Appendix

by J. Ellenberg and A. Venkatesh

A.1. Let $N(X)$ denote the number of isomorphism classes of number fields with discriminant less than X.

Theorem. *For every $\epsilon > 0$ there is a constant $C(\epsilon)$ such that $\log N(X) \leq C(\epsilon)(\log X)^{1+\epsilon}$, for every $X \geq 2$.*

In fact we prove the more precise upper bound that

$$\log N(X) \leq C_6 \log X \exp(C_7 \sqrt{\log \log X})$$

for absolute constants C_6, C_7.

This theorem (almost) follows from [EV, Theorem 1.1], the only point being to control the dependence of implicit constants on the degree of the number field.

We refer to [EV] for further information and for some motivational comments about the method. In the proof $C_1, C_2, \ldots$ will denote certain *absolute* constants.

A.2. Let K be an extension of $\mathbb{Q}$ of degree $d \geq 200$. Denote by $\Sigma(K)$ the set of embeddings of K into $\mathbb{C}$ ($\#\Sigma(K) = d$), and by $\overline{\Sigma}(K)$ a set of representatives for $\Sigma(K)$ modulo complex conjugation (in the notations of the paper [EV] $\overline{\Sigma}(K) = V_\infty(K)$). We regard the ring of integers $\mathcal{O}_K$ as a lattice in $K \otimes_{\mathbb{Q}} \mathbb{R} = \prod_{\sigma \in \Sigma(K)} K_\sigma$. We endow the real vector space $K \otimes_{\mathbb{Q}} \mathbb{R}$ with the supremum norm, i.e. $\|(x_\sigma)\| = \sup_\sigma |x_\sigma|$. Here $|\cdot|$ denotes the standard absolute value on $\mathbb{C}$. In particular, we obtain a "norm" on $\mathcal{O}_K$ by restriction. Explicitly, for $z \in \mathcal{O}_K$, we have $\|z\| = \sup_{\sigma \in \Sigma(K)} |\sigma(z)|$.

We denote by $M_d(\mathbb{Z})$ (resp. $M_d(\mathbb{Q})$) the algebra of d by d matrices over $\mathbb{Z}$ (resp. $\mathbb{Q}$).

By the "trace form" we mean the pairing $(x, y) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(xy)$. It is a symmetric nondegenerate $\mathbb{Q}$-bilinear pairing on K^2.

Let s be a positive integer which we shall specify later. We denote by $\mathbf{y} = (y_1, y_2, \ldots, y_s)$ an ordered s-tuple of elements of $\mathcal{O}_K$ and write $\|\mathbf{y}\| := \max(\|y_1\|, \ldots, \|y_s\|)$. For $\mathbf{y} = (y_1, \ldots, y_s) \in \mathcal{O}_K^s$ and $l \geq 1$, we shall set

$$\begin{aligned} S(l) &= \{(k_1, \ldots, k_s) \in \mathbb{Z}^s : k_1 + \ldots + k_s \leq l, k_1, \ldots, k_s \geq 0\}, \\ S(\mathbf{y}, l) &= \{y_1^{k_1} y_2^{k_2} \ldots y_s^{k_s} : (k_1, \ldots, k_s) \in S(l)\} \subset \mathcal{O}_K. \end{aligned} \tag{5}$$

If S is a subset of $S(l)$ we denote by $S(\mathbf{y})$ the set $\{y_1^{k_1} y_2^{k_2} \ldots y_s^{k_s} : (k_1, \ldots, k_s) \in S.\}$

A.3. Lemma. *Let S be a subset of $S(l)$ such that $S(\mathbf{y})$ spans a $\mathbb{Q}$-linear subspace of K with dimension strictly greater than $d/2$. Let $S + S$ be the set of sums of two elements of S. Then $(S + S)(\mathbf{y})$ spans K over $\mathbb{Q}$.*

Proof. (cf. [EV, Lemma 2.1].) Suppose that there existed $z \in K$ which was perpendicular, w.r.t. the trace form, to the $\mathbb{Q}$-span of $(S + S)(\mathbf{y})$. Since $(S + S)(\mathbf{y})$ consists precisely of all products $\alpha\beta$, with $\alpha, \beta \in S(\mathbf{y})$, it follows that

$$\mathrm{Tr}_{K/\mathbb{Q}}(z\alpha\beta) = 0, \quad (\alpha, \beta \in S(\mathbf{y})). \tag{6}$$

