de nombres à degré d'extension fixé et discriminant borné. Ainsi, pour commencer je vais rappeler les différentes définitions dont nous aurons besoin ici.

2.1 Rappels et définitions

Définition 2.1. *Un corps de nombre est une extension finie K du corps $\mathbb{Q}$. On appelle degré de l'extension la dimension de K en tant que $\mathbb{Q}$-espace vectoriel.*

Définition 2.2. *Soit K un corps de nombre, alors on peut définir l'anneau des entiers de K :*

$$O_K := \{x \in K | \exists P \in \mathbb{Z}[X], P(x) = 0 \text{ et le } coefficient \text{ dominant de } P \text{ est } 1\}.$$

Remarque 2.3. *L'anneau des entiers est bien un anneau. De plus, si L/K est une extension finie avec K un corps de nombres, on peut également définir l'anneau des entiers de L en tant qu'extension de K, simplement les éléments doivent annuler des polynômes unitaires à coefficients dans O_K.*

Proposition 2.4. *Soit K un corps de nombre de degré n, alors O_K est un $\mathbb{Z}$-module libre de rang n et il existe $b_2, \cdots, b_n$ tel que $O_K \cong \mathbb{Z} + \mathbb{Z}b_2 + \cdots + \mathbb{Z}b_n$.*

On dit que $(1, b_2, \cdots, b_n)$ est une base intégrale de K.

Définition 2.5. *Soit K un corps de nombres et n son degré. Soit L sa cloture de Galois et G le groupe de galois de l'extension de $L/\mathbb{Q}$, alors il y a n automorphismes de L qui fixent K, ce sont les plongements de K.*

Définition 2.6. *Soit K un corps de nombre et n son degré, soit $(b_1, \cdots, b_n)$ une base intégrale, $(\sigma_1, \cdots, \sigma_n)$ les plongements de K, alors on définit le discriminant de K par :*

$$disc(K) = (\det(\sigma_i(b_j))_{1 \leq i,j \leq n})^2.$$

On peut de même définir le discriminant relatif de L/K où K est un corps de nombre, en utilisant une définition analogue. Pour toute base, $(b_1, \cdots, b_n)$ de L comme K-espace vectoriel, on considère la matrice dont le coefficient (i, j) est $\sigma_i(b_j)$, où les σ_i correspondent aux plongements de L définis en les prenant comme étant les éléments de la clôture de Galois de L au-dessus de K qui laisse L invariant, et on note $d(b_1, \cdots, b_n)$ le carré du déterminant de cette matrice. Alors le discriminant relatif est l'idéal engendré par ces $d(b_1, \cdots, b_n)$.

De plus, pour I un idéal de O_L, on définit la norme de I comme étant le cardinal de O_L/I.

Proposition 2.7. *La norme du discriminant relatif de K un corps de nombre pris au dessus de $\mathbb{Q}$ est le discriminant de K.*

De plus, si on a $L/K/\mathbb{Q}$, alors $Disc(L) = \mathcal{N}(D_{L/K}) Disc(K)^{[L:K]}$, où $D_{L/K}$ désigne le discriminant relatif de L.

On peut également définir la trace et la norme d'un élément.

Définition 2.8. *Soit K un corps de nombre et $x \in K$, alors on peut définir sa trace et sa norme. Soit $f : y \in K \mapsto xy \in K$, f est une application linéaire sur K en tant que $\mathbb{Q}$-espace vectoriel, et la trace de x est : $Tr(f)$ et la norme de $x, N(x)$ est $det(f)$.*

Exemple 2.9. *Soit K un corps de nombre de degré n et $x \in \mathbb{Q}$ alors $Tr(x) = nx, N(x) = x^n$.*

Définition 2.10. *Ici, on ne considère que la définition dans $\mathbb{R}^n$, $n \in \mathbb{N}$, mais la définition se généralise à tout espace euclidien.*

Un réseau de rang n est un sous-groupe discret de $\mathbb{R}^n$ tel que l'espace vectoriel engendré soit $\mathbb{R}^n$ tout entier.

Ainsi, de manière générale, un réseau est de la forme $\Lambda = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n$ avec $\mathbb{R}^n = Vect(a_1, \cdots, a_n)$, où $Vect$ désigne l'espace vectoriel engendré.

Définition 2.11. *Dans $\mathbb{R}^n$, soit Λ un réseau, et C un compact symétrique par rapport à l'origine et de volume non nul, alors on définit les n minimas successifs au sens de Minkoswki $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$, où λ_j est défini comme étant le plus petit réel λ tel que λC contienne j vecteurs linéairement indépendants.*

Proposition 2.12. *Soit K un corps de nombre, alors on peut plonger O_K dans un R^n qui en fait un réseau.*

De plus, si on considère $O_K^0 := \{x \in O_K | Tr(x) = 0\}$, alors on obtient un réseau de rang $n - 1$.

De plus, en prenant comme compact $B(1)$ la boule unité pour la norme l^2, et en prenant les minimas au sens de Minkowski, alors le deuxième théorème de Minkoswki dit que

$$a_1 \cdots a_{n-1} \approx Disc_K^{\frac{1}{2}},$$

où cela signifie qu'il existe des constantes K_1, K_2 dépendant seulement de n tel que $K_1 Disc_K^{\frac{1}{2}} \leq a_1 \cdots a_{n-1} \leq K_2 Disc_K^{\frac{1}{2}}$.

2.2 Intérêt de l'étude

Prenons le cas $n = 2$, toute extension de degré 2 de $\mathbb{Q}$ est de la forme $\mathbb{Q}(\sqrt{d})$ où $d \in \mathbb{Z}$ n'est divisible par aucun carré.

De plus, $Disc(\mathbb{Q}(\sqrt{d})) = d$ si $d = 4k + 1, k \in \mathbb{Z}$ ou $4d$ sinon.

On voit donc que le nombre de corps de nombres de degré 2 avec un discriminant à valeur absolue plus petite que X grossit comme une constante multipliée par X.

De manière générale si $N^n(X)$ désigne le nombre de corps de nombres de degré n et avec un discriminant borné par X alors on conjecture que pour tout n,

$$\lim \frac{N^n(X)}{X} = c_n, c_n > 0.$$

De même, on parlera parfois de $N_K^n(X)$ qui sont les extensions de K de degré n, avec un discriminant relatif ayant une norme plus petite que X, et la même conjecture existe où les limites obtenues dépendent du corps de nombre de base.

Il se trouve que ce résultat a été prouvé pour les cas $n = 3, 4$ et 5. De plus, des bornes supérieures et inférieures ont été trouvées. Durant ce stage, j'ai pu étudier les cas $n = 4, 5$ prouvés par Bhargava dans les articles [**Bhar**] et [**Bhar2**]. Ellenberg et Venkatesh ont donné une borne supérieure et une borne inférieure dans [**EV**], cette borne supérieure a été améliorée par Couveignes dans [**Couv**] et ensuite, Lemke et Thorne ont réussi à améliorer de nouveau ce résultat dans [**LT**]. La borne inférieure donnée par Ellenberg et Venkatesh est quelque peu améliorable en utilisant ces améliorations dans la preuve.

