Enumerating number fields

Jean-Marc Couveignes

ENUMERATING NUMBER FIELDS

JEAN-MARC COUVEIGNES

ABSTRACT. We construct small models of number fields and deduce a better bound for the number of number fields of given degree and bounded discriminant.

CONTENTS

1. INTRODUCTION

We prove the two theorems below.

Theorem 1 (Number fields have small models)**.** *There exists a positive constant $\mathcal{Q}$ such that the following is true. Let $\mathbf{K}$ be a number field of degree $n \geqslant \mathcal{Q}$ and root discriminant $\delta_{\mathbf{K}}$ over $\mathbf{Q}$. There exist integers $r \leqslant \mathcal{Q}\log n$ and $d \leqslant \mathcal{Q}\log n$ such that $\binom{d+r}{r} \leqslant \mathcal{Q}n\log n$ and there exists r polynomials E_1, E_2, …, E_r of degree $\leqslant d$ in $\mathbf{Z}[x_1,\dots,x_r]$ all having coefficients bounded in absolute value by $(n\delta_{\mathbf{K}})^{\mathcal{Q}\log n}$ such that the (smooth and zero-dimensional affine) scheme with equations*

$$E_1 = E_2 = \cdots = E_r = 0 \text{ and } \det\left(\partial E_i/\partial x_j\right)_{1\leqslant i,\, j\leqslant r} \neq 0$$

contains $\operatorname{Spec}\mathbf{K}$ as one of its irreducible components.

Theorem 2 (Number fields with bounded discriminant)**.** *There exists a positive constant $\mathcal{Q}$ such that the following is true. Let $n \geqslant \mathcal{Q}$ be an integer. Let $H \geqslant 1$ be an integer. The number of isomorphism classes of number fields with degree n and discriminant $\leqslant H$ is $\leqslant n^{\mathcal{Q}n\log^3 n} H^{\mathcal{Q}\log^3 n}$.*

The meaning of Theorem 1 is that we can describe a number field using few parameters in some sense. We have a short description of it as a quotient of a finite algebra : the smooth zero-dimensional part of a complete intersection of small degree and small height in a projective space of small dimension.

Theorem 2 improves on previous results by Schmidt [18] and Ellenberg-Venkatesh [12].

Date: August 11, 2020.

Schmidt uses Minkowski theorem on successive minima of the lattice of integers and obtains a bound $H^{\frac{n+2}{4}}$ times a function of n for the number $N_n(H)$ of number fields with degree n and discriminant bounded by H in absolute value.

Ellenberg and Venkatesh consider r-uples of small integers $(\alpha_i)_{1\leqslant i\leqslant r}$ in $\mathbf{K}$ and define the mixed trace $\chi_\sigma = \mathrm{Tr}(\prod_i \alpha_i^{\sigma_i})$ for every r-uple $\sigma = (\sigma_i)_i$ of rational integers. They show how to reconstruct the multiplicative structure of $\mathbf{K}$ from a collection of χ_σ where σ runs over a subset $\Sigma \in \mathbf{N}^r$ of managable size. As a result they prove $N_n(H) \ll_n H^{\exp(\mathcal{Q}\sqrt{\log n})}$ with a subexponential (halfway between n and polynomial in $\log n$) exponent in H. The semigroup $\mathbf{N}^r$ of all possible σ plays an important role in their proof.

We too make use of a few small integers in $\mathbf{K}$. We find small algebraic relations between them using Minkowski theorem. Proving that the ideal of relations can be generated by a few of such small relations seems out of reach to us but we can cope with local equations. Familiar generic well-posedness results in multivariate Lagrange interpolation shows through Ellenberg and Venkatesh's work e.g. in the proof of [12, Lemma 2.3]. Similarly the key to find local equations is a generic well-posedness result in multivariate Hermite interpolation. Such a result has been proven by Alexander and Hirschowitz. We use it to produce a small projective model of $\mathrm{Spec}\,\mathbf{K}$ in dimension and degree $O(\log n)$ and with bit size of order $n(\log n)^3(\log \delta_{\mathbf{K}} + \log n)$. As a consequence one can lower the exponent of H in an upper bound for $N_n(H)$ down to a polynomial in $\log n$, namely $O(\log^3 n)$.