Call $W \subset K$ the $\mathbb{Q}$-linear span of $S(\mathbf{y})$. Then (6) implies that zW is perpendicular to W w.r.t. the trace form, contradicting $\dim(W) > d/2$. □

A.4. Lemma. *Let $\mathcal{C} \subset \mathcal{O}_K$ be a finite subset containing 1 and generating K as a field over $\mathbb{Q}$. Let $z_1, z_2, \dots, z_d$ be a $\mathbb{Q}$-linear basis for K. For each $u \in \mathcal{C}$, let $M(u) = \big(\mathrm{Tr}_{K/\mathbb{Q}}(uz_iz_j)\big)_{1\le i,j\le d} \in M_d(\mathbb{Q})$. Then the $\mathbb{Q}$-subalgebra of $M_d(\mathbb{Q})$ generated by $M(u)M(1)^{-1}$, as u ranges over $\mathcal{C}$, is isomorphic to K.*

Proof. (cf. [EV, Lemma 2.2].) In fact, $M(u)M(1)^{-1}$ gives the matrix of "multiplication by u," in the basis $\{z_i\}$. □

A.5. We denote by $\mathcal{D}_K$ the absolute value of the discriminant of K.

Lemma. *There is an absolute constant $C_1 \in \mathbb{R}$ such that, for any K as above, there exists a basis $\gamma_1, \gamma_2, \dots, \gamma_d$ for $\mathcal{O}_K$ over $\mathbb{Z}$ such that*

$$\|\gamma_j\| \le \|\gamma_{j+1}\|, \quad \prod_{i=1}^{d} \|\gamma_d\| \le \mathcal{D}_K^{1/2} C_1^d, \quad \|\gamma_i\| \le (C_1^d \mathcal{D}_K^{1/2})^{\frac{1}{d-i}} \ (i < d). \tag{7}$$

Proof. This is reduction theory (cf. [EV, Prop. 2.5]). The final statement of (7) follows from the preceding statements, in view of the fact that $\|\gamma_j\| \ge 1$ for each j. □

A.6. Let r, l be integers such that $d/2 < r \le |S(l)| = \binom{l+s}{s}$.

Lemma. *Suppose $W \subset K$ is a $\mathbb{Q}$-linear subspace of dimension r, and let $S \subset S(l)$ be a subset of size r. Then there exists $\mathbf{y} = (y_1, y_2, \dots y_s) \in W^s$ such that the elements of $S(\mathbf{y})$ are $\mathbb{Q}$-linearly independent.*

Proof. This is precisely [EV, Lemma 2.3]. □

A.7. Lemma. *Let $\Lambda = \mathbb{Z}\gamma_1 + \mathbb{Z}\gamma_2 + \cdots + \mathbb{Z}\gamma_r$ and let $S \subset S(l)$ be a subset of size r. Then there is $\mathbf{y} = (y_1, y_2, \dots, y_s) \in \Lambda^s$ such that the elements of $S(\mathbf{y})$ are linearly independent over $\mathbb{Q}$, and $\|\mathbf{y}\| \le r^2 l (C_1^d \mathcal{D}_K^{1/2})^{\frac{1}{d-r}}$.*

Proof. Considering Λ^s as a $\mathbb{Z}$-module of rank rs, the proof of [EV, Lemma 2.3] shows that there is a polynomial F of degree at most rl in the rs variables so that the elements of $S(\mathbf{y})$ are linearly independent over $\mathbb{Q}$ whenever $F(\mathbf{y}) \neq 0$. Lemma 2.4 of [EV] then shows that we can choose such a $\mathbf{y}$ whose coefficients are at most $(1/2)(rl+1) \le rl$. It follows that

$$\|y_i\| \le r^2 l (C_1^d \mathcal{D}_K^{1/2})^{\frac{1}{d-r}}$$

for $i = 1, 2, \dots s$. □

A.8. Lemma. *The number of number fields with degree $d \geq 200$ and discriminant of absolute value at most X is at most*

$$(C_3 d)^{d \exp(C_4 \sqrt{\log d})} X^{\exp(C_5 \sqrt{\log d})}.$$

Proof. Fix once and for all a total ordering of $S(2l)$. We denote the order relation as $(k_1, \ldots, k_s) \prec (k_1', \ldots, k_s')$. Choose $S \subset S(l)$ of cardinality r as above.

