ON NUMBER FIELDS WITH NONTRIVIAL SUBFIELDS

MARTIN WIDMER

Abstract. What is the probability for a number field of composite degree en to have a nontrivial subfield? As the reader might expect the answer heavily depends on the interpretation of probability. We show that if the fields are enumerated by the smallest height of their generators the probability is zero, at least if $en > 6$. This is in contrast to what one expects when the fields are enumerated by the discriminant. The main result of this article is an estimate for the number of algebraic numbers of degree en and bounded height which generate a field that contains an unspecified subfield of degree e. If $n > \max\{e^2+e, 10\}$ we get the correct asymptotics as the height tends to infinity.

1. Introduction and results

The most natural way to enumerate number fields of fixed degree is probably by their discriminant Δ or the modulus thereof. For positive integers e and n let $\Delta(en, X)$ be the number of field extensions F of $\mathbb{Q}$ of degree en in an algebraic closure $\overline{\mathbb{Q}}$ with $|\Delta_F| \leq X$. The asymptotics are predicted by a classical conjecture (possibly due to Linnik) but proved only for degree $en = 2, 3, 4, 5$.

Conjecture 1.1. *Suppose $en > 1$. Then there exists a positive constant c_{en} such that as X tends to infinity*

$$\Delta(en, X) = c_{en}X + o(X).$$

Linnik's Conjecture is usually stated in a more general form which asserts that for any number field K the number of field extensions F of K of relative degree n satisfying $|\Delta_F| \leq X$ is given by $c_{K,n}X + o(X)$ for a positive constant $c_{K,n}$.

Let G be a subgroup of the symmetric group S_{en} containing a subgroup of index en. Malle [2] has given conjectural asymptotics for $\Delta_G(en, X)$, the number of fields in $\overline{\mathbb{Q}}$ of degree en whose Galois closure has Galois group isomorphic to G and whose modulus of the discriminant is not larger than X. Klüners [8] found counterexamples to Malle's conjecture but a slight adjustement of the conjecture proposed by Türkelli [14] seems promising.

Date: September 29, 2009.

2000 *Mathematics Subject Classification.* Primary 11R04; Secondary 11G50, 11G35.

Key words and phrases. Number fields, Height, Northcott's Theorem, counting.

But once again this is proved only in very special cases. Bhargava's work [2] implies $\Delta_{S_4}(4,X) \sim \lambda X$ for

$$\lambda = \frac{5}{6}\prod_p \left(1+\frac{1}{p^2}-\frac{1}{p^3}-\frac{1}{p^4}\right) = 1.01389....$$

And according to Cohen, Diaz y Diaz and Olivier [6] the number with Dihedral group $\Delta_{D_4}(4,X)$ is $\sim \mu X$ where $\mu = 0.1046520224....$ A quartic field has a quadratic subfield if and only if its Galois closure is D_4 or an abelian group of order four. Bailey [1] and Wong [18] have shown that $\Delta_G(4,X) = o(X)$ for $G = A_4$ and abelian groups G of order four. Thus when we enumerate the quartic fields by the modulus of their discriminant the probability that a quartic field has a quadratic subfield is the positive number

$$\frac{\mu}{\mu+\lambda} = 0.09356....$$

Suppose the (generalized) Linnik Conjecture is true. We fix a number field K of degree e and then we count extensions F of K of relative degree n satisfying $|\Delta_F| \leq X$. In this way we conclude that the lower density for the set of fields of degree en that contain a subfield of degree e is positive; of course here density is understood with respect to the modulus of the discriminant. Hence when enumerated by the modulus of the discriminant the ("lower") probability that a field of degree en has a subfield of degree e remains positive, subject to the (generalized) Linnik Conjecture.

This is in stark contrast to the situation when one enumerates by the following, also classical, invariant

$$\pi(F) = \inf_{\substack{\alpha \\ \mathbb{Q}(\alpha)=F}} |D_\alpha|.$$

Here D_α is the unique minimal polynomial of α in $\mathbb{Z}[x]$ with positive leading coefficient and coprime coefficients and $|D_\alpha|$ denotes the maximum norm of the coefficient vector. The quantity $|D_\alpha|$ is sometimes referred to as the naive height of α. We define the counting function $\pi(e,n,X)$ as the number of fields $F \subseteq \overline{\mathbb{Q}}$ of degree en that contain a subfield of degree e and satisfy $\pi(F) \leq X$.

In this note we shed some light on the distribution of number fields by counting generators. Let H be the absolute multiplicative Weil height (or briefly the height) on $\overline{\mathbb{Q}}$, as defined in [3] p.16. A result of Masser and Vaaler (Theorem in [10]) gives the asymptotics for the number of generators of degree en with bounded height. We extend Masser and Vaaler's result by estimating $Z(e,n,X)$ which counts the numbers with height at most X

generating a field of degree en that contains a subfield of degree e

$$Z(e,n,X) = |\{\alpha \in \overline{\mathbb{Q}}; [\mathbb{Q}(\alpha):\mathbb{Q}] = en, \mathbb{Q}(\alpha) \text{ contains a field of degree } e,\ H(\alpha) \leq X\}|.$$

Our first result is a simple by-product of the proof of our main result Theorem 1.2 combined with a result of Schmidt, and gives an upper bound for $Z(e,n,X)$.

Theorem 1.1. *With $c = n \cdot 2^{e(n^2+ne+2e+n+13)+n^2+10n}$ and $X > 0$ we have*

$$Z(e,n,X) \leq cX^{en(n+e)}.$$

The invariant $\delta(F) = \inf\{H(\alpha); F = \mathbb{Q}(\alpha)\}$ plays a crucial role in the proofs. If α is an algebraic number of degree en then $H(\alpha)^{en} = M(D_\alpha)$ where M denotes the Mahler measure (see [3] p.22 or [11] p.434 for a definition). A crude estimate comparing $M(D_\alpha)$ and $|D_\alpha|$ gives

$$(2^{-1}H(\alpha))^{en} \leq |D_\alpha| \leq (2H(\alpha))^{en} \tag{1.1}$$

and hence

$$(2^{-1}\delta(F))^{en} \leq \pi(F) \leq (2\delta(F))^{en}.$$

We therefore conclude from Theorem 1.1

$$\pi(e,n,X) \leq c \cdot 2^{en(n+e)} X^{n+e}.$$

On the other hand Corollary 5.1 in [16] yields

$$\pi(1,en,X) \geq C_{en} X^{en-1}$$

for a positive constant C_{en} and $X \geq X_0(en)$. Combining these two estimates we find: when ordered by the invariant π the probability that a field F of degree en has a subfield different from $\mathbb{Q}$ and F is zero, at least for $en > 6$.

Another consequence of Theorem 1.1 concerns polynomials with certain Galois groups. Let f in $\mathbb{Z}[x]$ be irreducible of degree en. Since Van der Waerden [15] it is known that almost all polynomials f have the full symmetric group S_{en} as Galois group when enumerated by the maximum norm of the coefficient vector. That is any root α of f generates a field $L = \mathbb{Q}(\alpha)$ whose Galois closure F_G has Galois group S_{en} over $\mathbb{Q}$. The group corresponding to F is some S_{en-1}. It is easy to see that there is no group lying strictly between these two groups. This means that $F/\mathbb{Q}$ has no proper intermediate field in this case. Van der Waerden's result can be further quantified through sharpenings of the Hilbert Irreducibility Theorem. A general version due to S.D. Cohen ([5] Theorem 2.1) gives an upper bound of order $X^{en+1/2}\log X$ for the number of exceptional polynomials. Gallagher and Dietmann [7] improved the exponent $en + 1/2$ for $en = 4, 5$. It is likely that the exponent $en+1/2$ can always be improved but this might be hard to achieve in general. However, under the stronger condition that there exists a proper intermediate field Theorem 1.1 in combination with (1.1) tells us that the exponent $en+1/2$ can be reduced to $en/2+2$.

So much for the consequences of the proof of our main result. We now come to the main result itself. As already mentioned it asymptotically estimates the counting function $Z(e,n,X)$ as the height bound X tends to infinity. To state the result we have to introduce further notation. In [11] Masser and Vaaler defined the following two quantities

$$V_{\mathbb{R}}(n) = (n+1)^l \prod_{i=1}^{l} \frac{(2i)^{n-2i}}{(2i+1)^{n+1-2i}}$$

where $l=[(n-1)/2]$ and the empty product is interpreted as 1 and

$$V_{\mathbb{C}}(n) = \frac{(n+1)^{n+1}}{((n+1)!)^2}.$$

These formulae give the volumes of the unit balls in $\mathbb{R}^{n+1}$ and $\mathbb{C}^{n+1}$ with respect to the Mahler measure distance function and have been calculated by Chern and Vaaler in [4]. We also need the Schanuel constant $S_K(n)$ for a number field K, defined as follows

$$S_K(n) = \frac{h_K R_K}{w_K \zeta_K(n+1)} \left(\frac{2^{r_K}(2\pi)^{s_K}}{\sqrt{|\Delta_K|}} \right)^{n+1} (n+1)^{r_K+s_K-1}. \tag{1.2}$$

Here h_K is the class number, R_K the regulator, w_K the number of roots of unity in K, ζ_K the Dedekind zeta-function of K, Δ_K the discriminant, r_K is the number of real embeddings of K and s_K is the number of pairs of distinct complex conjugate embeddings of K.

All fields are considered to lie in a fixed algebraic closure $\overline{\mathbb{Q}}$. It will be convenient to use Landau's O-notation. For non-negative real functions $f(X), g(X), h(X)$ we say that $f(X) = g(X) + O(h(X))$ as $X > X_0$ tends to infinity if there is a constant C_0 such that $|f(X) - g(X)| \leq C_0 h(X)$ for each $X > X_0$. Now we can state the main result.

Theorem 1.2. *Suppose $n > \max\{e^2+e, 10\}$. Then as $X > 0$ tends to infinity we have*

(1.3)

$$Z(e,n,X) = \left(\sum_K n V_{\mathbb{R}}(n)^{r_K} V_{\mathbb{C}}(n)^{s_K} S_K(n) \right) X^{en(n+1)} + O(X^{en(n+1)-n}),$$

where the sum runs over all number fields of degree e and the implied constant in the O-term depends only on e and n.

The above theorem states implicitly, subject to the constraints on e and n, that the sum on the right hand-side of (1.3) converges. Notice that by Masser and Vaaler's Theorem [10] (or its generalization from $\mathbb{Q}$ to arbitrary ground fields in [11])

$$Z(1, en, X) = Z(en, 1, X) = enV_{\mathbb{R}}(en)S_{\mathbb{Q}}(en)X^{en(en+1)} + O(X^{(en)^2}\mathfrak{L}).$$

So for instance the asymptotics for the numbers of degree 22 involve X^{506} whereas those for the numbers that generate a field which contains a quadratic subfield involve only X^{264}.

If each divisor > 1 of n is larger than e we can relax the constraints on e and n.