Following the pre-publication of the present text Lemke and Thorne [17] improved the latter exponent to $O(\log^2 n)$ by applying the Alexander-Hirshowitz theorem to prove the local smoothness of the multisymmetric map of Ellenberg and Venkatesh.

It is sometimes conjectured that $N_n(H) \sim c_n H$ for $n \geqslant 2$ where c_n does not depend on H. This is known for $2 \leqslant n \leqslant 5$ according to work by Davenport and Heilbronn [11] for $n = 3$, and Bhargava [4, 5] for $n = 4, 5$. Cohen, Diaz and Olivier have collected experimental data e.g. in [8, 9, 10] suggesting that $N_n(H)$ should grow linearly in H for fixed $n \geqslant 2$. Malle has stated in [14] a more general and accurate conjecture on the distribution of Galois groups of number fields that would confirm this intuition.

In Section 2 we recall notation, definitions and elementary results from the geometry of numbers. In Section 3 we construct models for number fields as irreducible components of complete intersections with small height in low dimensional projective spaces. The last section is devoted to the proof of Theorem 1 and Theorem 2.

The author thanks Pascal Autissier, Karim Belabas, Georges Gras and Christian Maire for their comments and suggestions. This study has been carried out with financial support from the French State, managed by the French National Research Agency(ANR) in the frame of the Programmes FLAIR (ANR-17-CE40-0012 ANR-10-IDEX-03-02) and CLapCLap (ANR-18-CE40-0026).

2. Short integers

Let $\mathbf{K}$ be a number field and let n be the degree of $\mathbf{K}$ over $\mathbf{Q}$. Let $\mathbf{O}$ be the ring of integers of $\mathbf{K}$. Let $(\rho_i)_{1\leqslant i\leqslant r}$ be the r real embeddings of $\mathbf{K}$. Let $(\sigma_j, \bar\sigma_j)_{1\leqslant j\leqslant s}$ be the $2s$ complex embeddings

of $\mathbf{K}$. We also denote by $(\tau_k)_{1\leqslant k\leqslant n}$ the $n = r + 2s$ embeddings of $\mathbf{K}$. Let

$$\mathbf{K_R} = \mathbf{K} \otimes_{\mathbf{Q}} \mathbf{R} = \mathbf{R}^r \times \mathbf{C}^s$$

be the Minkowski space. We follow the presentation in [16, Chapitre 1, §5]. An element x of $\mathbf{K_R}$ can be given by r real components $(x_\rho)_\rho$ and s complex components $(x_\sigma)_\sigma$. So we write $x = ((x_\rho)_\rho, (x_\sigma)_\sigma)$. For such an x in $\mathbf{K_R}$ we denote by $||x||$ the maximum of the absolute values of its $r + s$ components. The canonical metric on $\mathbf{K_R}$ is defined by

$$< x, y >= \sum_{1\leqslant i\leqslant r} x_i y_i + \sum_{1\leqslant j\leqslant s} x_j \bar{y}_j + \bar{x}_j y_j.$$

In particular the contribution of complex embeddings is counted twice

$$< x, x >= \sum_{1\leqslant i\leqslant r} x_i^2 + 2 \sum_{1\leqslant j\leqslant s} |x_j|^2.$$