Let K have degree d over $\mathbb{Q}$ and satisfy $\mathcal{D}_K < X$. Chose $\mathbf{y}$ as in Lemma A.7. By Lemma A.3, $S(2l)(\mathbf{y})$ spans K over $\mathbb{Q}$. It follows that there exists a subset $\Pi \subset S(2l)$ of size d such that $\{z_1, \ldots, z_d\} := \{y_1^{k_1} y_2^{k_2} \ldots y_s^{k_s} : (k_1, k_2, \ldots, k_s) \in \Pi\}$ forms a $\mathbb{Q}$-basis for K, and such that the ordering $z_1, \ldots, z_d$ conforms with the specified ordering on $\Pi \subset S(2l)$.

We apply Lemma A.4 to $\{z_1, \ldots, z_d\}$ and $\mathcal{C} = (1, y_1, y_2, \ldots, y_s)$. Then each product uz_iz_j ($u \in \mathcal{C}, 1 \leq i, j \leq d$) is contained in $S(4l+1)$.

Put $\mathbf{A} = (\mathrm{Tr}_{K/\mathbb{Q}}(y_1^{k_1} y_2^{k_2} \ldots y_s^{k_s}))_{(k_1, k_2, \ldots k_s) \in S(4l+1)}$. For each K, the collection of matrices $M(u)$ is determined by $\mathbf{A}$ and Π. Since $|\mathrm{Tr}_{K/\mathbb{Q}}(z)| \leq d\|\mathbf{y}\|^{4l+1}$ for any $z \in S(\mathbf{y}, 4l+1)$, the number of possibilities for $\mathbf{A}$ is at most $(d\|\mathbf{y}\|^{4l+1})^{|S(4l+1)|}$; since Π is a subset of $|S(2l)|$, the number of possibilities for Π is at most $2^{|S(2l)|}$.

Lemma A.4 now yields that the number of possibilities for the isomorphism class of K is at most $2^{|S(2l)|}(d\|\mathbf{y}\|^{4l+1})^{|S(4l+1)|}$. By our bound on $\|\mathbf{y}\|$ we now have that the number of possibilities for K is at most

$$2^{|S(2l)|}(d(r^2 l(C_1^d \mathcal{D}_K^{1/2})^{\frac{1}{d-r}})^{4l+1})^{|S(4l+1)|}. \tag{8}$$

Note that $|S(4l+1)| = \binom{s+4l+1}{s}$.

Now, just as in the paragraph following (2.6) of [EV], we choose s to be the greatest integer less than $\sqrt{\log d}$ and l to be the least integer greater than $(ds!)^{1/s}$. Note that $l < \exp(C_2\sqrt{\log d})$. Now $|S(l)| = \binom{s+l}{s}$ is at least d, so we may choose r between $d/2$ and $3d/4$. In particular, $r^2 l < d^3$. Also, $\binom{s+4l+1}{s}$ is at most $10^s d$ and $|S(2l)| = \binom{s+2l}{s} \leq 6^s d$. Finally, $s < 2\sqrt{\log d}$.

Substituting these values into (8) we get that the number of possible K is at most

$$2^{6^s d}(d(d^3(C_1^d X^{1/2})^{4/d})^{5\exp(C_2\sqrt{\log d})})^{10^s d}$$

which is in turn at most

$$(C_3 d)^{d \exp(C_4 \sqrt{\log d})} X^{\exp(C_5 \sqrt{\log d})}.$$

□

A.9. Proposition. *There are absolute constants C_6, C_7 with*

$$\log N(X) \leq C_6 \log X \exp(C_7 \sqrt{\log \log X}).$$

Proof. By Minkowski's discriminant bound, there is an absolute constant $C_6 > 1$ such that $\mathcal{D}_K > C_6^{[K:\mathbb{Q}]}$ for any extension $K/\mathbb{Q}$; so we may take d to be bounded by a constant multiple of $\log X$. From Lemma A.8 it now follows that the logarithm of the number of extensions $K/\mathbb{Q}$ with $\mathcal{D}_K < X$ and $[K : \mathbb{Q}] \geq 200$ is bounded by

$C_6 \log X \exp(C_7\sqrt{\log\log X})$. Trivial bounds suffice to show that the number of K with $\mathcal{D}_K < X$ and $[K:\mathbb{Q}] < 200$ is $\leq C_8 X^{200}$. □

References

[BL] M. Belolipetsky, A. Lubotzky, Counting manifolds and class field towers, preprint.