Theorem 1.3. *Suppose $l > 1$ and $l|n$ implies $l > e$ and suppose $n > \max\{6e-6, 10\}$. Then as $X > 0$ tends to infinity we have*

$$Z(e, n, X) = \left(\sum_{K} nV_{\mathbb{R}}(n)^{r_K}V_{\mathbb{C}}(n)^{s_K}S_K(n)\right)X^{en(n+1)} + O(X^{en(n+1)-n})$$

where the sum runs over all number fields of degree e. The implied constant in the O-term depends only on e and n.

Our proof strategy for Theorem 1.2 can be roughly (and oversimplified) described as follows. First fix a field K of degree e and count those numbers having degree n over K and degree en over $\mathbb{Q}$. Combining ideas of Masser and Vaaler from [11] and of the author's works [17] and [16] this can be achieved by counting monic polynomials $x^n + \alpha_1 x^{n-1} + ... + \alpha_n$ in $K[x]$ with $K = \mathbb{Q}(\alpha_1, ..., \alpha_n)$ and with bounded Mahler measure. For the error term one has to take into account the reducible polynomials and also the polynomials irreducible over K but reducible over the Galois closure of K. Then we sum these estimates over all fields K of degree e. This requires that the emerging error terms converge when summed over all fields K. The error terms are expressed using the invariant $\delta(K)$, because they have better summatory properties than the discriminant.

We can use the same ideas to prove asymptotic results for

$$\begin{aligned} Z(e, m, n, X) = |\{\alpha \in \overline{\mathbb{Q}}; [\mathbb{Q}(\alpha) : \mathbb{Q}] = emn, H(\alpha) \leq X,& \\ \mathbb{Q}(\alpha) \text{ contains a field of degree } e \text{ and a field of degree } em\}|.& \end{aligned}$$

We state just one particularly simple result.

Theorem 1.4. *Suppose $l > 1$ and $l|n$ implies $l > em$ and suppose $n > \max\{6em-6, 10\}$. Then as $X > 0$ tends to infinity we have*

$$Z(e,m,n,X) = \left(\sum_{K} nV_{\mathbb{R}}(n)^{r_K} V_{\mathbb{C}}(n)^{s_K} S_K(n)\right) X^{emn(n+1)} + O(X^{emn(n+1)-n})$$

where the sum runs over all number fields of degree em that contain a subfield of degree e.

Notice that under the above conditions on e, m and n the functions $Z(1, em, n, X)$ and $Z(e, m, n, X)$ both have order of magnitude $X^{emn(n+1)}$ whereas $Z(1, 1, emn, X)$ has order of magnitude $X^{emn(emn+1)}$.

Let us mention one final side product of the proof of Theorem 1.2. We obtain a version of Theorem in [11] with particular good error term regarding the ground field K under the necessary condition that we exclude those numbers that have also degree n over a proper subfield k of K.

Theorem 1.5. *Let K be a number field of degree e. Then as $X > 0$ tends to infinity the number of elements β in $\overline{\mathbb{Q}}$ with*

$$\begin{aligned}
&[K(\beta) : K] = n,\\
&k \subseteq K \text{ and } [k(\beta) : k] = n \Longrightarrow k = K, \qquad (1.4)\\
&H(\beta) \leq X
\end{aligned}$$

is

$$nV_{\mathbb{R}}(n)^{r_K} V_{\mathbb{C}}(n)^{s_K} S_K(n) X^{en(n+1)} + O(\delta(K)^{-\frac{e}{2}(n-\max\{4e-8,2e-3\})+1.1} X^{en(n+1)-n}\mathfrak{L})$$

where $\mathfrak{L} = 1$ unless $en = 1$ or $en = 2$ in which case $\mathfrak{L} = \log(X+2)$. The constant in O depends only on e and n.

If e and $n > \max\{4e-8, 2\}$ are fixed then the constant in the error term goes rapidly to zero as the fields K become more complicated. The additive constant 1.1 in the exponent on $\delta(K)$ has no particular significance and could be replaced by any other value > 1.
For $e = 1$ or $n = 1$ Theorem 1.1 is covered by Schmidt's Theorem in [12]. The cases $e = 1$ in Theorem 1.2, Theorem 1.3 and Theorem 1.5 are all covered by Masser and Vaaler's Theorem in [10] and the case $n = 1$ in Theorem 1.5 counts generators $\alpha \in K$ with bounded height and thus is covered by a special case of Corollary 3.2 in [17] (which we cite as Theorem 4.1 in Section 4). Finally the cases $e = 1$ or $m = 1$ in Theorem 1.4 are covered by Theorem 1.3. We emphasize that our work neither gives a proof of Schmidt's nor a new proof of Masser and Vaaler's result but rather uses their method and ideas in combination with the work done in [17] and [16]

to extend these results.
Throughout this article X and T denote positive real numbers.

Acknowledgements

Although the presented work is not included in my Ph.D. thesis the major part has been carried out during my graduate studies. I am indebted to my Ph.D. adviser David Masser for his generosity in sharing his thoughts and ideas, in particular for pointing out to me that the results from [16] might yield results in the style of Theorem 1.2. I also would like to thank Wolfgang Schmidt for interesting and fruitful discussions. This work was financially supported by the Swiss National Science Foundation.

2. Reformulation of Theorem 1.2 step one

Let K be a number field of degree e. We define

$$Z_K(e,n,X) = |\{\beta \in \overline{\mathbb{Q}}; [\mathbb{Q}(\beta):\mathbb{Q}] = en, [K(\beta):K] = n, H(\beta) \leq X\}|.$$

If $\beta \in \overline{\mathbb{Q}}$ with $[\mathbb{Q}(\beta):\mathbb{Q}] = en$ and $\mathbb{Q}(\beta)$ contains the field K of degree e then $[K(\beta):K] = n$. Therefore

$$Z(e,n,X) \leq \sum_K Z_K(e,n,X), \tag{2.1}$$

where K runs over all fields of degree e. On the other hand if β is in $\overline{\mathbb{Q}}$ with $[K(\beta):K] = n$ and $[\mathbb{Q}(\beta):\mathbb{Q}] = en$ then $\mathbb{Q}(\beta)$ contains the field K of degree e. However, some elements β may be counted for several different fields K on the right hand-side of (2.1). To keep track of these multiply counted numbers we have to introduce two further quantities.

$$\begin{aligned}
&\overline{Z}(e,n,X) = \\
&\qquad |\{\beta \in \overline{\mathbb{Q}}; [\mathbb{Q}(\beta):\mathbb{Q}] = en, \\
&\qquad \mathbb{Q}(\beta) \text{ contains more than one field of degree } e, H(\beta) \leq X\}|, \\
&\overline{Z}_K(m,n,X) = \\
&\qquad |\{\beta \in \overline{\mathbb{Q}}; [\mathbb{Q}(\beta):\mathbb{Q}] = en, [K(\beta):K] = n, \\
&\qquad \mathbb{Q}(\beta) \text{ contains more than one field of degree } e, H(\beta) \leq X\}|.
\end{aligned}$$

For all e, n we have

$$Z(e,n,X) = \sum_K \left(Z_K(e,n,X) - \overline{Z}_K(e,n,X)\right) + \overline{Z}(e,n,X). \tag{2.2}$$

where K runs over all fields of degree e. Moreover

$$\overline{Z}(e,n,X) \leq \sum_K \overline{Z}_K(e,n,X) \leq 2^{en}\overline{Z}(e,n,X). \tag{2.3}$$

The first inequality is obvious the second one holds because every field of degree en contains at most 2^{en} subfields.

Now suppose $\mathbb{Q}(\beta)$ contains more than one subfield of degree e. So the composite field of two different subfields of degree e lies in $\mathbb{Q}(\beta)$. But this composite field has degree le where $l \mid n$ and $l \in \{2, 3, ..., e\}$. Hence by (2.1)

$$\overline{Z}(e,n,X) \leq \sum_{\substack{l|n \\ 1<l\leq e}} Z(le, n/l, X) \leq \sum_{\substack{l|n \\ 1<l\leq e}} \sum_{\substack{F \\ [F:\mathbb{Q}]=le}} Z_F(le, n/l, X).$$

Together with (2.2) and (2.3) we get

$$Z(e,n,X) = \sum_{\substack{K \\ [K:\mathbb{Q}]=e}} Z_K(e,n,X) + O\left(\sum_{\substack{l|n \\ 1<l\leq e}} \sum_{\substack{F \\ [F:\mathbb{Q}]=le}} Z_F(le, n/l, X) \right) \tag{2.4}$$

The sums in (2.4) can essentially be reduced to the counting of projective points P in $\mathbb{P}^n$ of degree e with $H_{\mathcal{N}}(P) \leq X$ for a certain adelic-Lipschitz height $H_{\mathcal{N}}$. The next section is devoted to the basic definitions of this concept and the necessary results to derive the statements of this article.

3. Adelic-Lipschitz systems and adelic-Lipschitz heights

This section is (in fact in a more general form) contained in [16]. However, for convenience of the reader we recall the general concept of an adelic-Lipschitz system and its basic definitions.

3.1. **Adelic-Lipschitz systems on a number field.** Let r be the number of real embeddings and s the number of pairs of complex conjugate embeddings of K so that $e = r + 2s$. Recall that M_K denotes the set of places of K. For every place v we fix a completion K_v of K at v and we write $d_v = [K_v : \mathbb{Q}_v]$ with $\mathbb{Q}_v$ being the completion with respect to the place that extends to v. A place v in M_K corresponds either to a non-zero prime ideal $\mathfrak{p}_v$ in the ring of integers $\mathcal{O}_K$ or to an embedding σ of K into $\mathbb{C}$. If v comes from a prime ideal we call v a finite or non-archimedean place and denote this by $v \nmid \infty$ and if v corresponds to an embedding we say v is an infinite or archimedean place and denote this by $v \mid \infty$. For each place in M_K we choose a representative $|\cdot|_v$, normalized in the following way: if v is finite and $\alpha \neq 0$ we set by convention

$$|\alpha|_v = N\mathfrak{p}_v^{-\frac{\mathrm{ord}_{\mathfrak{p}_v}(\alpha\mathcal{O}_K)}{d_v}}$$

where $N\mathfrak{p}_v$ denotes the norm of $\mathfrak{p}_v$ from K to $\mathbb{Q}$ and $\mathrm{ord}_{\mathfrak{p}_v}(\alpha\mathcal{O}_K)$ is the power of $\mathfrak{p}_v$ in the prime ideal decomposition of the fractional ideal $\alpha\mathcal{O}_K$. Moreover we set

$$|0|_v = 0.$$

And if v is infinite and corresponds to an embedding $\sigma : K \hookrightarrow \mathbb{C}$ we define

$$|\alpha|_v = |\sigma(\alpha)|.$$

The value set of v, $\Gamma_v := \{|\alpha|_v; \alpha \in K_v\}$ is equal to $[0,\infty)$ if v is archimedean, and to

$$\{0, (N\mathfrak{p}_v)^0, (N\mathfrak{p}_v)^{\pm 1/d_v}, (N\mathfrak{p}_v)^{\pm 2/d_v}, ...\}$$

if v is non-archimedean. For $v \mid \infty$ we identify K_v with $\mathbb{R}$ or $\mathbb{C}$ respectively and we identify $\mathbb{C}$ with $\mathbb{R}^2$ via $\xi \longrightarrow (\Re(\xi), \Im(\xi))$ where we used $\Re$ for the real and $\Im$ for the imaginary part of a complex number.
For a vector $\mathbf{x}$ in $\mathbb{R}^n$ we write $|\mathbf{x}|$ for the euclidean length of $\mathbf{x}$.