The corresponding Haar measure is said to be canonical also. The canonical measure of the convex body $\{x, ||x|| \leqslant 1\}$ is

$$2^r (2\pi)^s \geqslant 2^n.$$

The map $a \mapsto a \otimes 1$ injects $\mathbf{K}$ and $\mathbf{O}$ into $\mathbf{K_R}$. For every non-zero x in $\mathbf{O}$ we have

$$||x|| \geqslant 1.$$

Let $(\alpha_i)_{1\leqslant i\leqslant n}$ be any $\mathbf{Z}$-basis of $\mathbf{O}$. Set $A = (\tau_j(\alpha_i))_{1\leqslant i,j\leqslant n}$. The product $A\bar{A}^t$ is the Gram matrix $B = (< \alpha_i, \alpha_j >)_{1\leqslant i,j\leqslant n}$ of the canonical form in the basis $(\alpha_i)_i$. This is a real symmetric positive matrix. The volume of $\mathbf{O}$ according to the canonical Haar measure is

$$v_{\mathbf{O}} = \sqrt{\det(B)} = |\det(A)|.$$

We let

$$d_{\mathbf{K}} = \det(AA^t)$$

be the discriminant of $\mathbf{K}$ and we denote by

$$\delta_{\mathbf{K}} = |d_{\mathbf{K}}|^{\frac{1}{n}}$$

the root discriminant. The square of the volume of $\mathbf{O}$ is $|d_{\mathbf{K}}|$. Applying Minkowski's second theorem [19, Lecture III, §4, Theorem 16] to the gauge function $x \mapsto ||x||$ we find that $\mathbf{O}$ contains n linearly independant elements $\omega_1, \omega_2, \ldots, \omega_n$ such that

$$\prod_{1\leqslant i\leqslant n} ||\omega_i|| \leqslant v_{\mathbf{O}} = \delta_{\mathbf{K}}^{n/2}.$$

We assume that the sequence $i \mapsto ||\omega_i||$ is non-decreasing and deduce that

$$||\omega_i|| \leqslant v_{\mathbf{O}}^{1/(n+1-i)}$$

for every $1 \leqslant i \leqslant n$. This inequality is a bit unsatisfactory because it provides little information on the largest ω_i. To improve on this estimate we use the fact that $\mathbf{O}$ is an integral domain. We let $m = \lceil (n+1)/2 \rceil$ be the smallest integer bigger than $n/2$. On the one hand

$$||\omega_i|| \leqslant \delta_{\mathbf{K}}$$

for every $1 \leqslant i \leqslant m$. On the other hand the products

$$(\omega_i \omega_j)_{1 \leqslant i,j \leqslant m}$$

generate a $\mathbf{Z}$-module of rank n. Otherwise there would exist a non-zero linear form $f : \mathbf{O} \to \mathbf{Z}$ vanishing on these products. So the m forms $f \circ \omega_i$ would be orthogonal to the m vectors ω_j. Then $m + m \leqslant n$. A contradiction. We deduce that all the successive minima of $\mathbf{O}$ are

$$\leqslant \delta_{\mathbf{K}}^2.$$

In other words $\mathbf{O}$ is well balanced.

Proposition 1 (Number fields have small integers)**.** *The ring of integers* $\mathbf{O}$ *of a number field* $\mathbf{K}$ *with degree* n *and root discriminant* $\delta_{\mathbf{K}}$ *contains* n *linearly independant elements* $(\alpha_i)_{1 \leqslant i \leqslant n}$ *over* $\mathbf{Z}$ *such that all the absolute values of all the* α_i *are* $\leqslant \delta_{\mathbf{K}}^2$.

Bhargava, Shankar, Taniguchi, Thorne, Tsimerman, and ZhaoSee prove in [3][Theorem 3.1] a similar statement which is somewhat stronger but less accurate.