[B] A. Borel, Commensurability classes and volumes of hyperbolic 3-manifolds, *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4),* **8** (1981), 1–33.

[BH] A. Borel, G. Harder, Existence of discrete cocompact subgroups of reductive groups over local fields, *J. Reine Angew. Math.,* **298** (1978), 53–64.

[BP] A. Borel, G. Prasad, Finiteness theorems for discrete subgroups of bounded covolume in semi-simple groups, *Inst. Hautes Études Sci. Publ. Math.,* **69** (1989), 119–171; Addendum: *ibid.,* **71** (1990), 173–177.

[BGLM] M. Burger, T. Gelander, A. Lubotzky, S. Mozes, Counting hyperbolic manifolds, *Geom. Funct. Anal.,* **12** (2002), 1161–1173.

[Coh] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Math., **193**, Springer-Verlag (2000).

[Cor] G. Cornell, Relative genus theory and the class group of l-extensions. *Trans. Amer. Math. Soc.,* **277** (1983), 421–429.

[CR] V. I. Chernousov, A. A. Ryzhkov, On the classification of maximal arithmetic subgroups of simply connected groups, *Sb. Math.,* **188** (1997), 1385–1413.

[EV] J. Ellenberg, A. Venkatesh, The number of extensions of a number field with fixed degree and bounded discriminant, *Ann. of Math. (2),* **163** (2006), 723–741.

[GLP] D. Goldfeld, A. Lubotzky, L. Pyber, Counting congruence subgroups, *Acta Math.,* **193** (2004), 73–104.

[Gr] B. H. Gross, On the motive of a reductive group, *Invent. Math.,* **130** (1997), 287–313.

[K] M. Kneser, Galois-Kohomologie halbeinfacher algebraischer Gruppen uber p-adischen Korpern, I, *Math. Z.,* **88** (1965), 40–47; II, *ibid.,* **89** (1965), 250–272.

[L] A. Lubotzky, Subgroup growth and congruence subgroups, *Invent Math.,* **119** (1995), 267–295.

[LN] A. Lubotzky, N. Nikolov, Subgroup growth of lattices in semisimple Lie groups, *Acta Math.,* **193** (2004), 105–139.

[LS] A. Lubotzky, D. Segal, *Subgroup growth*, Progress in Math., **212**, Birkhäuser Verlag (2003).

[M] G. A. Margulis, *Discrete subgroups of semi-simple Lie groups*, Ergeb. der Math., **17**, Springer-Verlag (1989).

[Od] A. M. Odlyzko, Lower bounds for discriminants of number fields, *Acta Arith.,* **29** (1976), 275–297.

[Ono] T. Ono, On Tamagawa numbers. *Proc. Symp. Pure Math.,* **9** (1966), 122–132.

[PlR] V. P. Platonov, A. S. Rapinchuk, *Algebraic groups and number theory*, Academic Press (1994).

[P] G. Prasad, Volumes of S-arithmetic quotients of semi-simple groups, *Inst. Hautes Études Sci. Publ. Math.,* **69** (1989), 91–117.

[R] J. Rohlfs, Die maximalen arithmetisch definierten Untergruppen zerfallender einfacher Gruppen, *Math. Ann.,* **244** (1979), 219–231.

[S] J.-P. Serre, Quelques applications du theoreme de densite de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.,* **54** (1981), 323–401.

[T] J. Tits, Reductive groups over local fields, *Proc. Symp. Pure Math.,* **33** (1979), Part I, 29–69.

[W] H. C. Wang, Topics on totally discontinuous groups, in *Symmetric spaces*, (ed. by W. M. Boothby and G. Weiss), Marcel Dekker (1972), 459–487.

M. Belolipetsky

Department of Mathematical Sciences, Durham University, Durham DH1 3LE, U.K.

Institute of Mathematics, Koptyuga 4, 630090 Novosibirsk, Russia

E-mail address: mbel@math.nsc.ru

J. Ellenberg
Department of Mathematics, Princeton University, Princeton, NJ 08544, U.S.A.
E-mail address: ellenber@math.princeton.edu

A. Venkatesh
Department of Mathematics, Massachusetts Institute of Technology,
Cambridge, MA 02139-4307, U.S.A.
E-mail address: akshayv@math.mit.edu