Definition 1. *Let M and $D > 1$ be positive integers and let L be a non-negative real. We say that a set S is in Lip(D, M, L) if S is a subset of $\mathbb{R}^D$, and if there are M maps $\phi_1, ..., \phi_M : [0,1]^{D-1} \longrightarrow \mathbb{R}^D$ satisfying a Lipschitz condition*

$$|\phi_i(\mathbf{x}) - \phi_i(\mathbf{y})| \leq L|\mathbf{x} - \mathbf{y}| \textit{ for } \mathbf{x}, \mathbf{y} \in [0,1]^{D-1}, i = 1, ..., M$$

such that S is covered by the images of the maps ϕ_i.

We call L a Lipschitz constant for the maps ϕ_i. By definition the empty set lies in Lip(D, M, L) for any positive integers M and $D > 1$ and any non-negative L.

Definition 2 (Adelic-Lipschitz system)**.** *An adelic-Lipschitz system (ALS) $\mathcal{N}_K$ on K (of dimension n) is a set of continuous maps*

$$N_v : K_v^{n+1} \to \Gamma_v \quad v \in M_K$$

such that for $v \in M_K$ we have

(i) $N_v(\mathbf{z}) = 0$ *if and only if* $\mathbf{z} = \mathbf{0}$,

(ii) $N_v(\omega \mathbf{z}) = |\omega|_v N_v(\mathbf{z})$ *for all ω in K_v and all $\mathbf{z}$ in K_v^{n+1}*,

(iii) if $v \mid \infty$: $\{\mathbf{z}; N_v(\mathbf{z}) = 1\}$ is in Lip$(d_v(n+1), M_v, L_v)$ for some M_v, L_v,

(iv) if $v \nmid \infty$: $N_v(\mathbf{z}_1 + \mathbf{z}_2) \leq \max\{N_v(\mathbf{z}_1), N_v(\mathbf{z}_2)\}$ for all $\mathbf{z}_1, \mathbf{z}_2$ in K_v^{n+1}.

Moreover we assume that

$$N_v(\mathbf{z}) = \max\{|z_0|_v, ..., |z_n|_v\} \tag{3.1}$$

for all but a finite number of $v \in M_K$. To deduce our results we will use an *ALS* with (3.1) for all finite places v. This simplifies the notation and arguments in the sequal considerably. Therefore we assume from now on

$$N_v(\mathbf{z}) = \max\{|z_0|_v, ..., |z_n|_v\} \qquad \text{for all } v \nmid \infty. \tag{3.2}$$

So the functions N_v with $v \nmid \infty$ are as in Masser and Vaaler's [11] and the subset of N_v with $v \mid \infty$ defines an (r,s)-Lipschitz system (of dimension n) in the sense of [11]. However, opposed to Masser and Vaaler we will have to define a uniform *ALS* on the collection of all number fields of degree e, as introduced in [16]. Therefore we will use the terminology of [16]. With M_v and L_v from (iii) we define

$$\begin{aligned} M_{\mathcal{N}_K} &= \max_{v|\infty} M_v, \\ L_{\mathcal{N}_K} &= \max_{v|\infty} L_v. \end{aligned}$$

The set defined in (iii) is the boundary of the set $\mathbf{B}_v = \{\mathbf{z}; N_v(\mathbf{z}) < 1\}$ and therefore $\mathbf{B}_v$ is a bounded symmetric open star-body in $\mathbb{R}^{n+1}$ or $\mathbb{C}^{n+1}$ (see also [11] p.431). In particular $\mathbf{B}_v$ has a finite volume V_v.

Let us consider the system where N_v is as in (3.1) for all places v. If v is an infinite place then $\mathbf{B}_v$ is a cube for $d_v = 1$ and the complex analogue if $d_v = 2$. Their boundaries are clearly in $\mathrm{Lip}(d_v(n+1), M_v, L_v)$ most naturally with $M_v = 2n+2$ maps and $L_v = 2$ if $d_v = 1$ and with $M_v = n+1$ maps and for example $L_v = 2\pi\sqrt{2n+1}$ if $d_v = 2$. This system is called the standard adelic-Lipschitz system.

We return to general adelic-Lipschitz systems. We claim that for any $v \in M_K$ there is a c_v in the value group $\Gamma_v^* = \Gamma_v \backslash \{0\}$ with

$$N_v(\mathbf{z}) \geq c_v \max\{|z_0|_v, ..., |z_n|_v\} \tag{3.3}$$

for all $\mathbf{z} = (z_0, ..., z_n)$ in K_v^{n+1}. For if v is archimedean then $\mathbf{B}_v$ is bounded open and it contains the origin. Since Γ_v^* contains arbitrary small positive numbers the claim follows by (ii). Now for v non-archimedean it is trivially true by (3.2) and we can choose $c_v = 1$.

So let $\mathcal{N}_K$ be an ALS on K of dimension n. For every v in M_K let c_v be an element of Γ_v^*, such that $c_v \leq 1$ and (3.3) holds. Recall we can assume $c_v = 1$ for all finite places v. We define

$$C_{\mathcal{N}_K}^{fin} = \prod_{v\nmid\infty} c_v^{-\frac{d_v}{e}} = 1 \tag{3.4}$$

and

$$C_{\mathcal{N}_K}^{inf} = \max_{v|\infty}\{c_v^{-1}\} \geq 1.$$

Multiplying the finite and the infinite part gives rise to another constant

$$C_{\mathcal{N}_K} = C_{\mathcal{N}_K}^{fin} C_{\mathcal{N}_K}^{inf}. \tag{3.5}$$

Besides $M_{\mathcal{N}_K}$ and $L_{\mathcal{N}_K}$ this is another important quantity for an ALS. We say that $\mathcal{N}_K$ *is an ALS with associated constants* $C_{\mathcal{N}_K}, M_{\mathcal{N}_K}, L_{\mathcal{N}_K}$.

In [17] and [16] we introduced for an ALS $\mathcal{N}_K$ on K (of dimension n) the quantity $V_{\mathcal{N}_K}^{fin}$. This quantity depends only on the functions N_v in ALS

with $v \nmid \infty$ and we have shown in [17] (first paragraph on p.11) and also in [16] (just after equation (3.5)) that if (3.2) holds then $V_{\mathcal{N}_K}^{fin} = 1$. Hence we define

$$V_{\mathcal{N}_K}^{fin} = 1. \tag{3.6}$$

The infinite part is defined by

$$V_{\mathcal{N}_K}^{inf} = \prod_{v|\infty} V_v.$$

By virtue of (3.3) we observe that

$$V_{\mathcal{N}_K}^{inf} = \prod_{v|\infty} V_v \leq \prod_{v|\infty} (2C_{\mathcal{N}_K}^{inf})^{d_v(n+1)} = (2C_{\mathcal{N}_K}^{inf})^{e(n+1)}.$$

We multiply the finite and the infinite part to get a global volume

$$V_{\mathcal{N}_K} = V_{\mathcal{N}_K}^{inf} V_{\mathcal{N}_K}^{fin}. \tag{3.7}$$

Note that from (3.4), (3.5), (3.6) and (3.7) we derive

$$V_{\mathcal{N}_K} \leq (2C_{\mathcal{N}_K}^{inf} C_{\mathcal{N}_K}^{fin})^{e(n+1)} = (2C_{\mathcal{N}_K})^{e(n+1)}. \tag{3.8}$$

3.2. **Adelic-Lipschitz heights on $\mathbb{P}^n(K)$.** Let $\mathcal{N}_K$ be an *ALS* on K of dimension n. Write σ_v for the canonical embedding of K into K_v, extended componentwise to K^{n+1}. Then the height $H_{\mathcal{N}_K}$ on K^{n+1} is defined by

$$H_{\mathcal{N}_K}(\boldsymbol{\alpha}) = \prod_{v \in M_K} N_v(\sigma_v(\boldsymbol{\alpha}))^{\frac{d_v}{e}}.$$

Thanks to the product formula and (ii) from Subsection 3.1 $H_{\mathcal{N}_K}(\boldsymbol{\alpha})$ does not change if we multiply each coordinate of $\boldsymbol{\alpha}$ with a fixed element of K^*. Therefore $H_{\mathcal{N}_K}$ is well-defined on $\mathbb{P}^n(K)$ by setting

$$H_{\mathcal{N}_K}(P) = H_{\mathcal{N}_K}(\boldsymbol{\alpha})$$

where $P = (\alpha_0 : ... : \alpha_n) \in \mathbb{P}^n(K)$ and $\boldsymbol{\alpha} = (\alpha_0, ..., \alpha_n) \in K^{n+1}$. Multiplying (3.3) over all places with suitable multiplicities yields

$$H_{\mathcal{N}_K}(P) \geq C_{\mathcal{N}_K}^{-1} H(P) \tag{3.9}$$

for $P \in \mathbb{P}^n(K)$.

3.3. **Adelic-Lipschitz systems on a collection of number fields.** We define $\mathcal{C}_e$ as the collection of all number fields K of degree e

$$\mathcal{C}_e = \{K \subseteq \overline{\mathbb{Q}}; [K : \mathbb{Q}] = e\}.$$

Let $\mathcal{N}$ be a collection of adelic-Lipschitz systems $\mathcal{N}_K$ of dimension n - one for each K of $\mathcal{C}_e$. Then we call $\mathcal{N}$ an *adelic-Lipschitz system* (ALS) *on* $\mathcal{C}_e$ *of dimension* n. We say $\mathcal{N}$ is a *uniform ALS* on $\mathcal{C}_e$ of dimension n with associated constants $C_{\mathcal{N}}, M_{\mathcal{N}}, L_{\mathcal{N}}$ in $\mathbb{R}$ if the following holds: for each *ALS*

$\mathcal{N}_K$ of the collection $\mathcal{N}$ we can choose associated constants $C_{\mathcal{N}_K}, M_{\mathcal{N}_K}, L_{\mathcal{N}_K}$ satisfying

$$C_{\mathcal{N}_K} \leq C_{\mathcal{N}}, \quad M_{\mathcal{N}_K} \leq M_{\mathcal{N}}, \quad L_{\mathcal{N}_K} \leq L_{\mathcal{N}}.$$

A standard example for a uniform ALS on $\mathcal{C}_e$ (of dimension n) is given as follows: for each K in $\mathcal{C}_e$ choose the standard ALS on K (of dimension n) so that N_v is as in (3.1) for each v in M_K. For this system we may choose $C_{\mathcal{N}} = 1$, $M_{\mathcal{N}} = 2n+2$ and $L_{\mathcal{N}} = 2\pi\sqrt{2n+1}$.