3. Small models

Let

$$\mathbf{K}_{\mathbf{C}} = \mathbf{K} \otimes_{\mathbf{Q}} \mathbf{C} = \mathbf{C}^n.$$

Let $d \geqslant 5$ and $r \geqslant 1$ be two integers. We assume that

$$n(r+1) \leqslant \binom{d+r}{d}.$$

Let M be the set of monomials of total degree $\leqslant d$ in the r variables $x_1, \ldots, x_r$. We have

$$\mathbf{A}^r_{\mathbf{C}} = \operatorname{Spec} \mathbf{C}[x_1, \ldots, x_r] \subset \operatorname{Proj} \mathbf{C}[x_0, x_1, \ldots, x_r] = \mathbf{P}^r_{\mathbf{C}}.$$

Let $V_{\mathbf{C}}$ be the $\mathbf{C}$-linear space generated by M. We may associate to every element in M the corresponding degree d monomial in the $r+1$ variables $x_0, x_1, \ldots, x_r$. We thus identify $V_{\mathbf{C}}$ with $H^0(\mathcal{O}_{\mathbf{P}^r_{\mathbf{C}}}(d))$, the space of homogeneous polynomials of degree d.

Let $(P_\tau)_\tau$ be n pairwise distinct points in

$$\mathbf{C}^r = \mathbf{A}^r(\mathbf{C}).$$

The P_τ are indexed by the n embeddings of $\mathbf{K}$. These n points form a set (a reduced zero-dimensional subscheme of $\mathbf{P}^r_{\mathbf{C}}$) called P. We call $\mathcal{I}$ the corresponding ideal sheaf on $\mathbf{P}^r_{\mathbf{C}}$. We denote by $2P$ the scheme associated with $\mathcal{I}^2$. It consists of n double points. We say that the scheme $2P$ is well poised (or non-special) in degree d if it imposes $n(r+1)$ independent conditions on degree d homogeneous polynomials. Equivalently, the map

$$H^0(\mathcal{O}_{\mathbf{P}^r}(d)) \to H^0(\mathcal{O}_{2P}(d))$$

is surjective. This is the case if and only if the $n(r+1) \times \binom{d+r}{d}$ matrix

$$\mathcal{M}^1_P = [(m(P_\tau))_{\tau, m \in M}, (\partial m/\partial x_1(P_\tau))_{\tau, m \in M}, (\partial m/\partial x_2(P_\tau))_{\tau, m \in M}, \ldots, (\partial m/\partial x_r(P_\tau))_{\tau, m \in M}]$$

has maximal rank $n(r+1)$. We note that $\mathcal{M}^1_P$ consists of $r+1$ blocks of size $n \times \binom{d+r}{d}$ piled vertically. It has maximal rank for a generic P when $d \geqslant 5$, according to a theorem of Alexander

[1], generalized by Alexander and Hirschowitz [2]. Chandler [7, Theorem 1] provides a simpler statement and proof. The recent exposition and simplification by Brambilla and Ottaviani [6] is very useful also.

We now let $(\alpha_i)_{1\leqslant i\leqslant n}$ be n linearly independant short elements in $\mathbf{O}$ as in Proposition 1. We pick rn rational integers $(u_{i,j})_{1\leqslant i\leqslant n,\,1\leqslant j\leqslant r}$ and we set

$$\kappa_j = \sum_{1\leqslant i\leqslant n} u_{i,j}\alpha_i$$

for $1 \leqslant j \leqslant r$. Let

$$\epsilon_{\mathbf{Q}} : \mathbf{Q}[x_1, \ldots, x_r] \to \mathbf{K}$$

be the homomorphism of $\mathbf{Q}$-algebras sending x_j to κ_j for $1 \leqslant j \leqslant r$. Let

$$e_{\mathbf{Q}} : \operatorname{Spec} \mathbf{K} \to \mathbf{A}^r_{\mathbf{Q}} \subset \mathbf{P}^r_{\mathbf{Q}}$$

be the corresponding morphism of schemes. Tensoring $\epsilon_{\mathbf{Q}}$ by $\mathbf{R}$ we obtain an homomorphism

$$\epsilon_{\mathbf{R}} : \mathbf{R}[x_1, \ldots, x_r] \to \mathbf{K}_{\mathbf{R}}$$

sending x_j to $((\rho(\kappa_j))_\rho, (\sigma(\kappa_j))_\sigma)$. We call

$$e_{\mathbf{R}} : \operatorname{Spec} \mathbf{K}_{\mathbf{R}} \to \mathbf{A}^r_{\mathbf{R}} \subset \mathbf{P}^r_{\mathbf{R}}$$