2.3 Les cas $n = 4$ et $n = 5$

Dans cette section, je vais me rapporter aux articles [**Bhar**] et [**Bhar2**] rédigés par Bhargava traitant les cas $n = 4$ et $n = 5$.

2.3.1 Le cas $n = 4$

Soit $N_4(X) := \#\{K | [K : \mathbb{Q}] = 4, |disc(K)| \leq X$ *et sa clôture de Galois a groupe de galois* $\mathcal{S}_4\}$.

Alors,

Proposition 2.13. *On obtient :*

$$\lim \frac{N_4(X)}{X} = (\frac{1}{48} + \frac{1}{8} + \frac{1}{16}) \prod_p (1 + p^{-2} - p^{-3} - p^{-4}).$$

Remarque 2.14. *Le résultat n'est donné que sur les corps $\mathcal{S}_4$-quartiques (i.e. dont le groupe de galois de la cloture de Galois est $\mathcal{S}_4$) et non sur tous les corps quartiques. Néanmoins, en prenant le résultat de Cohen, Diaz et Olivier dans [***CDO***], il est prouvable qu'asymptotiquement seuls les corps $\mathcal{S}_4$-quartiques et $\mathcal{D}_4$-quartiques ont une importance dans le nombre total de corps quartiques et la proportion de corps $\mathcal{S}_4$-quartiques est environ $82,9\%$.*

Donc, le cas $n = 4$ est bien complètement prouvé.

Pour montrer ce résultat Bhargava s'intéresse à l'espace $V_{\mathbb{R}}$ des paires (A, B) des matrices réelles symétriques 3×3.

Définition 2.15. *Soit $(A, B) \in V_{\mathbb{R}}$, on dit que cette paire est entière ssi $A, B \in M_3(\mathbb{Z})$. On note $V_{\mathbb{Z}}$ le sous-espace contenant les paires entières.*

On définit le groupe $G_{\mathbb{Z}}$ par $G_{\mathbb{Z}} := GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$. Ce groupe agit sur $V_{\mathbb{R}}$ par :

- *si $g_2 \in GL_2(\mathbb{Z})$, alors $g_2 \cdot (A, B) := (g_2(A, B)^t)^t$,*
- *et si $g_3 \in SL_3(\mathbb{Z})$, alors $g_3 \cdot (A, B) := (g_3 A g_3^t, g_3 b g_3^t)$.*

Remarque 2.16. *Toute matrice symétrique 3×3 peut-être vue comme étant une forme quadratique à 3 variables : si $A = (a_{ij})_{1 \leq i,j \leq 3}$ est une telle matrice, on lui associe la forme ; $a_{11}x^2 + a_{12}xy + a_{13}xz + a_{22}y^2 + a_{23}yz + a_{33}z^2$.*

Le groupe $G_{\mathbb{Z}}$ laisse stable le sous-ensemble $V_{\mathbb{Z}}$.

Définition 2.17. *Il est possible de définir le discriminant d'une paire $(A, B) \in V_{\mathbb{R}}$ comme étant : $Disc(A, B) = Disc(4Det(Ax - By))$ où le discriminant est celui de la forme cubique à 2 variables.*

On dit qu'un anneau Q est un anneau quartique s'il est isomorphe à $\mathbb{Z}^4$ en tant que $\mathbb{Z}$-module.

On a maintenant toutes les définitions nécessaires pour énoncer le théorème suivant.

Theorème 2.18. *Les deux ensembles suivants sont en bijection :*

- *L'ensemble des $G_{\mathbb{Z}}$-classes d'équivalence d'élements $(A, B) \in V_{\mathbb{Z}}$ et*
- *l'ensemble des classes d'isomorphismes des paires (Q, R) où Q est un anneau quartique et R est un anneau cubique lié à Q.*

De plus, on a $Disc(A, B) = Disc(Q)$.

A la vue de ce théorème, on voit que l'on ne va avoir besoin de ne s'interesser qu'aux paires $(A, B) \in V_{\mathbb{Z}}$ ayant un discriminant compris entre $-X$ et X. De plus, il est clair que tous les anneaux quartiques ne nous intéressent pas, on ne souhaite que ceux qui seront liés à des corps $\mathcal{S}_4$-quartiques. On définit ainsi la notion d'asbolue irréductibilité.

Définition 2.19. *Une paire $(A, B) \in V_{\mathbb{Z}}$ est dite absolument irréductible ssi*

- *A et B ne possèdent pas de zéro commun dans $\mathbb{P}^2(\mathbb{Q})$ (où A et B sont vus comme des formes quadratiques à 3 variables),*
- *Le polynôme à deux variables $Det(Ax - By)$ est irréductible sur $\mathbb{Q}$.*

Ces conditions sont équivalentes au fait que A et B possèdent un zéro commun dans $\mathbb{P}^2(K)$ où K est un corps $\mathcal{S}_4$-quadratique.

Ce que nous devons faire est compter le nombre de classes d'équivalence. Pour ce faire, Bhargava utilise le groupe $G_{\mathbb{R}} := GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$ qui agit lui aussi sur $V_{\mathbb{R}}$.

Cette action possède 3 orbites :

$V_{\mathbb{R}}^{(i)} = \{(A, B) \in V_{\mathbb{R}} | A, B \text{ possèdent } 4 - 2i \text{ zéros communs dans } \mathbb{P}^2(\mathbb{R})\}, 0 \leq i \leq 2.$

Définition 2.20. *Ainsi, il devient naturel de considerer 3 sous-espaces qui seront traités de la même façon : pour $0 \leq i \leq 2, V_{\mathbb{Z}}^{(i)} := V_{\mathbb{Z}} \cap V_{\mathbb{R}}^{(i)}$.*

On peut définir $N(V_{\mathbb{Z}}^{(i)}, X)$ comme étant le nombre de $G_{\mathbb{Z}}$ classe d'équivalences d'éléments irréductibles $(A, B) \in V_{\mathbb{Z}}^{(i)}$ et avec $|Disc(A, B)| < X$, alors

$$\lim \frac{N(V_{\mathbb{Z}}^{(i)}, X)}{X} = \frac{\zeta(2)^2 \zeta(3)}{2n_i},$$

avec $n_0 = 24, n_1 = 4, n_2 = 8$.

Pour compter ce nombre, on va s'intéresser à certains domaines fondamentaux de l'action de $G_{\mathbb{Z}}$ sur $V_{\mathbb{R}}$.

Soit $\mathcal{F}$ un domaine fondamental de l'action de $G_{\mathbb{Z}}$ sur $G_{\mathbb{R}}$ par multiplication à gauche. Alors, bien que $\mathcal{F}$ soit compliqué à décrire, on peut trouver des sous-groupes plus classiques tels que leur produit contienne $\mathcal{F}$.

Pour chaque élément $v \in V_{\mathbb{R}}^{(i)}$, on peut considérer le stablilisateur dans $G_{\mathbb{R}}$ de cet élément. Alors, on peut définir n_i comme étant le cardinal de ce stabilisateur. Pour retrouver les valeurs données ci-dessus, on peut considérer que le stabilisateur va "agir" sur les zéros communs et donc on trouve $\mathcal{S}_4$ s'il y a 4 zéros dans $\mathbb{P}^2(\mathbb{R})$, si on en a 2 dans $\mathbb{P}^2(\mathbb{R})$ et les 2 autres dans $\mathbb{P}^2(\mathbb{C})$, on peut simplement les intervertir 2 à 2, donc $n_1 = 4$.