3.4. **Adelic-Lipschitz heights on** $\mathbb{P}^n(\mathbb{Q}; e)$**.** Let $P = (x_0 : ... : x_n) \in \mathbb{P}^n(\overline{\mathbb{Q}})$ and define $\mathbb{Q}(P) = \mathbb{Q}(..., x_i/x_j, ...)$ $(0 \leq i, j \leq n;\ x_j \neq 0)$. Then we define the degree of P (over $\mathbb{Q}$) as $[\mathbb{Q}(P) : \mathbb{Q}]$. Write $\mathbb{P}^n(\mathbb{Q}; e)$ for the set of points P in $\mathbb{P}^n(\overline{\mathbb{Q}})$ with $[\mathbb{Q}(P) : \mathbb{Q}] = e$. Let $\mathcal{N}$ be an ALS of dimension n on $\mathcal{C}_e$. Now we can define heights on $\mathbb{P}^n(\mathbb{Q}; e)$. Let $P \in \mathbb{P}^n(\mathbb{Q}; e)$ so that $\mathbb{Q}(P) \in \mathcal{C}_e$. According to Subsection 3.2 we know that $H_{\mathcal{N}_K}(\cdot)$ defines a projective height on $\mathbb{P}^n(K)$ for each K in $\mathcal{C}_e$. Now we define

$$H_{\mathcal{N}}(P) = H_{\mathcal{N}_{\mathbb{Q}(P)}}(P).$$

If $\mathcal{N}$ is the standard adelic-Lipschitz system on $\mathcal{C}_e$ as defined in Subsection 3.3 then $H_{\mathcal{N}}$ is simply the multiplicative Weil height H on $\mathbb{P}^n(\overline{\mathbb{Q}})$ (as defined in [3] p.16) restricted to $\mathbb{P}^n(\mathbb{Q}; e)$.

4. Preliminary results

For K a number field let $\mathbb{P}^n(K/\mathbb{Q})$ be the set of primitive points in $\mathbb{P}^n(K)$

$$\mathbb{P}^n(K/\mathbb{Q}) = \{P \in \mathbb{P}^n(K); \mathbb{Q}(P) = K\}.$$

Let $\mathcal{N}_K$ be an adelic-Lipschitz system of dimension n on K. Then $H_{\mathcal{N}_K}(\cdot)$ defines a height on $\mathbb{P}^n(K)$. Now (3.9) combined with Northcott's Theorem implies that the counting function

$$Z_{\mathcal{N}_K}(\mathbb{P}^n(K/\mathbb{Q}), T) = |\{P \in \mathbb{P}^n(K/\mathbb{Q}); H_{\mathcal{N}_K}(P) \leq T\}|$$

is finite for all T in $[0, \infty)$. The main result Theorem 3.1 in [17] gives a precise estimate for this counting function. Here we need only a special case of Corollary 3.2 in [17] which by itself is a special case of Theorem 3.1 in [17]. Recall the definitions of $S_K(n)$ from (1.2) and $V_{\mathcal{N}_K}$ from (3.7).

Theorem 4.1. *Let K be number fields of degree e. Let $\mathcal{N}_K$ be an adelic-Lipschitz system of dimension n on K with associated constants $C_{\mathcal{N}_K}, L_{\mathcal{N}_K}, M_{\mathcal{N}_K}$ and write*

$$A_{\mathcal{N}_K} = M_{\mathcal{N}_K}^e (C_{\mathcal{N}_K}(L_{\mathcal{N}_K} + 1))^{e(n+1)-1}.$$

Then as $T > 0$ tends to infinity we have

$$\begin{aligned}Z_{\mathcal{N}_K}(\mathbb{P}^n(K/\mathbb{Q}), T) =&2^{-r_K(n+1)}\pi^{-s_K(n+1)}V_{\mathcal{N}_K}S_K(n)T^{e(n+1)}\\ &+O(A_{\mathcal{N}_K}R_K h_K \delta(K)^{-e(n+1)/2+1}T^{e(n+1)-1}\mathfrak{L}_0)\end{aligned}$$

where

$$\mathfrak{L}_0 = \log\max\{2, 2C_{\mathcal{N}_K}T\} \textit{ if } (n,e) = (1,1) \textit{ and } \mathfrak{L}_0 = 1 \textit{ otherwise}$$

and the implied constant in the O depends only on n and e.

Now let $\mathcal{N}$ be a uniform ALS on $\mathcal{C}_e$ of dimension n. Then $H_{\mathcal{N}}(\cdot)$ defines a height on $\mathbb{P}^n(\mathbb{Q}; e)$ and (3.9) implies for any $P \in \mathbb{P}^n(\mathbb{Q}; e)$

$$H_{\mathcal{N}}(P) \geq C_{\mathcal{N}}^{-1}H(P).$$

Again by Northcott's Theorem we conclude that the associated counting function $Z_{\mathcal{N}}(\mathbb{P}^n(\mathbb{Q}; e), T)$ (which denotes the number of points P in $\mathbb{P}^n(\mathbb{Q}; e)$ with $H_{\mathcal{N}}(P) \leq T$) is finite for all T in $[0, \infty)$. Bearing in mind the definitions of $S_K(n)$ and $V_{\mathcal{N}_K}$ from (1.2) and (3.7) we define the sum

$$D_{\mathcal{N}} = D_{\mathcal{N}}(\mathbb{Q}, e, n) = \sum_{K \in \mathcal{C}_e} 2^{-r_K(n+1)}\pi^{-s_K(n+1)}V_{\mathcal{N}_K}S_K(n). \tag{4.1}$$

We claim that the sum in (4.1) converges if n is large enough. Now we can state the main result of [16]. Again we need only a simpler form and so we state only this special case of the result.

Theorem 4.2. *Let e, n be positive integers. Suppose $\mathcal{N}$ is a uniform adelic-Lipschitz system of dimension n on $\mathcal{C}_e$, the collection of all number fields of degree e, with associated constants $C_{\mathcal{N}}, M_{\mathcal{N}}$ and $L_{\mathcal{N}}$. Write*

$$A_{\mathcal{N}} = M_{\mathcal{N}}^e(C_{\mathcal{N}}(L_{\mathcal{N}} + 1))^{e(n+1)-1}.$$

Suppose that either $e = 1$ or

$$n > 5e/2 + 4 + 2/e.$$

Then the sum in (4.1) converges and as $T > 0$ tends to infinity we have

$$Z_{\mathcal{N}}(\mathbb{P}^n(\mathbb{Q}; e), T) = D_{\mathcal{N}}T^{e(n+1)} + O(A_{\mathcal{N}}T^{e(n+1)-1}\mathfrak{L}_0),$$

where $\mathfrak{L}_0 = \log\max\{2, 2C_{\mathcal{N}}T\}$ if $(e, n) = (1, 1)$ and $\mathfrak{L}_0 = 1$ otherwise. The constant in O depends only on e and n.

The following upper bounds are immediate consequences of Schmidt's Theorem in [12].

Lemma 4.1. *Suppose $\mathcal{N}_K$ is an adelic-Lipschitz system (of dimension n) on K with associated constants $C_{\mathcal{N}_K}, M_{\mathcal{N}_K}, L_{\mathcal{N}_K}$. Then*

$$Z_{\mathcal{N}_K}(\mathbb{P}^n(K), T) \leq c_1(C_{\mathcal{N}_K}T)^{e(n+1)}. \tag{4.2}$$

One can choose $c_1 = 2^{e(n+4)+n^2+10n+11}$.

Now suppose $\mathcal{N}$ *is a uniform adelic-Lipschitz system (of dimension* n*) on* $\mathcal{C}_e$ *with associated constants* $C_{\mathcal{N}}, M_{\mathcal{N}}, L_{\mathcal{N}}$. *Then*

$$Z_{\mathcal{N}}(\mathbb{P}^n(\mathbb{Q};e),T) \leq c_2(C_{\mathcal{N}}T)^{e(e+n)}. \tag{4.3}$$

Here one can choose $c_2 = 2^{e(e+n+3)+e^2+n^2+10e+10n}$.

Proof. By (3.9) we know $H_{\mathcal{N}_K}(P) \geq C_{\mathcal{N}_K}^{-1}H(P)$ for $P \in \mathbb{P}^n(K)$, and similar for $P \in \mathbb{P}^n(\mathbb{Q},e)$ one has $H_{\mathcal{N}}(P) \geq C_{\mathcal{N}}^{-1}H(P)$. Thus the statements follow from Theorem, inequality (1.4) in [12]. □

We will also use Vinogradov's notation $A \ll B$ (or equivalently $B \gg A$) meaning that there exists a positive constant c depending solely on e and n (unless specified otherwise) such that $A \leq cB$. We remind the reader to the definition of the invariant $\delta(K) = \inf\{H(\alpha); K = \mathbb{Q}(\alpha)\}$. The following arguments will be used several times. It is therefore convenient to state them as two individual lemmas.

Lemma 4.2. *Let* K *be a number field of degree* $e > 1$ *and let* $P \in \mathbb{P}^n(K)$ *with* $\mathbb{Q}(P) = K$. *Then*

$$H(P) \geq \frac{1}{e(n+1)}\delta(K),$$
$$\delta(K) \geq e^{-\frac{1}{2(e-1)}}|\Delta_K|^{\frac{1}{2e(e-1)}}.$$

Proof. Let us start with the first inequality. Let $P = (\alpha_0 : ... : \alpha_n)$ then we can assume that one of the coordinates of P is 1. Hence $K = \mathbb{Q}(\alpha_0,...,\alpha_n)$. Now Lemma 3.3 in [17] gives an element $\alpha = \sum_{i=0}^n m_i\alpha_i$ with $0 \leq m_i < e$ in $\mathbb{Z}$ and $K = \mathbb{Q}(\alpha)$. Therefore $H(\alpha) \geq \delta(K)$, and a straightforward computation shows that $H(\alpha) \leq e(n+1)H(P)$. This proves the first inequality. The second inequality is a a special case of Silverman's inequality (Theorem 2 in [13]), but see also (4.10) and (4.12) in [16] (with $k = \mathbb{Q}$ and $m = 1$) for more details. □

Lemma 4.3. *Let* η *be a real number satisfying* $\eta < -e(e+1)$. *Then we have*

$$\sum_{K \in \mathcal{C}_e} \delta(K)^\eta \ll_\eta 1.$$

Proof. This lemma is an immediate consequence of Lemma 4.1 and Lemma 4.3 in [16]. □

5. Reformulation of Theorem 1.2 step two: choosing the right Adelic Lipschitz system

Let M be the Mahler measure on polynomials in one variable with complex coefficients as in [11]. For each number field F we define an *ALS* (of dimension n) denoted by $\mathcal{N}'_F$ by choosing

$$\begin{aligned} N_v(z_0,...,z_n) &= M(z_0x^n + ... + z_n) \quad (v \mid \infty), \\ N_v(z_0,...,z_n) &= \max\{|z_0|_v,...,|z_n|_v\} \quad (v \nmid \infty). \end{aligned} \tag{5.1}$$

Here v runs over all places in M_F. Masser und Vaaler have shown that M satisfies $(i),(ii),(iii)$ from Definition 2 and with N_v as in (5.1) clearly (iv) is satisfied as well. Therefore $H_{\mathcal{N}'_F}$ defines an adelic-Lipschitz height height on $\mathbb{P}^n(F)$. Now M_v and L_v depend on v (and n), but more precisely they depend only on $d_v \in \{1,2\}$ (and n). Hence $M_{\mathcal{N}'_F}$ and $L_{\mathcal{N}'_F}$ can be chosen independently of F, depending solely on n. Recall the definition of c_v from (3.3) in Section 3.1. For $v \nmid \infty$ we have $c_v = 1$ and for $v|\infty$ we may use $c_v = 2^{-n}$ (see [9] Lemma 2.2 p.56). Hence we may set

$$C_{\mathcal{N}'_F} = 2^n.$$

So we have shown that we can choose associated constants $C_{\mathcal{N}'_F} = 2^n$, $M_{\mathcal{N}'_F}$ and $L_{\mathcal{N}'_F}$ of the adelic-Lipschitz system $\mathcal{N}'_F$ depending only on n.