the corresponding morphism of schemes. We define

$$\epsilon_{\mathbf{C}} : \mathbf{C}[x_1, \ldots, x_r] \to \mathbf{K}_{\mathbf{C}}$$

and

$$e_{\mathbf{C}} : \operatorname{Spec} \mathbf{K}_{\mathbf{C}} \to \mathbf{A}^r_{\mathbf{C}} \subset \mathbf{P}^r_{\mathbf{C}}$$

similarly. In particular $\epsilon_{\mathbf{C}}$ maps x_j onto $(\tau(\kappa_j))_\tau$.

We now consider the points $(P_\tau)_\tau$ such that $x_0(P_\tau) = 1$ and

$$(x_j(P_\tau))_\tau = \left(\sum_{1\leqslant i\leqslant n} u_{i,j}\tau(\alpha_i) \right)_\tau,$$

for $1 \leqslant j \leqslant r$ or equivalently

$$P_\tau = (\sum_{1\leqslant i\leqslant n} u_{i,j}\tau(\alpha_i))_{1\leqslant j\leqslant r} \in \mathbf{C}^r = \mathbf{A}^r(\mathbf{C}) \subset \mathbf{P}^r(\mathbf{C}).$$

The maximal minors of the corresponding matrix $\mathcal{M}^1_P$ are polynomials of degree $\leqslant dn(r+1)$ in each of the $u_{i,j}$ and one of them is not identically zero. The latter determinant cannot vanish on the cartesian product $[0, dn(r+1)]^{nr}$. Thus there exist nr rational integers $u_{i,j}$ in the range

$$[0, dn(r+1)]$$

such that the corresponding scheme $2P$ is well poised. We assume that the $u_{i,j}$ meet these conditions.

Since $2P$ is well poised, P is well poised also. So $e_{\mathbf{Q}}$, $e_{\mathbf{R}}$ and $e_{\mathbf{C}}$ are closed immersions. In order to describe them efficiently we look for polynomials with degree $\leqslant d$ and small integer coefficients vanishing at P. We denote by $V_{\mathbf{R}} = \mathbf{R}[x_1, \ldots, x_r]_d$ the $\mathbf{R}$-vector space of polynomials in $\mathbf{R}[x_1, \ldots, x_r]$ of degree $\leqslant d$. There is a unique $\mathbf{R}$-bilinear form on $V_{\mathbf{R}}$ that turns the set M

of monomials into an orthonormal basis. The lattice of relations with integer coefficients and degree $\leqslant d$ is the intersection between $\mathrm{Ker}\,\epsilon_{\mathbf{R}}$ and

$$V_{\mathbf{Z}} = \mathbf{Z}[x_1, \ldots, x_r]_d.$$

This is a free $\mathbf{Z}$-module $\mathcal{L} \subset V_{\mathbf{R}}$ of rank

$$\ell = \binom{d+r}{d} - n.$$

We set $L = \mathcal{L} \otimes_{\mathbf{Q}} \mathbf{R}$ the underlying $\mathbf{R}$-vector space and $L^\perp$ its orthogonal complement in $V_{\mathbf{R}}$. We denote by $\mathcal{L}^\perp$ the intersection $\mathcal{L}^\perp = L^\perp \cap V_{\mathbf{Z}}$. Since $V_{\mathbf{Z}}$ is unimodular, $\mathcal{L}$ and $\mathcal{L}^\perp$ have the same volume. See [15, Corollary 1.3.5.]. We denote by $\hat{\mathbf{O}} = \mathrm{Hom}(\mathbf{O}, \mathbf{Z})$ the dual of $\mathbf{O}$, the ring of integers of $\mathbf{K}$, as a $\mathbf{Z}$-module. We call