Ainsi, si $v \in V_{\mathbb{R}}^{(i)}, \mathcal{F}v$ est l'union non nécessairement disjointe de n_i domaines fondamentaux de l'action de $G_{\mathbb{Z}}$ sur $V_{\mathbb{R}}^{(i)}$.

Néanmoins, avec notre choix d'éléments irréductibles, chaque classe d'équivalence d'éléments irréductibles apparaît exactement n_i fois dans $\mathcal{F}v$.

Proposition 2.21. *Ainsi, $n_i N(V_{\mathbb{Z}}^{(i)}, X)$ est exactement le nombre de points entiers dans $\mathcal{F}v$ qui ont un discriminant borné par X.*

Il est difficile de compter ce nombre de points dans un certain $\mathcal{F}v$, donc l'astuce de Bhargava est de moyenner ce nombre pour v qui varie dans un compact H, on peut par exemple prendre pour H, l'ensemble des paires dont tous les coefficients matriciels sont en valeur absolue plus petits que 10.

La seconde méthode principale pour arriver à ce résultat est de découper $\mathcal{F}v$ en différents sous-ensembles où le nombre de points entiers irréductibles sera négligeable devant X, ce qui ne laissera plus qu'un sous-ensemble où l'on sera en mesure de compter le nombre de points.

Proposition 2.22. *Le découpage de $\mathcal{F}v$ se fait selon la valeur prise par a_{11} (le premier coefficient diagonal de A).*

Ainsi,

- *Le nombre d'éléments entiers irréductibles avec $a_{11} = 0$ dans $\mathcal{F}v$ est $o(X)$,*
- *Le nombre d'éléments entiers réductibles avec $a_{11} \neq 0$ est $o(X)$,*
- *Si $\delta < \frac{11}{12}$, le nombre d'éléments entiers irréductibles avec $0 < |a_{11}| < X^{\delta}$ dans $\mathcal{F}v$ est $o(X)$.*

Finalement, on obtient :

Proposition 2.23. *Pour $v \in V_{\mathbb{R}}^{(i)}$, soit $R_X(v)$ le sous-ensemble de $\mathcal{F}v$ comportant les points avec $|Disc(A, B)| < X$, alors*

$$n_i N(V_{\mathbb{Z}}^{(i)}, X) = Vol(R_X(v)) + o(X).$$

De plus, on peut calculer le volume et

$$Vol(R_X(v)) = \frac{\zeta(2)^2\zeta(3)}{2}.$$

Pour pouvoir conclure, on ne veut pas compter l'ensemble des classes d'éléments irréductibles dans tout $V_{\mathbb{Z}}$, mais seulement dans un sous-ensemble. Et nous disposons de la prochaine proposition pour conclure.

Proposition 2.24. *Soit $S \subset V_{\mathbb{Z}}$, alors*

$$\lim \frac{N(S \cap V_{\mathbb{Z}}^{(i)}, X)}{X} = \frac{\zeta(2)^2\zeta(3)}{2n_i} \prod_p \mu_p(S),$$

où $\mu_p(S)$ désigne la mesure p-adique de S dans $V_{\mathbb{Z}}$.

Nous allons rapidement présenter la mesure p-adique.

Définition 2.25. *Soit p un nombre premier et $x \in \mathbb{Q}$, alors $x = p^m \frac{a}{b}, a, b, m \in \mathbb{Z}$ et p ne divise ni a, ni b. Alors, on peut definir la norme $|\cdot|_p$ de x par $|x|_p = \frac{1}{p^m}$.*

Ainsi, on définit $\mathbb{Q}_p$ comme étant la complétion de $\mathbb{Q}$ suivant cette norme.

On peut également définir l'anneau des entiers de $\mathbb{Q}_p$ par

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p | |x|_p \leq 1\}.$$

Alors $\mathbb{Z}_p$ est compact.

De plus, avec cette définition, on sait qu'il existe une unique, à constante multiplicative près, mesure finie sur les compactes de $\mathbb{Q}_p$ et invariante par translation, appelée mesure de Haas.

On note μ_p la mesure de Haas qui après multiplication par la bonne constante est telle que $\mu_p(\mathbb{Z}_p) = 1$.

Définition 2.26. *Soit p un nombre premier, et considérons $\mathcal{U}_p$ l'ensemble des paires dont l'anneau quartique correspondant est maximal à p ce qui revient à dire que $Q \otimes \mathbb{Z}_p$ n'est pas une sous $\mathbb{Z}_p$-algèbre propre d'une $\mathbb{Z}_p$-quartique algèbre et $\mathcal{U} = \cap_p \mathcal{U}_p$, ainsi $\mathcal{U}$ correspond à toutes les paires qui correspondent à un anneau quartique intègre dont le corps de fraction est un corps $\mathcal{S}_4$-quadratique.*

*De plus, on a $\mu_p(\mathcal{U}_p) = (1 - p^{-2})^2(1 - p^{-3})(1 + p^{-2} - p^{-3} - p^{-4})$ ce qui permet de conclure. Pour les détails de ce calcul, on pourra regarder le lemme 23 de [***Bhar3***].*

2.3.2 Le cas $n = 5$

Pour le cas $n = 5$, Bhargava va utiliser la même méthode. Néanmoins, le résultat est quelque peu meilleur que le précédent car ici, on obtient un résultat sur tous les corps quintiques.

Soit $N_5(X)$ le nombre de corps de nombres avec un discriminant compris entre $-X$ et X.

Proposition 2.27. *Alors,*

$$\frac{\mathrm{N_5(X)}}{\mathrm{X}} = (\frac{1}{240} + \frac{1}{24} + \frac{1}{16}) \prod_p (1 + p^{-2} - p^{-4} - p^{-5}).$$

Remarque 2.28. *La limite obtenue peut-être vue comme un produit de constantes connues. En effet, $1 + p^{-2} - p^{-4} - p^{-5} = \frac{p-1}{p} \sum_{[K_p:\mathbb{Q}_p]=5} \frac{1}{|Aut_{\mathbb{Q}_p}(K_p)|} \frac{1}{Disc(K_p)}$ et*

$\frac{1}{240} + \frac{1}{24} + \frac{1}{16} = \frac{1}{2}(\frac{1}{|Aut_{\mathbb{R}}(\mathbb{R}^5)|} + \frac{1}{|Aut_{\mathbb{R}}(\mathbb{R}^3 \oplus \mathbb{C})|} + \frac{1}{|Aut_{\mathbb{R}}(\mathbb{R} \oplus \mathbb{C}^2)|}) = \frac{1}{2} \sum_{[K:\mathbb{R}]=5} \frac{1}{|Aut_{\mathbb{R}}(K)|}$.

L'idée est la même que précédemment, mais l'espace $V_{\mathbb{R}}$ utilisé est l'espace des quadruplés de matrices anti-symétriques 5×5 et le groupe $G_{\mathbb{Z}}$ est maintenant $G_{\mathbb{Z}} := GL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$.