Now let K run over all fields in $\mathcal{C}_e$. The collection of adelic-Lipschitz systems $\mathcal{N}'_K$, one for each number field in $\mathcal{C}_e$, defines an adelic-Lipschitz system denoted by $\mathcal{N}'$ on $\mathcal{C}_e$. Then the corresponding height $H_{\mathcal{N}'}$ is defined on $\mathbb{P}^n(\mathbb{Q}; e)$. Furthermore we just have seen that the associated constants $C_{\mathcal{N}'_K} = 2^n, M_{\mathcal{N}'_K}, L_{\mathcal{N}'_K}$ of $\mathcal{N}'_K$ may be chosen uniformly, depending solely on n. Thus $\mathcal{N}'$ defines a uniform ALS on $\mathcal{C}_e$ with associated constants $C_{\mathcal{N}'} = 2^n, M_{\mathcal{N}'}, L_{\mathcal{N}'}$.

The proofs of our results require also the analogous heights to $H_{\mathcal{N}'_K}$ and $H_{\mathcal{N}'}$ on $\mathbb{P}^n$ but with n replaced by smaller values. By abuse of notation we will use the same symbols $H_{\mathcal{N}'_K}$ and $H_{\mathcal{N}'}$ for the analogous heights on e.g. $\mathbb{P}^{n-1}$. But this will cause no confusion.

We have a $1:1$-correspondence between monic polynomials in $K[x]$ of degree not exceeding n and $\mathbb{P}^n(K)$

$$f_0x^n + ... + f_1x + f_n \longleftrightarrow (f_0 : ... : f_n).$$

In this way $H_{\mathcal{N}'_K}$ can be considered as a function on the monic polynomials in $K[x]$ of degree $\leq n$. In this case we will use M_0 instead of $H_{\mathcal{N}'_K}$, so that $M_0(f) = H_{\mathcal{N}'_K}(P_f)$, where $P_f = (f_0 : ... : f_n)$ and $f = f_0x^n + ... + f_n$. However, we have also to count monic polynomials whose coefficents do not lie in K. Therefore it is convenient to notice that M_0 provides a definition on non-zero polynomials in $\overline{\mathbb{Q}}[x]$ of degree at most n. This can be seen in the following way; if F is any number field containing the coefficients of the non-zero polynomial $f = \alpha_0 x^n + ... + \alpha_n$ then we set

$$M_0(f) = H_{\mathcal{N}'_F}(P_f) = \prod_{v \in M_F} N_v(\sigma_v(\alpha_0), ..., \sigma_v(\alpha_n))^{d_v/[F:\mathbb{Q}]}.$$

But just as for the usual Weil height it is easy to see that this definition does not depend on the field F containing the coordinates and thus M_0 is well-defined on the non-zero polynomials in $\overline{\mathbb{Q}}[x]$ of degree at most n. The Mahler measure M is multiplicative which together with Gauss' Lemma implies

$$M_0(gh) = M_0(g)M_0(h) \tag{5.2}$$

for g, h in $\overline{\mathbb{Q}}[x]\backslash 0$ with $\deg gh \leq n$.

In the next section we shall see that the proofs of all the theorems can essentially be reduced to finding (asymptotic) estimates for $Z_{\mathcal{N}'}(\mathbb{P}^n(\mathbb{Q}; e), T)$ as given in Theorem 4.2.

6. Proofs of the Theorems

We remind the reader that K denotes a number field of degree e. As mentioned in the introduction for $e = 1$ or $n = 1$ all our theorems are covered by results of Schmidt [12], Masser and Vaaler [10], [11] and the author [17]. From now on we assume

$$e > 1 \text{ and } n > 1.$$

We start with the set

$$\mathcal{M}_K(n, T) = \{f \in K[x]; f \text{ monic}, \deg f \leq n, \mathbb{Q}(P_f) = K, M_0(f) \leq T\}.$$

Recall that $\mathbb{P}^n(K/\mathbb{Q})$ is the set of primitive points in $\mathbb{P}^n(K)$ and $Z_{\mathcal{N}'_K}(\mathbb{P}^n(K/\mathbb{Q}), T)$ is its counting function with respect to $H_{\mathcal{N}'_K}$. Then of course

$$|\mathcal{M}_K(n, T)| = Z_{\mathcal{N}'_K}(\mathbb{P}^n(K/\mathbb{Q}), T). \tag{6.1}$$

For any f in $\mathcal{M}_K(n, T)$ one has

$$T \geq M_0(f) = H_{\mathcal{N}'_K}(P_f).$$

Moreover we know $H_{\mathcal{N}'_K}(P_f) \geq C_{\mathcal{N}'_K}^{-1} H(P_f) = 2^{-n} H(P_f)$. Now $f \in \mathcal{M}_K(n, T)$ implies $K = \mathbb{Q}(P_f)$ and hence we can apply Lemma 4.2 to deduce

$$H(P_f) \geq \frac{1}{e(n+1)} \delta(K).$$

Note also that the Mahler measure of a monic polynomial is at least 1 and therefore $M_0(f) \geq 1$. So whenever $\mathcal{M}_K(n, T)$ is non-empty we have

$$T \geq 1, \tag{6.2}$$

$$T \geq \frac{\delta(K)}{2^n e(n+1)} \gg \delta(K). \tag{6.3}$$

For a subfield k of K let $\mathrm{Hom}_k(K)$ be the set of k-invariant field homomorphisms from K to its Galois closure K_G over $\mathbb{Q}$.
Let $\mathcal{M}_K^{(cp)}(n,T)$ be the set of all monic, irreducible polynomials f of degree n in $K[x]$, with σf are pairwise coprime as σ runs over $\mathrm{Hom}_{\mathbb{Q}}(K)$ and $M_0(f) \leq T$. Here the homomorphisms σ act on the coefficients of the polynomials. Note that the coprimality of the polynomials σf implies $\mathbb{Q}(P_f) = K$. Hence

$$\mathcal{M}_K^{(cp)}(n,T) = \{f \in \mathcal{M}_K(n,T)\backslash\mathcal{M}_K(n-1,T); f \text{ irreducible over } K, \\ \sigma f \text{ pairwise coprime } (\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K))\}.$$

Lemma 6.1. *We have*

$$Z_K(e,n,X) = n|\mathcal{M}_K^{(cp)}(n,X^n)|. \tag{6.4}$$

Proof. We will show that the map that sends β to its monic minimal polynomial over K defines a $n:1$-correspondence between the set $S_K(e,n,X) = \{\beta \in \overline{\mathbb{Q}}; [\mathbb{Q}(\beta):\mathbb{Q}] = en, [K(\beta):K] = n, H(\beta) \leq X\}$ (corresponding to the counting function $Z_K(e,n,X)$) and the set $\mathcal{M}_K^{(cp)}(n,X^n)$.
Let f be in $K[x]$ irreducible with $\deg f = n$. Then f has n zeros, they are pairwise distinct and, of course, each of them has degree n over K. Therefore we get a factor n. On the other hand every β with $[K(\beta):K] = n$ is a zero of exactly one irreducible monic polynomial f in $K[x]$. We factor $f = (x-\beta_1)...(x-\beta_n)$. Then

$$M_0(f) = M_0(x-\beta_1)...M_0(x-\beta_n).$$

Since f is irreducible all the zeros of f have the same height. But $H(\alpha) = M_0(x-\alpha)$ for any $\alpha \in \overline{\mathbb{Q}}$ and so we get

$$M_0(f) = H(\beta_1)^n. \tag{6.5}$$

This explains the power X^n.
Now let $D_{\beta,\mathbb{Q}}$ be the monic minimal polynomial of β over $\mathbb{Q}$. Then clearly $f|D_{\beta,\mathbb{Q}}$. If the σf are not pairwise coprime then

$$\prod_{\mathrm{Hom}_{\mathbb{Q}}(K)} \sigma f,$$

which of course lies in $\mathbb{Q}[x]\backslash\mathbb{Q}$, cannot be irreducible over $\mathbb{Q}$. Hence $[\mathbb{Q}(\beta):\mathbb{Q}] < |\mathrm{Hom}_{\mathbb{Q}}(K)| \deg f = en$ which means $\beta \notin S_K(e,n,X)$. Next we notice that for any σ of $\mathrm{Hom}_{\mathbb{Q}}(K)$ we have

$$\sigma f|\sigma D_{\beta,\mathbb{Q}} = D_{\beta,\mathbb{Q}}| \prod_{\mathrm{Hom}_{\mathbb{Q}}(K)} \sigma f.$$

Now suppose the σf are pairwise coprime then

$$\prod_{\mathrm{Hom}_{\mathbb{Q}}(K)} \sigma f|D_{\beta,\mathbb{Q}}$$

and we end up with $[\mathbb{Q}(\beta):\mathbb{Q}] = |\mathrm{Hom}_{\mathbb{Q}}(K)|\deg f = en$ which shows $\beta \in S_K(e,n,X)$. This completes the proof. □

To count $|\mathcal{M}_K^{(cp)}(n,T)|$ via $|\mathcal{M}_K(n,T)|$ another two sets are required. First we define the subset

$$\mathcal{M}_K^{(red)}(n,T) = \{f \in \mathcal{M}_K(n,T)\backslash\mathcal{M}_K(n-1,T); f \text{ reducible over } K\}.$$