$$\epsilon_{\mathbf{Z},d} : \mathbf{Z}[x_1, \ldots, x_r]_d \to \mathbf{O}$$

the evaluation map in degree $\leqslant d$. We observe that $\mathcal{L}^\perp$ contains the image of $\hat{\mathbf{O}}$ by the transpose map

$$\hat{\epsilon}_{\mathbf{Z},d} : \hat{\mathbf{O}} \to \mathbf{Z}[x_1, \ldots, x_r]_d$$

where we have identified $\mathbf{Z}[x_1, \ldots, x_r]_d$ with its dual thanks to the canonical bilinear form. So the volume of $\mathcal{L}$ is bounded from above by the volume of $\hat{\epsilon}_{\mathbf{Z},d}(\hat{\mathbf{O}})$. We consider the matrix

$$\mathcal{M}_P^0 = [(m(P_\tau))_{\tau, m \in M}]$$

of the map $\epsilon_{\mathbf{C},d} = \epsilon_{\mathbf{Z},d} \otimes_{\mathbf{Z}} \mathbf{C}$ in the canonical bases. If we prefer to use an integral basis of $\mathbf{O}$ on the right we should multiply $\mathcal{M}_P^0$ on the left by the inverse T of the matrix of a basis of $\mathbf{O}$ in the canonical basis. We deduce that the square of the volume of $\hat{\epsilon}_{\mathbf{Z},d}(\hat{\mathbf{O}})$ is the determinant of $T\mathcal{M}_P^0(\mathcal{M}_P^0)^t T^t$. Since $T\mathcal{M}_P^0$ has real coefficients we have

$$\det(T\mathcal{M}_P^0(\mathcal{M}_P^0)^t T^t) = \det\left(T\mathcal{M}_P^0 \left(\overline{\mathcal{M}_P^0}\right)^t \bar{T}^t\right) = \det\left(\mathcal{M}_P^0 \left(\overline{\mathcal{M}_P^0}\right)^t\right) / |d_{\mathbf{K}}|.$$

So the square of the volume of the lattice of relations is bounded by the determinant of the hermitian positive definite matrix $\mathcal{M}_P^0 \left(\overline{\mathcal{M}_P^0}\right)^t$ divided by $|d_{\mathbf{K}}|$.

Recall that the coefficients in $\mathcal{M}_P^0$ are degree $\leqslant d$ monomials in the $\kappa_j = \sum_{1 \leqslant i \leqslant n} u_{i,j}\alpha_i$. The coefficients $u_{i,j}$ are bounded form above by $dn(r+1)$. All the absolute values of the α_i are bounded from above by $\delta_{\mathbf{K}}^2$. So the coefficients in $\mathcal{M}_P^0$ are bounded from above by

$$(n^2 d(r+1))^d \delta_{\mathbf{K}}^{2d}.$$

The coefficients in $\mathcal{M}_P^0 \left(\overline{\mathcal{M}_P^0}\right)^t$ are bounded from above by

$$\mathfrak{D} = \binom{d+r}{d} (n^2 d(r+1))^{2d} \delta_{\mathbf{K}}^{4d}.$$

The matrix $\mathcal{M}_P^0 \left(\overline{\mathcal{M}_P^0}\right)^t$ being hermitian positive definite, its determinant is bounded from above by the product of the diagonal terms. We deduce that the volume of the lattice $\mathcal{L}$ of relations is

bounded from above by $\mathfrak{D}^{n/2}$. Recall that the dimension of $\mathcal{L}$ is

$$\ell = \binom{d+r}{d} - n.$$

For any x in $V_{\mathbf{R}}$ we denote by $\|x\|$ the ℓ_2-norm in the monomial basis. The volume of the sphere $\{x \in L, \|x\| \leqslant 1\}$ is $\geqslant 2^{\ell}\ell^{-\ell/2}$. Applying Minkowski's second theorem [19, Lecture III, §4, Theorem 16] to the gauge function $x \mapsto \|x\|$ we find that $\mathcal{L}$ contains ℓ linearly independant elements $E_1, E_2, \ldots, E_\ell$ such that

$$\prod_{1 \leqslant i \leqslant \ell} \|E_i\| \leqslant \ell^{\ell/2}\mathfrak{D}^{n/2}.$$