Il est également possible de définir le discriminant de (A, B, C, D) en utilisant la même stratégie que précédemment mais on ne l'explicitera pas ici.

Ainsi, on obtient un théorème équivalent au cas $n = 4$.

Theorème 2.29. *Les deux ensembles suivants sont en bijection :*

- *L'ensemble des $G_{\mathbb{Z}}$-classes d'équivalence d'élements $(A, B, C, D) \in V_{\mathbb{Z}}$ et*
- *l'ensemble des classes d'isomorphismes des paires (R, R') où R est un anneau quintique et R' est un anneau sextique lié à R.*

De plus, on a $Disc(A, B, C, D) = Disc(R)$.

Cette fois encore on va seulement compter les éléments irréductibles, cette fois la condition est : R doit être un anneau intègre, pour pouvoir donner naissance à un corps quintique via son corps de fraction.

Proposition 2.30. *En reprenant les notations précédentes et en les adaptant à la situation actuelle,*

$$\lim \frac{N(V_{\mathbb{Z}}^{(i)}, X)}{X} = \frac{\zeta(2)^2\zeta(3)^2\zeta(4)^2\zeta(5)}{2n_i},$$

où n_i désigne le cardinal du stabilisateur, ces groupes sont ceux présentés dans la deuxième partie de la remarque 2.28.

L'idée est maintenant la même, seulement le découpage de $\mathcal{F}v$ se fait selon la valeur de a_{12}, comme on sait déjà que $a_{11} = 0$, et de nouveau ce qu'il reste à faire est calculer le volume de $R_X(v)$.

Proposition 2.31. *Le nombre d'éléments $(A, B, C, D) \in V_{\mathbb{Z}}$ ayant $a_{12} \neq 0$, un anneau quintique associé intègre et tel que le corps de fractions associé ne soit pas un corps $\mathcal{S}_5$-quintique est $o(X)$.*

Ainsi, les seuls corps qui comptent assymptotiquement sont les $\mathcal{S}_5$-quintiques, ce qui explique que le résultat soit "meilleur".

Remarque 2.32. *Malheuresement, il n'est pas possible de poursuivre ce raisonnement dans les cas $n > 5$, en effet le théorème sur lequel s'appuie la preuve est lié à la théorie des espaces vectoriel pré-homogènes, dont il n'en existe qu'un nombre fini à isomorphisme près, et on ne peut lier ces espaces qu'à des extensions de $\mathbb{Q}$ de dimension $3, 4 ou 5$.*

2.4 Le cas général

Bien qu'aucune preuve de ce fait n'existe dans le cas général, il y a néanmoins des bornes supérieures et inférieures auxquelles nous allons maintenant nous intéresser.

2.4.1 Borne supérieure

Dans leur article, Ellenberg et Venkatesh, [**EV**], Couveignes, [**Couv**], et Lemke et Thorne, [**LT**], ont prouvé une borne supérieure améliorée de plus en plus. La technique utilisée par Lemke et Thorne ressemble quelque peu à celle d'Ellenberg et Venkatesh, donc on traitera leur article en deuxième et non dans l'ordre chronologique de publication des articles.

Tout d'abord, la première borne supérieure connue est celle de Schimdt, si $N^n(X)$ désigne le nombre de corps de nombre de degré, n, et ayant un discriminant avec une valeur absolue plus petite que X, alors

$$N^n(X) \ll X^{\frac{n+2}{4}}.$$

Cette borne vient du fait que par le résultat du deuxième théorème de Minkowski, 2.12, on peut trouver $\alpha \in O_K^0$ avec $||\alpha|| = O(Disc(K)^{\frac{1}{2n-2}})$, où la valeur absolue d'un élément désigne le maximum des modules de tous les plongements de α.

Comme le polynôme minimal de α est $X^n + a_{n-2}X^{n-2} + \cdots + a_1X + a_0$, et donc tous les coefficients $a_i, 0 \leq i \leq n-2$, sont bornés par $Disc(K)^{\frac{n-i}{2n+2}}$. Donc il y a $O(X^{\frac{2+\cdots+n}{2(n-1)}})$ possibilités des coefficients polynomiaux.

Donc, il y a $O(X^{\frac{n+2}{4}})$ choix pour les coefficients et donc ce nombre de choix pour le nombre de corps de nombres.

— Commençons par l'article d'Ellenberg et Venkatesh, [**EV**].

Soit $N_K^n(X)$ le nombre d'extensions de degré n de K ayant un discriminant relatif ayant une norme plus petite que X, où K est un corps de nombre.

Theorème 2.33. *Alors,*

$$N_K^n(X) \ll (C'X)^{\exp(C\sqrt{\ln n})}$$

où les constantes supposées par le symbole $\ll$ sont indépendantes de K et C est indépendant de n.

L'idée de la preuve est de trouver des polynômes dont l'évaluation en un certain point permettra de caractériser toute extension de degré n. Ainsi, on devra calculer le nombre de polynômes nécessaires pour caractériser tout extension pour savoir combien d'extensions peuvent être trouvées.

Soit $n \in \mathbb{N}$, et soit L une extension de K de degré n.

Définition 2.34. *Définissons $\mathbb{A}^n := Spec(\mathbb{Z}[x_1, \cdots, x_n])$ et soient $\rho_1, \cdots, \rho_n$ les plongements de L dans $\overline{K}$. Alors, pour chaque $\alpha \in O_L$, on obtient un élement de $\mathbb{A}^n(\overline{K}) = \overline{K}^n$. Ainsi, il est possible de considérer l'application $\phi_L : O_L^r \to \mathbb{A}^{nr}(\overline{K})$.*

On sait que les éléments de $\mathbb{Z}[x_{i,j}]_{1\leq i\leq n, 1\leq j\leq r}$ agissent sur $\mathbb{A}^{nr}$. De plus, $\mathcal{S}_n$ agit sur ces polynômes en agissant sur $x_{1,k}, \cdots, x_{n,k}$ pour tout k.

On appelle fonction multisymétrique, toute fonction invariante sous cette action.

Soit f une fonction multisymétrique, alors $f \circ \phi_L : O_L^r \to O_K$.

Ainsi, en prenant R comme étant un sous-anneau de $\mathbb{Z}[x_{i,j}]_{1\leq i\leq n, 1\leq j\leq r}$ ne comportant que des fonctions multisymétriques, on obtient une application

$$\begin{aligned}\mathcal{F} : \bigcup_{L:[L:K]=n} O_L^r &\to Spec(R)(O_K)\\ (\alpha_1, \cdots, \alpha_r) &\mapsto (f \mapsto \phi_L(\alpha_1, \cdots, \alpha_r)(f)),\end{aligned}$$

où l'union est prise sur toutes les extensions finies de K de degré n.

Notre objectif va donc être de trouver des certains $\alpha_1, \cdots, \alpha_r$ dans chaque L, extension de K de degré n, et un certain sous-anneau suffisamment gros de manière à ce qu'un nombre fini et contrôlable d'extensions soit envoyé sur le même point de $Spec(R)(O_K)$, en essayant d'avoir une norme "petite" pour les α_i et que R ne soit pas trop gros pour avoir la meilleure borne possible.