So $\mathcal{M}_K^{(red)}(n,T)$ is the set of all monic reducible polynomials f of degree n in $K[x]$ with $K = \mathbb{Q}(P_f)$ and $M_0(f) \leq T$. Finally let

$$\begin{aligned}\mathcal{M}_K^{(ncp)}(n,T) = \{f \in \mathcal{M}_K(n,T)\backslash\mathcal{M}_K(n-1,T); f \text{ irreducible over } K,\\ \sigma f \text{ not pairwise coprime } (\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K))\}.\end{aligned}$$

Immediately from the definition we get

(6.6)
$$\mathcal{M}_K^{(cp)}(n,T) = \mathcal{M}_K(n,T)\backslash\left(\mathcal{M}_K(n-1,T) \cup \mathcal{M}_K^{(red)}(n,T) \cup \mathcal{M}_K^{(ncp)}(n,T)\right).$$

In particular

$$|\mathcal{M}_K^{(cp)}(n,T)| \leq |\mathcal{M}_K(n,T)|. \tag{6.7}$$

From (6.1) we get

$$\sum_{K\in\mathcal{C}_e} |\mathcal{M}_K(n,T)| = \sum_{K\in\mathcal{C}_e} Z_{\mathcal{N}'_K}(\mathbb{P}^n(K/\mathbb{Q}),T) = Z_{\mathcal{N}'}(\mathbb{P}^n(\mathbb{Q};e),T). \tag{6.8}$$

Now (2.1) and Lemma 6.1 yields

$$Z(e,n,X) \leq \sum_{K\in\mathcal{C}_e} Z_K(e,n,X) = n\sum_{K\in\mathcal{C}_e} |\mathcal{M}_K^{(cp)}(n,X^n)|.$$

Taking into account (6.6) and (6.8) gives

$$Z(e,n,X) \leq nZ_{\mathcal{N}'}(\mathbb{P}^n(\mathbb{Q};e),X^n). \tag{6.9}$$

In order to obtain asymptotic estimates more care is needed. Combining (2.4), (6.4) and (6.6) we get as $X > 0$ tends to infinity

$$\begin{aligned}Z(e,n,X) = n\sum_{K\in\mathcal{C}_e} |\mathcal{M}_K(n,X^n)| &+ O(\sum_{K\in\mathcal{C}_e} |\mathcal{M}_K(n-1,X^n)|)\\ &+ O(\sum_{K\in\mathcal{C}_e} |\mathcal{M}_K^{(red)}(n,X^n)|)\\ &+ O(\sum_{K\in\mathcal{C}_e} |\mathcal{M}_K^{(ncp)}(n,X^n)|)\\ &+ O(\sum_{\substack{l|n\\ 1<l\leq e}}\sum_{F\in\mathcal{C}_{le}} |\mathcal{M}_F^{(cp)}(n/l,X^{n/l})|).\end{aligned}$$

Applying (6.7) gives $|\mathcal{M}_F^{(cp)}(n/l, X^{n/l})| \leq |\mathcal{M}_F(n/l, X^{n/l})|$ and then applying (6.8) for the first, second and the last term yields

$$\begin{aligned} Z(e,n,X) = nZ_{\mathcal{N}'}(\mathbb{P}^n(\mathbb{Q};e), X^n) &+ O(Z_{\mathcal{N}'}(\mathbb{P}^{n-1}(\mathbb{Q};e), X^n)) \qquad (6.10)\\ &+ O(\sum_{K\in\mathcal{C}_e} |\mathcal{M}_K^{(red)}(n, X^n)|) \qquad (6.11)\\ &+ O(\sum_{K\in\mathcal{C}_e} |\mathcal{M}_K^{(ncp)}(n, X^n)|) \qquad (6.12)\\ &+ O(\sum_{\substack{l|n\\ 1<l\leq e}} Z_{\mathcal{N}'}(\mathbb{P}^{n/l}(\mathbb{Q};le), X^{n/l})). \qquad (6.13)\end{aligned}$$

To handle the error terms we need good uniform upper bounds for $Z_{\mathcal{N}'_F}(\mathbb{P}^n(F), T)$ and $Z_{\mathcal{N}'_F}(\mathbb{P}^n(F/\mathbb{Q}), T)$.

Lemma 6.2. *Let F be a number field and let $m \leq n$ be a positive integer. Then*

$$Z_{\mathcal{N}'_F}(\mathbb{P}^m(F), T) \ll_{[F:\mathbb{Q}]} T^{[F:\mathbb{Q}](m+1)}. \qquad (6.14)$$

Proof. Recall that $C_{\mathcal{N}'_F} = 2^m$ and $m \leq n$. Thus the statement follows from (4.2) in Lemma 4.1. □

Lemma 6.3. *Let F be a number field and let $m \leq n$ be a positive integer. Then*

$$Z_{\mathcal{N}'_F}(\mathbb{P}^m(F/\mathbb{Q}), T) \ll_{[F:\mathbb{Q}]} \frac{R_F h_F}{\delta(F)^{\frac{[F:\mathbb{Q}](m+1)}{2}}} T^{[F:\mathbb{Q}](m+1)}. \qquad (6.15)$$

Proof. The case $F = \mathbb{Q}$ is covered by the preceeding lemma, so we can assume $[F:\mathbb{Q}] > 1$. If $Z_{\mathcal{N}'_F}(\mathbb{P}^m(F/\mathbb{Q}), T) = 0$ then the claim is certainly true. Now assume $Z_{\mathcal{N}'_F}(\mathbb{P}^m(F/\mathbb{Q}), T) > 0$. In this case we know from (6.1) and (6.3) that $T \gg_{[F:\mathbb{Q}],m} \delta(F)$. For $[F:\mathbb{Q}] > 1$ Theorem 4.1 immediately implies

$$\begin{aligned} Z_{\mathcal{N}'_F}(\mathbb{P}^m(F/\mathbb{Q}), T) \ll_{[F:\mathbb{Q}],m,C_{\mathcal{N}'_F},M_{\mathcal{N}'_F},L_{\mathcal{N}'_F}} &\frac{R_F h_F}{|\Delta_F|^{\frac{(m+1)}{2}}} V_{\mathcal{N}'_F} T^{[F:\mathbb{Q}](m+1)}\\ &+ \frac{R_F h_F}{\delta(F)^{\frac{[F:\mathbb{Q}](m+1)}{2}-1}} T^{[F:\mathbb{Q}](m+1)-1}. \end{aligned}$$

Recall that $C_{\mathcal{N}'_F}, M_{\mathcal{N}'_F}, L_{\mathcal{N}'_F}$ depend only on m; but $m \leq n$ and thus they are $\ll 1$. Therefore and due to (3.8) we have $V_{\mathcal{N}'_F} \ll 1$. Moreover we get $T \gg_{[F:\mathbb{Q}]} \delta(F)$ and hence

$$Z_{\mathcal{N}'_F}(\mathbb{P}^m(F/\mathbb{Q}), T) \ll_{[F:\mathbb{Q}]} \frac{R_F h_F}{|\Delta_F|^{\frac{(m+1)}{2}}} T^{[F:\mathbb{Q}](m+1)} + \frac{R_F h_F}{\delta(F)^{\frac{[F:\mathbb{Q}](n+1)}{2}}} T^{[F:\mathbb{Q}](m+1)}.$$

Now Lemma 4.5 in [16] gives $|\Delta_F| \gg_{[F:\mathbb{Q}]} \delta(F)^{[F:\mathbb{Q}]}$. This proves the lemma. □

Note that by Siegel-Brauer's Theorem $R_K h_K \ll |\Delta_K|^{1/2+1/(40e(e-1))}$ and recall the inequality $\delta(K) \gg |\Delta_K|^{\frac{1}{2e(e-1)}}$ from Lemma 4.2. Thus we get

$$R_K h_K \ll \delta(K)^{e(e-1)+1/20}. \tag{6.16}$$

6.1. **An upper bound for $|\mathcal{M}_K^{(red)}(n,T)|$.** In this subsection we will prove an upper bound for the number of polynomials $f \in \mathcal{M}_K(n,T)$ of degree n that are reducible over K. Recall that by definition $\delta(K) \geq 1$ and by (6.2) and (6.3) we can assume $T \geq 1$ and $T/\delta(K) \gg 1$.

Suppose f factors as

$$f = gh$$

where g, h are in $K[x]\backslash K$ and monic. Since $K = \mathbb{Q}(P_f) \subseteq \mathbb{Q}(P_g, P_h) \subseteq K$ three cases may occur.

$$\begin{aligned}
(A):&\quad \mathbb{Q}(P_g) = K, \quad \mathbb{Q}(P_h) = K,\\
(B):&\quad \mathbb{Q}(P_g) \subsetneqq K, \quad \mathbb{Q}(P_h) = K,\\
(C):&\quad \mathbb{Q}(P_g) \subsetneqq K, \quad \mathbb{Q}(P_h) \subsetneqq K.
\end{aligned}$$

Let $\deg g = p$ so that $1 \leq p \leq n-1$ and $\deg h = n-p$. Assume $M_0(f) \leq T$. Now $M_0(f) \geq 1$ and hence there exists a positive integer i such that $2^{i-1} \leq M_0(g) < 2^i$ and then the multiplicativity (5.2) of M_0 gives $M_0(h) \leq 2^{1-i}T$. For fixed i we will estimate the number of polynomials $f = gh$ in each of the three cases (A), (B) and (C) separately and then we sum over all possible values for i, i.e. $i = 1, ..., [\log_2 T] + 1$.
To simplify the notation we abbreviate $\delta(K)$ to δ.