We assume that the sequence $i \mapsto \|E_i\|$ is non-decreasing and deduce that the size of the i-th equation is bounded from above

$$\|E_i\| \leqslant \ell^{\frac{\ell}{2(\ell+1-i)}}\mathfrak{D}^{\frac{n}{2(\ell+1-i)}}$$

for every $1 \leqslant i \leqslant \ell$. Again, this inequality is a bit unsatisfactory because it provides little information on the largest equations. This time we see no other way around than forgetting the last $n-1$ equations. On the one hand

$$\|E_i\| \leqslant \ell^{\ell/2n}\mathfrak{D}^{1/2}$$

for every $1 \leqslant i \leqslant \ell + 1 - n$.

On the other hand the scheme $2P$ is well poised and the $\mathbf{C}$-vector space generated by the E_i for $1 \leqslant i \leqslant \ell + 1 - n$ has codimension $n - 1 < n$ in $L \otimes_{\mathbf{R}} \mathbf{C}$. So there exists at least one embedding τ such that the $(\ell + 1 - n) \times r$ matrix

$$((\partial E_i/\partial x_j)(P_\tau))_{1 \leqslant i \leqslant \ell+1-n,\, 1 \leqslant j \leqslant r}$$

has maximal rank r. In more geometric terms the $\mathbf{C}$-vector space generated by the $\ell + 1 - n$ first equations $(E_i)_{1 \leqslant i \leqslant \ell+1-n}$ surjects onto the cotangent space to $\mathbf{P}^r_{\mathbf{C}}$ at the geometric point P_τ for at least one τ. This means that there exist r integers $1 \leqslant i_1 < i_2 < \cdots < i_r \leqslant \ell + 1 - n$ such that the minor determinant

$$\det\left((\partial E_{i_k}/\partial x_j)(P_\tau)\right)_{1 \leqslant k,\, j \leqslant r}$$

is non-zero for some τ and thus for all τ by Galois action.

Proposition 2 (Number fields have small models)**.** *Let $\mathbf{K}$ be a number field of degree n and root discriminant $\delta_{\mathbf{K}}$ over $\mathbf{Q}$. Let $d \geqslant 5$ and $r \geqslant 1$ be rational integers such that*

$$n(r+1) \leqslant \binom{d+r}{d}.$$

There exists r polynomials $E_1, E_2, \ldots, E_r$ of degree $\leqslant d$ in $\mathbf{Z}[x_1, \ldots, x_r]$ having coefficients bounded in absolute value by

$$\ell^{\ell/2n} \times \binom{d+r}{d}^{1/2} (n^2 d(r+1))^d \delta_{\mathbf{K}}^{2d}$$

where

$$\ell = \binom{d+r}{d} - n,$$

and such that the (smooth and zero-dimensional affine) scheme with equations

$$E_1 = E_2 = \cdots = E_r = 0 \text{ and } \det\left(\partial E_i/\partial x_j\right)_{1\leqslant i,\, j\leqslant r} \neq 0$$

contains $\operatorname{Spec}\mathbf{K}$ *as one of its irreducible components.*

4. Proof of main results

In this section, the notation $\mathcal{Q}$ stands for a positive absolute constant. Any sentence containing this symbol becomes true if the symbol is replaced in every occurrence by some large enough real number.