Dans toute la suite, la norme d'un élément est le maximum des modules de ces plongements.

Définition 2.35. *Soit $\sigma = (i_1, \cdots, i_r) \in \mathbb{Z}^r_{\geq 0}$, alors on peut définir*

$$\begin{aligned}\chi_\sigma :&\mathbb{A}^{nr} \to \mathbb{A}^n\\ &x \mapsto x_1^{i_1} \cdots x_r^{i_r}\end{aligned}$$

où x_i est la i-ème colonne.

De plus, on peut définir $f_\sigma = Tr \circ \chi_\sigma$, qui est donc multisymétrique. Donc, si on considère le sous-ensemble $\Sigma \subset \mathbb{Z}^r_{\geq 0}$, on peut définir notre sous-anneau R_Σ, comme étant l'anneau engendré par les (f_σ).

On peut donc définir notre application $\mathcal{F}$ ci-dessus, comme étant $\mathcal{F}_\Sigma : \mathbb{A}^{nr}(K) \to Spec(R_\Sigma)(O_K)$.

Donc pour contrôler la taille de R, il faut contrôler la taille de ce sous-ensemble Σ.

Remarque 2.36. *Pour arriver à notre conclusion, il faut donc trouver un élément $\phi_L(\alpha_1, \cdots, \alpha_r) \in \mathbb{A}^{nr}(\overline{K})$, tel que cet élément caractérise dans un certain sens l'extension L/K, et tel qu'avec un bon choix de Σ, l'évaluation de ces polynômes sur chaque élément caractérise complètement notre extension L/K. Alors, compter le nombre de polynômes et le nombre de valeurs qu'ils peuvent prendre permettra de dénombrer le nombre maximum d'extensions de degré n de K.*

On a plusiseurs lemmes qui vont nous aider à comprendre la taille minimale de sous-ensemble que nous devons prendre.

Soit F un corps de caractéristique 0.

Lemme 2.37. *Soit V un sous-espace de F^n de dimension m en tant que F-espace-vectoriel. Soit $\Sigma_0 \subset \mathbb{Z}^r_{\geq 0}$ de cardinal m. Soit $Z \subset V^r$ le sous-espace des points $x \in V^r$ tels que les $(\chi_\sigma(x))_{\sigma\in\Sigma_0}$ ne sont pas linéairement indépendants, alors Z n'est pas tout V^r. De plus, Z est contenu dans les points à coordonnées dans F d'une hypersurface dont le degré est borné par n et m.*

Lemme 2.38. *Soit $x \in \mathbb{A}^{nr}(F)$ et Σ_0 un sous ensemble de $\mathbb{Z}^r_{\geq 0}$ tel que les vecteurs $\chi_\sigma(x)$ engendrent un F-espace vectoriel $\subset F^n$ de dimension $> \frac{n}{2}$.*

Alors, soit $\Sigma_1 := \Sigma_0 + \Sigma_0$ et soit W l'espace vectoriel engendré par les $\chi_\sigma(x), \sigma \in \Sigma_1$, alors le supplémentaire orthogonal de W est contenu dans un hyperplan du type $\{x = (x_1, \cdots x_n) | x_i = 0\} := H_i$.

Lemme 2.39. *Soit $x \in \mathbb{A}^{nr}(F)$, et Σ_1 un sous-ensemble de $\mathbb{Z}^r_{\geq 0}$ tel que les vecteurs $\chi_\sigma(x)$ pour $\sigma \in \Sigma_1$ engendrent F^n en tant que F-espace vectoriel.*

Alors soit $\Sigma \subset \mathbb{Z}^r_{\geq 0}$ tel que $\Sigma_1 + \Sigma_1 \subset \Sigma$ et pour tout $1 \leq k \leq r, \Sigma_1 + e_k \subset \Sigma$, où e_k désigne l'élément de $\mathbb{Z}^r_{\geq 0}$ avec un 1 en k-ième coordonnée et 0 sur toutes les autres.

Alors,

$$|\mathcal{F}_\Sigma^{-1}(\mathcal{F}_\Sigma(x))| \leq (n!)^r.$$

Remarque 2.40. *On ne peut pas vraiment espérer avoir une meilleure borne, comme nos polynômes f_σ sont invariants sous les permutations des coordonnées de chaque colonne, et ceci doit se retouver ici.*

Remarque 2.41. *Maintenant que nous avons ces lemmes, quelles informations peut-on obtenir ?*

Pour compléter la preuve, il faudra donc prendre un premier sous-ensemble Σ_0 de taille $m > \frac{n}{2}$, et nous serons en mesure de trouver un élément x tel que les $\chi_\sigma(x)$ soient linéariement indépendants, via le premier des trois lemmes. Ainsi, par le deuxième lemme, il sera possible de construire un espace vectoriel dont nous contrôlerons le supplémentaire orthogonal. Ainsi, avec un bon élément x, il devrait être possible de construire un W qui sera tout F^n entier. Ainsi, par le troisième lemme, on pourra construire Σ, tel que nous pouvons contrôler le nombre d'éléments envoyé sur le même point par $\mathcal{F}_\Sigma$. Ainsi, on n'a plus qu'à savoir combien de tels polynômes on a construit.

Néanmoins, comme notre application ϕ_L n'est pas surjective, on aura besoin d'un autre lemme pour s'assurer que l'image de ϕ_L rencontre bien $V^r \backslash Z$, en reprenant les notations précédentes.

Lemme 2.42. *Soit f un polynôme de degré d en les variables $x_1, \cdots, x_n$. Alors, il existe des entiers $\alpha_1, \cdots, \alpha_n$ tels que $f(\alpha_1, \cdots, \alpha_n) \neq 0$ et $\max_{1\leq i\leq n} |a_i| \leq \frac{d+1}{2}$.*

Finalement, on a la proposition suivante qui rassemble toutes ces informations.

Proposition 2.43. *Soit $\Sigma_0 \subset \mathbb{Z}^r_{\geq 0}$ de taille $m > \frac{n}{2}$; soit $\Sigma_1 \subset \mathbb{Z}^r_{\geq 0}$ qui contient $\Sigma_0 + \Sigma_0$. Soit $\Sigma \subset \mathbb{Z}^r_{\geq 0}$ qui contient $\Sigma_1 + \Sigma_1$ et $\Sigma_1 + e_k$ pour tout k.*

Finalement, soit L une extension finie de K avec $[L : K] = n$ et notons $d := [K : \mathbb{Q}]$.

Alors, il existe r éléments $(\alpha_1, \cdots, \alpha_r) \in O_L^r$ tels que

1. *Pour tout k,*
$$||\alpha_k|| \ll Disc(L)^{\frac{1}{d(n-2)}},$$
2. *L'ensemble $\mathcal{F}_\Sigma^{-1}(\mathcal{F}_\Sigma(x))$ est fini et son cardinal est au plus $(n!)^r$,*
3. *Les éléments $\alpha_1, \cdots, \alpha_r$ génèrent l'extension L/K.*

Nous sommes maintenant prêts à dénombrer le nombre d'extensions possible.