We start with the case (A). Here we can assume by symmetry that $p \leq n/2$. To bound the number of polynomials $f = gh$ we apply Lemma 6.3 with $F = K$. Thus for fixed i we get the upper bound

$$\begin{aligned}
&\ll \left(R_K h_K \delta^{-\frac{e}{2}(p+1)} (2^i)^{e(p+1)}\right) \left(R_K h_K \delta^{-\frac{e}{2}(n-p+1)} (2^{1-i}T)^{e(n-p+1)}\right)\\
&= 2^{e(n-p+1)} (2^i)^{e(2p-n)} (R_K h_K)^2 \delta^{-\frac{e}{2}(n+2)} T^{e(n-p+1)}
\end{aligned}$$

for the number of f. Now if $p < n/2$ then $\sum_i (2^i)^{e(2p-n)} \ll 1$ where the sum runs over all values $i = 1, ..., [\log_2 T] + 1$. So in this case we get the upper bound

$$\ll (R_K h_K)^2 \delta^{-\frac{e}{2}(n+2)} T^{en}$$

for the number of polynomials $f = gh$. Now suppose $n = p/2$. Then the sum over i introduces an additional logarithm and we find the upper bound

$$\ll (R_K h_K)^2 \delta^{-\frac{e}{2}(n+2)} T^{e(n/2+1)} \log(T+2) \ll (R_K h_K)^2 \delta^{-\frac{e}{2}(n+2)} T^{en}.$$

Next we use (6.16) to eliminate $R_K h_K$. This yields for the number in (A)

$$\ll \delta^{-\frac{e}{2}(n-4e+6)+0.1}T^{en}.$$

Next we estimate the number of polynomials in (B). We proceed similar as in (A). But here the situation is not symmetric hence we cannot assume $p \leq n/2$ and moreover we use (6.14) with $F \subsetneq K$ to bound the number of polynomials g. Note also that there are only $\leq 2^e \ll 1$ possibilities for F. For fixed i this yields the upper bound

$$\ll R_K h_K \delta^{-\frac{e}{2}(n-p+1)}T^{e(n-p+1)}2^{-\frac{ie}{2}(2n-3p+1)}.$$

Then summing over $i = 1, ..., [\log_2 T]+1$ we obtain 3 different upper bounds depending on whether $2n-3p+1 > 0$, $2n-3p+1 = 0$ or $2n-3p+1 < 0$. Finally we use $T/\delta \gg 1$ and (6.16) to deduce that also all of these 3 upper bounds are covered by

$$\ll \delta^{-\frac{e}{2}(n-4e+6)+0.1}T^{en}.$$

We are left with the case (C). Here we use (6.14) with $F \subsetneq K$ to bound the number of polynomials g and h. By symmetry we can assume $p \leq n/2$. Similar as in (A) we obtain the upper bound

$$\ll T^{\frac{en}{2}} \ll T^{\frac{en}{2}}(T/\delta)^{\frac{en}{2}} \ll \delta^{-\frac{e}{2}(n-4e+6)+0.1}T^{en}.$$

Again we can multiply the error terms arising from (A), (B) and (C) with $(T/\delta)^a$ as long as $a \geq 0$. We choose a such that the exponent on T is $e(n+1)-1$. Hence all three error terms are covered by

$$\ll \delta(K)^{-\frac{e}{2}(n-4e+8)+1.1}T^{e(n+1)-1}.$$

Thus we have proven

$$|\mathcal{M}_K^{(red)}(n,T)| \ll \delta(K)^{-\frac{e}{2}(n-4e+8)+1.1}T^{e(n+1)-1}. \tag{6.17}$$

6.2. **An upper bound for $|\mathcal{M}_K^{(ncp)}(n,T)|$.** As in the previous subsection we can assume $T \geq 1$ and $T/\delta(K) \gg 1$. Recall that K_G is the Galois closure of K over $\mathbb{Q}$. Suppose f is in $\mathcal{M}_K(n,T)$ and irreducible over K_G. Hence for all $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K)$ the σf are irreducible in $K_G[x]$ and since $\mathbb{Q}(P_f) = K$ they are pairwise distinct. Thus they are pairwise coprime. It follows

(6.18)

$$\mathcal{M}_K^{(ncp)}(n,T) \subseteq$$

$$\{f \in \mathcal{M}_K(n,T)\backslash\mathcal{M}_K(n-1,T); f \text{ irreducible over } K,\ f \text{ reducible over } K_G\}.$$

So let f be as above; that is $f \in K[x]$ monic, irreducible over K but reducible over K_G, $\deg f = n$ and $\mathbb{Q}(P_f) = K$. Let

$$f = g_1 ... g_s$$

be its decomposition into prime factors in $K_G[x]$ ($g_1, ..., g_s$ pairwise distinct, monic) and let

$$F = K(P_{g_1})$$

be the field, gotten by adjoining the coefficients of g_1 to K.

Lemma 6.4. *We have*

$$f = \prod_{\tau \in \mathrm{Hom}_K(F)} \tau g_1.$$

Proof. First notice that

$$\prod_{\tau \in \mathrm{Hom}_K(F)} \tau g_1 \in K[x].$$

For τ as in the product above we have

$$\tau g_1 | \tau f = f.$$

Since $\mathbb{Q}(P_{g_1}) = F$ the τg_1 are pairwise distinct. For any such τ there is a σ in Gal($\mathrm{K_G}/\mathbb{Q}$) with $\tau g_1 = \sigma g_1$. But g_1 is irreducible in $K_G[x]$ and so the σg_1 are all irreducible in $K_G[x]$. Thus the τg_1 are irreducible pairwise distinct divisors of f in $K_G[x]$ and therefore they are also pairwise coprime. This yields

$$\prod_{\tau \in \mathrm{Hom}_K(F)} \tau g_1 | f.$$

The left-hand side is in $K[x] \backslash K$ and monic. Since f is monic and irreducible over K they are equal. □

Let $f = (x - \beta_1)...(x - \beta_n)$ be the factorisation in $\overline{\mathbb{Q}}[x]$. The function M_0 is defined on polynomials in $\overline{\mathbb{Q}}[x]$ of degree not larger than n and is multiplicative. Therefore $M_0(f) = M_0(x - \beta_1)...M_0(x - \beta_n)$. Now f is irreducible in $K[x]$ so all the zeros have the same height or equivalently $M_0(x - \beta_1) = ... = M_0(x - \beta_n)$. In particular $M_0(g_1) = M_0(\tau g_1)$ for all $\tau \in \mathrm{Hom}_K(F)$. We conclude

$$T \geq M_0(f) = M_0(g_1)^{[F:K]}.$$

To bound the cardinality of the set in (6.18) above, we proceed as follows; for any intermediate field F with $K \subsetneq F \subseteq K_G$ we estimate the number of monic $g \in F[x]$ with

$$\deg g[F : K] = \deg f = n \tag{6.19}$$

$$M_0(g) \leq T^{\frac{1}{[F:K]}}. \tag{6.20}$$

Then we sum these estimates over all fields F. Hence we have

$$|\mathcal{M}_K^{(ncp)}(n, T)| \leq \sum_{\substack{F \\ K \subsetneq F \subseteq K_G}} |\{g \in F[x]; g \text{ monic }, \deg g = \frac{n}{[F : K]}, M_0(g) \leq T^{\frac{1}{[F:K]}}\}|.$$

Note that of course only fields F with $[F:K] \mid n$ give a contribution to the sum above. Hence we can assume $[F:K] \mid n$. Now clearly

$$Z_{\mathcal{N}'_F}(\mathbb{P}^{\frac{n}{[F:K]}}(F), T^{\frac{1}{[F:K]}}) = |\{g \in F[x]; g \text{ monic, } \deg g = \frac{n}{[F:K]}, M_0(g) \leq T^{\frac{1}{[F:K]}}\}|$$

and thus

$$|\mathcal{M}_K^{(ncp)}(n,T)| \leq \sum_{\substack{F \\ K \subsetneq F \subseteq K_G}} Z_{\mathcal{N}'_F}(\mathbb{P}^{\frac{n}{[F:K]}}(F), T^{\frac{1}{[F:K]}})$$

Applying Lemma 6.2, and not forgetting that by (6.19) $[F:\mathbb{Q}] \ll 1$, yields

$$Z_{\mathcal{N}'_F}(\mathbb{P}^{\frac{n}{[F:K]}}(F), T^{\frac{1}{[F:K]}}) \ll T^{\frac{[F:\mathbb{Q}]}{[F:K]}\left(\frac{n}{[F:K]}+1\right)} = T^{e\left(\frac{n}{[F:K]}+1\right)} \leq T^{\frac{en}{2}+e}.$$

The degree of K_G is bounded from above by $e!$. Therefore the number of intermediate fields F is bounded from above by $2^{e!} \ll 1$ and so we end up with

$$|\mathcal{M}_K^{(ncp)}(n,T)| \ll T^{\frac{en}{2}+e}.$$

As in the previous subsection we use (6.3) to deduce

$$\begin{aligned} |\mathcal{M}_K^{(ncp)}(n,T)| &\ll \delta(K)^{-\frac{en}{2}+1} T^{e(n+1)-1} \\ &\leq \delta(K)^{-\frac{e}{2}(n-4e+8)+1.1} T^{e(n+1)-1}. \end{aligned} \tag{6.21}$$

6.3. **Proof of Theorem 1.1.** Recall that $\mathcal{N}'$ defines a uniform ALS with $C_{\mathcal{N}'} = 2^n$. So (4.3) in Lemma 4.1 yields

$$Z_{\mathcal{N}'}(\mathbb{P}^n(\mathbb{Q};e), T) \leq c_2 (2^n T)^{e(n+e)}$$

where c_2 is defined in Lemma 4.1. This together with (6.9) yields immediately the following bound

$$Z(e,n,X) \leq n c_2 (2X)^{en(n+e)}$$

and thereby proves Theorem 1.1.

6.4. **Proof of Theorem 1.2.** Recall the fundamental equality (6.10). We start with the first term on the right hand-side of (6.10). Note that $n > \max\{e^2+e, 10\} \geq 5e/2+4+2/e$ unless $e=3$. But then $5e/2+4+2/e = 12+1/6$ and $e^2+e = 12$ and so $n > \max\{e^2+e, 10\}$ implies $n > 5e/2+4+2/e$ always. Hence we can apply Theorem 4.2 to conclude

$$nZ_{\mathcal{N}'}(\mathbb{P}^n(\mathbb{Q};e), X^n) = nD_{\mathcal{N}'}(\mathbb{Q},e,n) X^{en(n+1)} + O(X^{en(n+1)-n}) \tag{6.22}$$

where

$$D_{\mathcal{N}'}(\mathbb{Q},e,n) = \sum_{K \in \mathcal{C}e} 2^{-r_K(n+1)} \pi^{-s_K(n+1)} V_{\mathcal{N}'_K} S_K(n). \tag{6.23}$$

From (3.7) we recall that $V_{\mathcal{N}'_K} = V_{\mathcal{N}'_K}^{inf} V_{\mathcal{N}'_K}^{fin}$. The volume $V_{\mathcal{N}'_K}^{inf}$ has been computed by Masser und Vaaler in [11] p.435 (in their notation $V_{\mathcal{N}}$)

$$V_{\mathcal{N}'_K}^{inf} = 2^{r_K(n+1)} \pi^{s_K(n+1)} V_{\mathbb{R}}(n)^{r_K} V_{\mathbb{C}}(n)^{s_K}.$$

By definition (3.6) we have $V_{\mathcal{N}'_K}^{fin}=1$ and hence

$$V_{\mathcal{N}'_K}=2^{r_K(n+1)}\pi^{s_K(n+1)}V_{\mathbb{R}}(n)^{r_K}V_{\mathbb{C}}(n)^{s_K}, \tag{6.24}$$

supporting our main term.