We specialize the values of the parameters r and d in Proposition 2. We will take $d = r$. It is evident that $\binom{2r}{r} \geqslant 2^r$ so

$$\frac{1}{r+1}\binom{2r}{r} \geqslant 2^{\frac{r}{2}}$$

for r large enough. Further

$$\frac{1}{r+2}\binom{2r+2}{r+1} \leqslant \frac{1}{r+1}\binom{2r}{r} \times 4.$$

We choose r to be the smallest positive integer such that $n(r+1) \leqslant \binom{2r}{r}$. We have

$$n(r+1) \leqslant \binom{2r}{r} \leqslant 4n(r+1) \text{ and } r \leqslant 3\log n \tag{1}$$

for n large enough. We deduce that $\ell = \binom{2r}{r} - n \leqslant 4n(r+1) \leqslant \mathcal{Q}n\log n$. So

$$\ell^{\ell/2n} \leqslant n^{\mathcal{Q}\log n}.$$

From Equation (1) we deduce that $\binom{2r}{r} \leqslant \mathcal{Q}n\log n$. Also $n^2 d(r+1) \leqslant \mathcal{Q}n^2\log^2 n$ and

$$\left(n^2 d(r+1)\right)^r \leqslant n^{\mathcal{Q}\log n}.$$

So the coefficients of equations E_i are bounded in absolute value by

$$n^{\mathcal{Q}\log n}\delta_{\mathbf{K}}^{\mathcal{Q}\log n}.$$

This proves Theorem 1. Theorem 2 follows because there are $r\binom{2r}{r}$ coefficients to be fixed. We note also that there may appear several number fields in the smooth zero dimensional part of the complete intersection $E_1 = E_2 = \cdots = E_r = 0$. However the Chow class of this intersection is $r^r \leqslant (\log n)^{\mathcal{Q}\log n}$ and the number of isolated points is bounded by this intersection number [13, Chapter 13].

References

[1] J. Alexander. Singularités imposables en position générale à une hypersurface projective. *Compositio Math.*, 68(3):305–354, 1988.

[2] J. Alexander and A. Hirschowitz. Polynomial interpolation in several variables. *J. Algebraic Geom.*, 4(2):201–222, 1995.

[3] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao. Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves. *ArXiv e-prints*, January 2017.

[4] Manjul Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math. (2)*, 162(2):1031–1063, 2005.

[5] Manjul Bhargava. The density of discriminants of quintic rings and fields. *Ann. of Math. (2)*, 172(3):1559–1591, 2010.
[6] Maria Chiara Brambilla and Giorgio Ottaviani. On the Alexander-Hirschowitz theorem. *J. Pure Appl. Algebra*, 212(5):1229–1251, 2008.
[7] Karen A. Chandler. A brief proof of a maximal rank theorem for generic double points in projective space. *Trans. Amer. Math. Soc.*, 353(5):1907–1920, 2001.
[8] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.
[9] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.
[10] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. Counting discriminants of number fields. *J. Théor. Nombres Bordeaux*, 18(3):573–593, 2006.
[11] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551):405–420, 1971.
[12] Jordan S. Ellenberg and Akshay Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math. (2)*, 163(2):723–741, 2006.
[13] William Fulton. *Intersection theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge.* Springer-Verlag, Berlin, second edition, 1998.
[14] Gunter Malle. On the distribution of Galois groups. II. *Experiment. Math.*, 13(2):129–135, 2004.
[15] Jacques Martinet. *Perfect lattices in Euclidean spaces*, volume 327 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 2003.
[16] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1999.
[17] Robert J. Lemke Oliver and Frank Thorne. Upper bounds on number fields of given degree and bounded discriminant. 2020.
[18] Wolfgang M. Schmidt. Number fields of given degree and bounded discriminant. *Astérisque*, (228):4, 189–195, 1995. Columbia University Number Theory Seminar (New York, 1992).
[19] Carl Ludwig Siegel. *Lectures on the geometry of numbers*. Springer-Verlag, Berlin, 1989.

JEAN-MARC COUVEIGNES, UNIV. BORDEAUX, CNRS, BORDEAUX-INP, IMB, UMR 5251, F-33400 TALENCE, FRANCE.

JEAN-MARC COUVEIGNES, INRIA, F-33400 TALENCE, FRANCE.
Email address: Jean-Marc.Couveignes@u-bordeaux.fr