Soient r, c des entiers tels que $\binom{r+c}{r} > \frac{n}{2}$. Alors, on peut considérer Σ_0 comme étant l'ensemble des r-tuples dont la somme des coordonnées est au plus c. Aisni, Σ_1 est celui dont la somme des coordonnées est au moins $2c$, et on prend Σ comme étant celui dont la somme est au moins $4c$.

Soit L une extension de K de degré n. Soient $(\alpha_1, \cdots, \alpha_r)$ comme dans la proposition 2.43. Soit Q_L comme étant $\phi_L(\alpha_1, \cdots, \alpha_r)$, alors par cette même propositon, on sait que Q_L caractérise notre extension : si $Q_L = Q_{L'}$, alors L et L' sont isomorphes. Soit $P_L := \mathcal{F}_\Sigma(Q_L)$, alors on sait qu'au plus $(n!)^r$ extensions sont envoyées sur ce même point.

A partir d'ici, on ne considère plus que les extensions dont la norme du discriminant relatif de L/K est plus petite que X.

Ainsi, pour tout k,
$$||\alpha_k|| \ll (XDisc(K)^n)^{\frac{1}{d(n-2)}}.$$

Soit $f_\sigma \in R_\Sigma$, c'est un polynôme à coefficients entiers de degré au plus $4c$, et donc $f_\sigma(Q_L)$ est un élément de O_K et un polynôme de degré au plus $4c$ en les $\rho_j(\alpha_i)$.

Donc, on a
$$|f_\sigma(Q_L)| \ll (XDisc(K)^n)^{\frac{4c}{d(n-2)}}.$$

Comme c'est un élément de O_K et que $[K : \mathbb{Q}] = d$, on a $\ll (XDisc(K)^n A_n^d)^{\frac{4c}{(n-2)}}$ choix pour notre élément, où A_n est une constante, dépendant de K et n.

De plus, P_L est une application déterminée par les valeurs de tous les $f_\sigma(Q_L)$ et on a $\binom{r+4c}{r}$ éléments dans Σ. On a donc $\ll (XDisc(K)^n A_n^d)^{\frac{4c\binom{r+4c}{r}}{(n-2)}}$ possibilités pour P_L, comme P_L caractérise notre extension à un nombre fini près, donc on a :
$$N_K^n(X) \ll (XDisc(K)^n A_n^d)^{\frac{4c\binom{r+4c}{r}}{(n-2)}}.$$

Prenons maintenant $r \leq \sqrt{\ln(n)}$ et $c \geq n^{\frac{1}{r}} r!^{\frac{1}{r}}$.

Finalement, on obtient

$$N_K^n(X) \ll (XDisc(K)^n A_n^d)^{\exp(C\sqrt{\ln(n)})}.$$

— Passons maintenant à l'article de Lemke et Thorne, [**LT**].

Ici, on ne regarde que les extensions de $\mathbb{Q}$, néanmoins en changeant les constantes, le résultat tient pour les extensions d'un certain corps de nombre.

L'amélioration du résultat provient du fait que bien que l'on s'intéresse aux mêmes polynômes que précédemment, Lemke et Thorne ont trouvé une façon d'en compter beaucoup moins. Moralement, Ellenberg et Venkatesh ont considéré approximativement $\binom{\sqrt{\ln(n)}+n^{\frac{1}{\sqrt{\ln(n)}}}\sqrt{\ln(n)}}{\sqrt{\ln(n)}}$ polynômes qui ont un degré inférieur à $4n^{\frac{1}{\sqrt{\ln(n)}}}\sqrt{\ln(n)}$, ici, on va prendre seulement $c\ln(n)n$ polynômes qui ont un degré plus petit que $c\ln(n)$.

L'idée est encore une fois que les évalutions $Tr_{n,a}(x_0)$, pour $a \in A \subset \mathbb{Z}_{\geq 0}^r$ où $Tr_{n,a}(x_0) = \sum_{k=0}^{n} x_{1,k}^{a_1} \cdots x_{r,k}^{a_r}, x_0 \in \mathbb{A}^{nr}(\mathbb{C})$ déterminent chaque extension à un nombre fini d'extensions près. Donc, si on trouve un bon ensemble A, on trouvera les polynômes recherchés.

Ce que l'on veut prouver est :

Theorème 2.44. — *Soit $n \geq 2$, alors*

$$N^n(X) \ll X^{\frac{8\sqrt{n}}{3}}.$$

— *Soit $3 \leq r \leq n, d$ tel que $\binom{d+r-1}{r-1} > rn$. Alors,*

$$N^n(X) \leq X^{rd}.$$

En prenant un bon choix de r, d, on peut montrer que pour $c > \dfrac{1}{4\ln^2(2)} \approx 0.52, \exists M$ tel que

$$\forall n \geq M, N^n(X) \ll X^{c\ln^2(n)}.$$

Explicitement pour $c = 1.564$, on peut prendre $M = 6$.

Notre objectif est de pouvoir prendre aussi peu de polynômes que possible, le lemme suivant va nous permettre de le faire.

Lemme 2.45. *Soient $f_1, \cdots, f_N$ des polynômes de $\mathbb{A}^N(\mathbb{C})$ dans $\mathbb{A}^1(\mathbb{C})$. Supposons que le déterminant de la matrice $(\dfrac{\partial f_i}{\partial x_j})$ ne soit pas le polynôme nul. Alors, il existe un polynôme non nul $P : \mathbb{A}^{nr}(\mathbb{C}) \to \mathbb{A}^1(\mathbb{C})$ tel que si $P(x_0) \neq 0$ pour un certain x_0, il y a au plus $\prod_{i=1}^{n} deg\ f_i, x \in \mathbb{A}^{nr}$ tel que $f_1(x) = f_1(x_0), \cdots, f_N(x) = f_N(x_0)$.*

Comme précédemment, on va prendre un r-tuple qui va nous donner un point dans $\mathbb{A}^{nr}(\mathbb{C})$, et on va donc vouloir choisir $A \subset \mathbb{Z}^r_{\geq 0}$ constitué de rn vecteurs tel que la matrice $(\frac{\partial Tr_{n,a}}{\partial x_{i,j}})_{a\in A}$ n'a pas le polynôme nul comme déterminant.

Définition 2.46. *Posons :*

$$DTr_{n,a} := (\frac{\partial}{\partial x_{k,i}} Tr_{n,a})_{1\leq k\leq r, 1\leq i\leq n}$$

le vecteur colonne des dérivées partielles.

On va donc s'intéresser à la matrice $(DTr_{n,a})_{a\in A}$.

Notre objectif va être de trouver un bon ensemble A, prenons le cas $r = 2$ comme exemple.

Exemple 2.47. *Pour $n \in \mathbb{N}^*$, posons A_n comme étant l'ensemble inclus dans $\mathbb{Z}^2_{\geq 0}$ qui contient les $2n$ premiers éléments (i, j) ordonné par la valeur de $i + j$ et ensuite par j croissant.*

On va montrer que A_n convient par récurrence.

Tout d'abord, pour $n = 1, \det(DTr_{a,1})_{a\in A_1} = 1$.