Next we consider the second term on the right hand-side of (6.10). We could use Theorem 4.2 again, to get an upper bound for $Z_{\mathcal{N}'}(\mathbb{P}^{n-1}(\mathbb{Q};e),X^n)$. However, it is slightly better to proceed as follows. Clearly

$$Z_{\mathcal{N}'}(\mathbb{P}^{n-1}(\mathbb{Q};e),X^n)=\sum_{K\in\mathcal{C}_e}Z_{\mathcal{N}'_K}(\mathbb{P}^{n-1}(K/\mathbb{Q}),X^n).$$

Now from (6.15) and (6.16) we find

$$\begin{aligned}Z_{\mathcal{N}'_K}(\mathbb{P}^{n-1}(K/\mathbb{Q}),X^n)&\ll R_K h_K\delta(K)^{-en/2}X^{en(n-1)}\\&\ll \delta(K)^{-en/2+e(e-1)+0.05}X^{en(n-1)}.\end{aligned}\tag{6.25}$$

Next note that $n>\{e^2+e,10\}\geq 4e$. But $n>4e$ implies $-en/2+e(e-1)+0.05<-e(e+1)$ and so we conclude by virtue of Lemma 4.3

$$Z_{\mathcal{N}'}(\mathbb{P}^{n-1}(\mathbb{Q};e),X^n)\ll X^{en(n-1)}\ll X^{en(n+1)-n}, \tag{6.26}$$

where in the last inequality we used that we may assume $X\gg 1$ because $H_{\mathcal{N}'}(P)\gg 1$ for any P in $\mathbb{P}^{n-1}(\mathbb{Q};e)$.

Now appealing to (6.17) and (6.21) shows that the remaining terms coming from (6.11) and (6.12) are bounded by

$$\ll X^{en(n+1)-n}\sum_K \delta(K)^{-\frac{e}{2}(n-4e+8)+1.1}.$$

The latter sum is convergent by virtue of Lemma 4.3 provided $-\frac{e}{2}(n-4e+8)+1.1<-e(e+1)$ or equivalently $n>6e-6+2.2/e$. But $n>\{e^2+e,10\}$ implies $n>6e-6+2.2/e$ and so we have proved

$$\sum_K|\mathcal{M}_K^{(red)}(n,X^n)|+\sum_K|\mathcal{M}_K^{(ncp)}(n,X^n)|\ll X^{en(n+1)-n}.$$

To bound the last term in (6.13) we apply (4.3). Recalling $C_{\mathcal{N}'}\ll 1$ we find

$$\sum_{\substack{l|n\\1<l\leq e}}Z_{\mathcal{N}'}(\mathbb{P}^{n/l}(\mathbb{Q};le),X^{n/l})\ll\sum_{\substack{l|n\\1<l\leq e}}X^{en(le+n/l)}.$$

Again we may assume $X\gg 1$ because $H_{\mathcal{N}'}(P)\gg 1$. Now for $2\leq l\leq e$ we have $en(le+n/l)\leq en(n+1)-n$ provided $n\geq e^2+e+1/(e-1)$. But by hypothesis we have $n>\{e^2+e,10\}$ which implies $n\geq e^2+e+1/(e-1)$. Hence

$$\sum_{\substack{l|n\\1<l\leq e}}Z_{\mathcal{N}}(\mathbb{P}^{n/l}(\mathbb{Q};le),X^{n/l})\ll X^{en(n+1)-n}.$$

This completes the proof of Theorem 1.2.

6.5. **Proof of Theorem 1.3.** Again we start with the equality (6.10). Note that the extra condition on e and n in Theorem 1.3 implies that the sum in (6.13) is empty. In the proof of Theorem 1.2 we have seen that the O-terms in (6.10), (6.11) and (6.12) are bounded from above by $\ll X^{en(n+1)-n}$, subject to $n > \max\{5e/2+4+2/e, 4e, 6e-6+2.2/e\}$. But $\max\{6e-6+2.2/e, 10\} \geq \max\{5e/2+4+2/e, 4e\}$ and clearly $n > \max\{6e-6+2.2/e, 10\}$ if and only if $n > \max\{6e-6, 10\}$. Therefore the statement of the theorem follows from (6.22) and (6.23).

6.6. **Proof of Theorem 1.4.** We claim that

$$Z(e,m,n,X) = \sum_{K} Z_K(em,n,X) \tag{6.27}$$

where the sum runs over fields K of degree em that contain a subfield of degree e. Recall that $S_K(em,n,X)$ denotes the set counted by $Z_K(em,n,X)$ and let $S(e,m,n,X)$ denote the set counted by $Z(e,m,n,X)$.

First we show ”$\leq$“. Suppose β lies in $S(e,m,n,X)$. Hence there exists a field $k \subseteq \mathbb{Q}(\beta)$ and a field $K \subseteq \mathbb{Q}(\beta)$ with $[k:\mathbb{Q}] = e$ and $[K:\mathbb{Q}] = em$. Suppose k is not contained in K. Then $\mathbb{Q}(\beta)$, which has degree emn, contains the field compositum of k and K which has degree lem for an l satisfying $1 < l \leq e \leq em$ and $l|n$. But the latter contradicts the hypothesis of Theorem 1.4. Hence each β in $S(e,m,n,X)$ lies in at least one $S_K(em,n,X)$. Now we prove the other inequality ”$\geq$“. Of course each $\beta \in S_K(em,n,X)$ lies in $S(e,m,n,X)$. Now if β lies in $S_K(em,n,X)$ and in $S_{K'}(em,n,X)$ then $\mathbb{Q}(\beta)$, which has degree emn, contains the field compositum of the two different fields K and K' which has degree lem for an l satisfying $1 < l \leq em$ and $l|n$; again this contradicts the hypothesis of Theorem 1.4. This proves (6.27).

Recalling (6.1) and then applying Theorem 4.1 with (6.24) gives; as $X > 0$ tends to infinity

$$|\mathcal{M}_K(n,X^n)| = V_{\mathbb{R}}(n)^{r_K} V_{\mathbb{C}}(n)^{s_K} S_K(n) X^{emn(n+1)} \tag{6.28}$$

$$+ O(R_K h_K \delta(K)^{-em(n+1)/2+1} X^{emn(n+1)-n}). \tag{6.29}$$

And thanks to (6.16) the error term above is covered by

$$\ll \delta(K)^{-\frac{em}{2}(n-2em+3)+1.05} X^{emn(n+1)-n}. \tag{6.30}$$

Applying Lemma 4.3 shows that the above error term converge when summed over $\mathcal{C}_{em}$ and so in particular when summed over the subset of $\mathcal{C}_{em}$ of fields containing a subfield of degree e. Recall the definition (1.2) of $S_K(n)$. Using Siegel-Brauer's Theorem, $\delta(K) \gg_{[K:\mathbb{Q}]} |\Delta_K|^{1/(em)}$ from Lemma 4.5 in [16] and Lemma 4.3 we see that also the main term converge when summed over the subset of $\mathcal{C}_{em}$ of fields containing a subfield of degree e.

In the proof of Theorem 1.3 (but now with e replaced by em and $\mathcal{C}_e$ replaced by the subset of $\mathcal{C}_{em}$ consisting of fields that contain a subfield of degree e) we have seen that the remaining error terms coming from (6.6), namely (6.10), (6.11) and (6.12), are covered by the error term in Theorem 1.4. This completes the proof of Theorem 1.4.
As a final remark we point out that the condition $n > \max\{6em-6, 10\}$ could be slightly relaxed since we are summing over a thinner set than $\mathcal{C}_{em}$.

6.7. **Proof of Theorem 1.5.** Let β be as in Theorem 1.5 and let f be the monic minimal polynomial of β over K. Thus $\deg f = n$, f is irreducible over K and so f has exactly n pairwise distinct zeros. Moreover (1.4) is equivalent to $\mathbb{Q}(P_f) = K$. We have seen in (6.5) that $M_0(f) = H(\beta)^n$. Thus as $X > 0$ tends to infinity the number of elements β counted in Theorem 1.5 is given by

$$n|\mathcal{M}_K(n, X^n)| + O(|\mathcal{M}_K(n-1, X^n)|) + O(|\mathcal{M}_K^{(red)}(n, X^n)|). \tag{6.31}$$

From (6.28) and (6.30), but now with K of degree e instead of em, we get as $X > 0$ tends to infinity

$$\begin{aligned}|\mathcal{M}_K(n, X^n)| = {} & V_{\mathbb{R}}(n)^{r_K} V_{\mathbb{C}}(n)^{s_K} S_K(n) X^{en(n+1)} \\ & + O(\delta(K)^{-\frac{e}{2}(n-2e+3)+1.05} X^{en(n+1)-n}).\end{aligned}$$

The error term above is not larger than the error term in Theorem 1.5. For the first error term in (6.31) we refer to (6.25) and then we use (6.3). In this way we see that the first error term in (6.31) is also covered by the error term in Theorem 1.5. Finally due to (6.17) the last error term in (6.31) is also covered by the error term in Theorem 1.5. This completes the proof of Theorem 1.5.

References

1. A. M. Bailey, *On the density of discriminants of quartic fields*, J. reine angew. Math. **315** (1980), 190–210.
2. M. Bhargava, *Higher Composition Laws*, Ph.D. Thesis, Princeton Univ. (2001).
3. E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.
4. S-J. Chern and J. D. Vaaler, *The distribution of values of Mahler's measure*, J. reine angew. Math. **540** (2001), 1–47.
5. S. D. Cohen, *The distribution of Galois groups and Hilbert's irreducibility theorem*, Proc. London. Math. Soc. **43** (1981), 227.
6. H. Cohen F. Diaz Y Diaz and M. Olivier, *Enumerating quartic dihedral extensions of* $\mathbb{Q}$, Comp. Math. **133** (2002), 65–93.
7. R. Dietmann, *Probabilistic Galois theory for quartic polynomials*, Glasgow Mathematical Journal **48 (3)** (2006), 553–556.
8. J. Klüners, *A counter example to Malles conjecture on the asymptotics of discriminants*, C. R. Acad. Sci. Paris, Série I **340** (2005).
9. S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.

10. D. W. Masser and J. D. Vaaler, *Counting algebraic numbers with large height I*, Diophantine Approximation - Festschrift für Wolfgang Schmidt (eds. H. P. Schlickewei, K. Schmidt, R. F. Tichy), Developments in Mathematics 16, Springer 2008, (pp.237–243).
11. ______, *Counting algebraic numbers with large height II*, Trans. Amer. Math. Soc. **359** (2007), 427–445.
12. W. M. Schmidt, *Northcott's Theorem on heights I. A general estimate*, Monatsh. Math. **115** (1993), 169–183.
13. J. Silverman, *Lower bounds for height functions*, Duke Math. J. **51** (1984), 395–403.
14. S. Türkelli, *Connected components of Hurwitz schemes and Malle's conjecture*, submitted (2009).
15. B. L. van der Waerden, *Die Seltenheit der Gleichungen mit Affekt*, Math. Ann. **109** (1934), 13–16.
16. M. Widmer, *Counting points of fixed degree and bounded height*, to appear in Acta Arith. (2009).
17. ______, *Counting primitive points of bounded height*, to appear in Trans. Amer. Math. Soc. (2009).
18. S. Wong, *Automorphic forms on GL(2) and the rank of class groups*, J. reine angew. Math. **515** (1999), 125–153.

Institut für Mathematik, Technische Universität Graz, Steyrergasse 30/II, A-8010 Graz, Austria

E-mail address: widmer@tugraz.at