Soit $D_{k,l}$ le coefficient (k, l) de la matrice correspondante. Ainsi, on a $D_{k,n} = a_{k,1}x_{1,n}^{a_{k,1}-1}x_{2,n}^{a_{k,2}}$ et $D_{k,2n} = a_{k,2}x_{1,n}^{a_{k,1}}x_{2,n}^{a_{k,2}-1}$.

Le déterminant est une somme de produits incluant $D_{k,n}D_{l,2n}$ et $D_{k,2n}D_{l,n}$. Les produits contenant ces termes sont

$$\pm\det\begin{pmatrix} a_{k,1}x_{1,n}^{a_{k,1}-1}x_{2,n}^{a_{k,2}} & a_{k,2}x_{1,n}^{a_{k,1}}x_{2,n}^{a_{k,2}-1} \\ a_{l,1}x_{1,n}^{a_{l,1}-1}x_{2,n}^{a_{l,2}} & a_{l,2}x_{1,n}^{a_{l,1}}x_{2,n}^{a_{l,2}-1} \end{pmatrix}\delta_{k,l}$$

$$= \pm\det\begin{pmatrix} a_{k,1} & a_{k,2} \\ a_{l,1} & a_{l,2} \end{pmatrix} x_{1,n}^{a_{k,1}+a_{l,1}-1}x_{2,n}^{a_{k,2}+a_{l,2}-1}\delta_{k,l}$$

où $\delta_{k,l}$ désigne le déterminant attendu.

Comme nos éléments sont ordonnés si $a_k + a_l = a_{2n-1} + a_{2n}$, alors $k, l = 2n - 1, 2n$.

Donc, pour prouver que le déterminant n'est pas le polynôme nul il suffit de prouver que $\det\begin{pmatrix} a_{2n,1} & a_{2n,2} \\ a_{2n-1,1} & a_{2n-1,2} \end{pmatrix}\delta_{2n-1,2n}$ n'est pas le polynôme nul.

Par récurrence, $\delta_{2n-1,2n}$ ne l'est pas.

Et par construction, le déterminant ne peut être nul. Donc, A_n convient.

On a donc vu que l'on pouvait trouver un tel ensemble dans le cas $r = 2$, pour le cas général, on va utiliser le théorème d'Alexander-Hirschowitz.

Theorème 2.48. *(Alexander-Hirschowitz)*

Soit V le $\mathbb{C}$-espace vectoriel constitué des polynômes dont tous les monômes sont de degré d en r variables. Soient n points dans $\mathbb{P}^{r-1}$, et $W \subset V$ le sous-espace qui contient les polynômes dont les dérivées partielles s'annulent en ces n points. Alors W a codimension :

$$\min(rn, \dim V),$$

sauf dans certains cas exceptionnels qui sont exclus si $d \geq 5$.

Lemme 2.49. *Soit $n \geq 6, 3 \leq r \leq n$ et d est tel que $\binom{d+r-1}{r-1} > rn$. Alors il existe un ensemble A constitué de rn éléments $a \in \mathbb{Z}^r_{\geq 0}$ de degré total d (la somme des coordonnées de chaque élément fait d) et tel que le déterminant $\det(DTr_{a,n})_{a\in A}$ n'est pas le polynôme nul.*

On remarque que pour trouver cet ensemble, on fixe le degré des éléments, et on pourrait se demander s'il était possible de trouver un ensemble où tous nos éléments ont un degré au plus $d' < d$, comme c'est le cas pour $r = 2$.

Finalement, deux derniers lemmes sont nécessaires, 2.42 prouvé par Ellenberg et Venkatesh dans [**EV**], et le lemme suivant.

Lemme 2.50. *Soit K un corps de nombre de degré n, alors il existe une base intégrale $\{\beta_1, \cdots, \beta_n\}$ de son anneau des entiers tel que $|\beta_i| \ll D_K^{\frac{1}{n}}$, pour tout i.*

On peut finalement prouver le théorème. Soit $r \geq 3$ et d comme dans le lemme 2.49. On sait par ce lemme qu'il existe un sous-ensemble de $\mathbb{Z}^r_{\geq 0}$,A, constitué de rn éléments de degré d, tel que le déterminant de la matrice des premières dérivées partielles des polynômes associés n'est pas le polynôme nul. Par le premier lemme, on sait qu'il existe un polynôme $P : \mathbb{A}^{nr}(\mathbb{C}) \to \mathbb{A}^1(\mathbb{C})$ tel que s'il existe x_0 avec $P(x_0) \neq 0$, alors l'ensemble

$$\{x \in \mathbb{A}^{nr}(\mathbb{C}) : Tr_{a,n}(x) = Tr_{a,n}(x), \forall a \in A\}$$

a $O_{d,r,n}(1)$ éléments. On peut aussi définir un polynôme qui peut être comparé à un discriminant sur la première copie de $\mathbb{A}^{nr}(\mathbb{C})$.

Définition 2.51. *Posons*

$$\begin{aligned} Disc^{(1)} : \mathbb{A}^{nr}(\mathbb{C}) &\to \mathbb{A}^1(\mathbb{C}) \\ x &\mapsto \prod_{1\leq i\neq j\leq n} (x_{1,i} - x_{1,j}). \end{aligned}$$

Soit K un corps de nombres de degré n, alors si on a $\alpha_1, \cdots, \alpha_r \in O_K$, on obtient un élément de $\mathbb{C}^n$ et donc un point $x_\alpha \in \mathbb{A}^{nr}(\mathbb{C})$.

En utilisant les lemmes 2.42 et 2.50, on trouve $\alpha_1, \cdots, \alpha_r \in O_K$ avec $|\alpha_i| \ll D_K^{\frac{1}{n}}$ et $P(x_\alpha) \neq 0, Disc^{(1)}(x_\alpha) \neq 0$. Comme $Disc^{(1)}(x_\alpha) \neq 0$, x_α caractérise l'extension K.

Ainsi, K est déterminé, à $O_{d,r,n}(1)$ choix, par toutes les évalutions $Tr_{a,n}(x_\alpha), a \in A$. On a rn telles évaluations, qui sont des éléments ayant une valeur absolue de l'ordre $\mathcal{O}(X^{\frac{d}{n}})$. Donc, on a $\mathcal{O}(X^{rd})$ choix pour K.

Pour $r = 2$, on peut prendre l'ensemble A_n défini précédemment. Comme chaque $Tr_{a,n}(x_\alpha)$ est un élément ayant une valeur absolue de l'ordre de $\mathcal{O}(X^{\frac{deg(a)}{n}})$, alors

$$\sum_{a \in A} deg(a) = 2nd - \frac{d(d-1)(d+4)}{6}$$

où d est le plus petit entier tel que $\binom{d+2}{2} \geq 2n+1$.

Finalement, $N^n(X) \ll X^{2d - \frac{d(d-1)(d+4)}{6n}}$, et on obtient la première partie du théorème en voyant que $d \leq 2\sqrt{n}$.

On conclut l'autre partie du théorème, en prenant $d \approx \dfrac{\ln n}{2 \ln 2} \approx r - 1$.

Remarque 2.52. *En prenant comme ensemble A, l'ensemble des rn premiers éléments de $\mathbb{Z}^r_{\geq 0}$ ordonnés par $i_1 + \cdots + i_r$ croissants, puis $i_2 + \cdots + i_r$ croissant, et ainsi de suite jusqu'à i_r croissant, alors on considère des éléments ayant une somme au plus d' avec un $d' < d$. On peut ainsi obtenir un résultat un peu meilleur. Le fait de prendre cet ensemble semble être possible au vu de ce qu'il se passe pour de petits r, néanmoins asymptotiquement d' et d vont être très proches.*

Il me semble que l'on pourrait obtenir un résultat de l'ordre de $N^n(X) \ll X^{\ln(n)^2 - \frac{A}{\sqrt{\ln n}}}$ avec A une constante, ce qui reste le même résultat asymptotiquement.

— Couveignes, quant à lui, a montré dans l'article [**Couv**] le résultat suivant :

Theorème 2.53. *Il existe une constante M, tel que si K est un corps de nombre de degré $n \geq M$, et de discriminant $Disc(K)$, alors il existe des entiers $r, d \leq M \ln n$ tels que $\binom{r+d}{r} \geq Mn \ln n$ et il existe $E_1, \cdots, E_r \in \mathbb{Z}[x_1, \cdots, x_r]$ de degré d dont les coefficients sont bornés par $n^{M \ln n} |Disc(K)|^{\frac{M \ln n}{n}}$ et tel que le schéma défini par*

$$E_1 = \cdots = E_r = 0 \text{ et } \det(\frac{\partial E_i}{\partial x_j}) \neq 0$$

contient Spec(K) dans une de ses composantes irréductibles.

Ainsi, il existe C une constante typiquement de l'ordre de M^3, tel que si $n \geq C$, alors $N^n(X) \leq n^{Cn(\ln n)^3} X^{C(\ln n)^3}$.

Contrairement aux deux précédents articles, Couveignes ne choisit pas des polynômes identiques pour toutes les extensions de $\mathbb{Q}$ qu'il évalue et dont l'évaluation caractérise chacune des extensions de $\mathbb{Q}$, ici, il dit que pour chaque corps de nombres, on peut trouver r(qui va être de l'ordre de $\ln n$) polynômes qui caractériseront chaque extension.

Les arguments utilisés regroupent des idées déjà présentées donc je ne rentrerai pas ici dans plus de détails.

2.4.2 Borne inférieure

Nous allons maintenant nous intéresser à une borne inférieure, cette section est tirée de la preuve d'Ellenberg et Venkatesh, [**EV**], avec quelques modifications.

Ici, nous nous intéresserons à $\mathbb{Q}$ comme corps de base, pour présenter une preuve plus "simple" mais le résultat reste vrai si on prend comme corps de base K un quelconque corps de nombre, simplement il faut une autre preuve pour arriver au lemme 2.55.

Le résultat que nous voulons prouver est le suivant :

Theorème 2.54. *Soit $A > 1.564$ une constante, alors pour tout entier naturel n,*

$$N^n(X) \gg X^{\frac{1}{2}+\frac{1}{2An\ln^2 n}},$$

où les notations sont les mêmes que dans les sections précédentes.

Soit L un corps de nombre de degré n qui ne possède pas de sous-corps autre que $\mathbb{Q}$, alors O_L^0 est un réseau de rang $n-1$. On peut appliquer le deuxième théorème de Minkowski, évoqué dans la proposition 2.12.

On peut donc trouver $a_1 \leq a_2 \leq \cdots \leq a_{n-1}$ qui sont les minimas successifs au sens de Minkowski. Comme L ne possède pas de sous-corps propre, on a pour $1 \leq j \leq n-2$,

$a_1 a_j \gg a_{j+1}$.

De plus, par le deuxième théorème de Minkowski, $a_1 \cdots a_{n-1} \approx \sqrt{D_L}$. On obtient donc

$$\begin{aligned}\sqrt{D_L} &\ll a_1^{1+2(n-2)+\frac{(n-2)(n-3)}{2}} \\ &\ll a_1^{1+\frac{(n-2)(n+1)}{2}} \\ &\ll a_1^{\frac{n(n-1)}{2}}.\end{aligned}$$

On obtient donc le lemme suivant :

Lemme 2.55. *Soit L une extension finie de $\mathbb{Q}$ de degré n qui ne possède pas de sous-corps. Alors, si $x \in O_L^0$, on a $||x|| \gg |Disc(L)^{\frac{1}{n(n-1)}}|$.*

Définition 2.56. *Pour $Y > 0$, on peut définir $S(Y) := \{x \in \overline{\mathbb{Q}}, [\mathbb{Q}(x) : \mathbb{Q}] = n, Tr(x) = 0, \exists P \in \mathbb{Z}[X]$ unitaire tel que $P(x) = 0\}$.*

En regardant les polynômes caractéristiques, et notamment les coefficients, on trouve :

$$\begin{aligned}|S(Y)| &\gg Y^{2+\cdots+n} \\ &\gg Y^{\frac{n(n+1)}{2}-1} \\ &\gg Y^{\frac{(n+2)(n-1)}{2}}.\end{aligned}$$

Soit L un corps de nombre de degré n, alors s'il existe $x \in L \cap S(Y)$, on doit avoir $|Disc(L)| \ll Y^{n(n-1)}$.

Ainsi, on obtient :

$$\sum_{[L:\mathbb{Q}]=n, |Disc(L)|<cY^{n(n-1)}} (\frac{1}{Disc(L)})^{\frac{1}{n}} \gg |S(Y)|Y^{-(n-1)}$$
$$\gg Y^{\frac{n(n-1)}{2}}.$$

Prenons A une constante $> c = 1.564$, alors on sait que pour tout $n \geq 6, N^n(X) \ll X^{c\ln^2 n}$ (théorème 2.44), et comme on sait le résultat vrai pour $n < 6$, cela suffit. Ainsi,

$$\sum_{[L:\mathbb{Q}]=n, Disc(L)<Y^{\frac{n(n-1)}{2A\ln^2 n}}} (\frac{1}{Disc(L)})^{\frac{1}{n}} \ll Y^{\frac{n(n-1)}{2}-\delta},$$

avec $\delta > 0$.

On peut donc commencer la sommation à $Disc(L) \geq Y^{\frac{n(n-1)}{2A\ln^2 n}}$.

Donc, $N^n(Y^{n(n-1)})Y^{-\frac{n-1}{2A\ln^2 n}} \gg Y^{\frac{n(n-1)}{2}}$.

Ainsi,

$$N^n(Y) \gg Y^{\frac{1}{2}+\frac{1}{2An\ln^2 n}}.$$

Références

[Bhar3] M. Barghava Higher composition laws III : The parametrization of quartic rings, 2004.

[Bhar] M. Barghava The density of discriminants of quartic rings and fields, 2005.

[Bhar2] M. Barghava The density of discriminants of quintic rings and fields, 2010.

[CDO] H. Cohen, F. Diaz, M. Olivier Enumerating quartic dihedral extensions of $\mathbb{Q}$, 2002.

[Couv] J-M. Couveignes Enumerating number fields, 2019.

[EV] J. Ellenberg, A. Venkatesh The number of extensions of a number field with bounded discriminant, 2006.

[LT] R. Lemke, F. Thorne Upper bounds on number fields of given degree and bounded discriminant, 2020.