A SHORT REMARK ON THE ℓ-TORSION PART OF CLASS GROUPS

MARTIN WIDMER

Abstract. In a 2008 paper Ellenberg suggested a strategy to improve the known upper bounds for the ℓ-torsion part of class groups of number fields of fixed degree d. Motivated by this he proposed a question about the number of primitive elements of small height in a number field. Here we answer Ellenberg's question. We also improve Heath-Brown's bound for the ℓ-torsion part of class groups of purely cubic number fields, and we generalize our improvement to pure fields of arbitrary odd degree d.

1. Introduction

Let K be a number field of degree $d > 1$ and denote by D_K the absolute value of its discriminant. For arbitrary $\ell \in \mathbb{N} = \{1, 2, 3, \ldots\}$ let $\mathrm{Cl}_K[\ell] = \{[\mathfrak{a}] \in \mathrm{Cl}_K \,;\, [\mathfrak{a}]^\ell = [\mathcal{O}_K]\}$ be the ℓ-torsion of the ideal class group of the number field K. The most important tool to upper bound $\#\,\mathrm{Cl}_K[\ell]$ in terms of D_K, d, ℓ is Ellenberg and Venkatesh's "Key-Lemma" [5, Lemma 2.3] which yields

$$\#\,\mathrm{Cl}_K[\ell] \ll_{d,\ell,\varepsilon} D_K^{1/2-1/(2\ell(d-1))+\varepsilon}, \tag{1.1}$$

provided there are sufficiently many small suitable (e.g., splitting) primes, which is guaranteed under GRH. In a subsequent paper Ellenberg [4] pointed out that the proof actually yields the stronger conclusion

$$\#\,\mathrm{Cl}_K[\ell] \ll_{d,\ell,\varepsilon} D_K^{1/2-f(\ell,d)+\varepsilon}$$

for a certain function $f(\ell, d) \geq 1/(2\ell(d-1))$ defined in (2.7). Ellenberg proposes to study this function, more specifically he wrote: *"But at present it is not at all clear how to bound $M(K, \ell)$ or $f(\ell, d)$. As far as we know it might be possible for $N'_K(X)$ to start growing quite quickly once it becomes nonzero; in this case we would have $f(\ell, d) = 1/2\ell(d-1)$ and no improvement would be made on the results of* [5]. *In fact, Lecoanet* [12] *has carried out experiments for several dozen cubic fields K which seem to show just this kind of behavior. It would be very interesting to understand more fully the situation for cubic fields."*

In this short note we compute $f(\ell, 3)$ and more generally $f(\ell, d)$ whenever $\ell \geq d/2$.

Proposition 1. *Let $d > 1$ and $\ell \geq d/2$ be integers. Then $f(\ell, d) = 1/(2\ell(d-1))$.*

Therefore, at least for $\ell \geq d/2$, a direct implementation of Ellenberg's idea does not work. However, the topic has much evolved since 2008. The Key-Lemma has seen various refinements ([9, Proposition 2.1], [7, Proposition 2.1], and [11, Theorem 3.3]), leading to more suitable quantities than the above $N'_K(X)$. For some of these refined quantities sufficiently good upper bounds can be established, so that an adapted version of Ellenberg's idea does work, see, e.g., Chan and Koymans' new bound [2, Theorem 1.1] on the 3-torsion part of the class group of quadratic number fields.

There are rather few other instances where the hypothesis of the Key-Lemma can be established unconditionally, hence giving unconditional pointwise upper bounds for the ℓ-torsion. Wang [16] handled non-cyclic elementary abelian extensions (and later extended her result to include many additional nilpotent extensions [15]). Heath-Brown [10, Theorem 10 and 11] established (1.1) for quadratic and cubic fields with smooth discriminant. Assuming the minimal polynomial of a generator of $K/\mathbb{Q}$ has a particular shape also allows for pointwise bounds. Heath-Brown [10, Theorem 1] pointed out that (1.1) holds for pure cubic number fields, i.e., one has the unconditional upper bound

$$\#\,\mathrm{Cl}_K[\ell] \ll_{\varepsilon,\ell} D_K^{1/2-1/(4\ell)+\varepsilon} \tag{1.2}$$

for ℓ prime and every $K = \mathbb{Q}(\sqrt[3]{a})$ where $a > 1$ is a cube-free integer. Using ideas of Dubickas we can sharpen (1.2).

Proposition 2. *Let $K = \mathbb{Q}(a^{1/d})$ be a pure cubic field, and $a = A_1 A_2^2$ with positive integers A_1, A_2 both squarefree and coprime. Then we have*

$$\#\,\mathrm{Cl}_K[\ell] \ll_{\varepsilon,\ell} D_K^{1/2-1/(3\ell)+\varepsilon} A_2^{1/(3\ell)}$$

2010 *Mathematics Subject Classification.* Primary 11R29 Secondary 11G50.

Key words and phrases. Class groups, torsion, number fields, Weil height, pure extensions, upper bound, primitive elements, generators, small height.

for any $\varepsilon > 0$, and any positive integer ℓ.

We have $(A_1A_2)^2 \ll D_K \ll (A_1A_2)^2$ (see (1.5) below). By replacing a with a^2/A_2^3 we can swap the roles of A_1 and A_2. Hence we can assume $A_2 \le A_1$, and therefore $A_2 \ll D_K^{1/4}$. If a is squarefree (or squarefull) then we get

$$\#\operatorname{Cl}_K[\ell] \ll_{\varepsilon,\ell} D_K^{1/2-1/(3\ell)+\varepsilon}.$$

In the worst case when $A_1 \asymp A_2$ we recover (1.2). It should also be mentioned that for $\ell = 3$ one has

$$\#\operatorname{Cl}_K[3] \ll_{\varepsilon} D_K^{\varepsilon}$$

by work of Gerth [8] (see [10, (1.4)] for more details).

Our results apply for pure fields of any odd degree. We say K is a pure field of degree d if $K = \mathbb{Q}(\theta)$, where θ is a root of some irreducible $f(x) \in \mathbb{Z}[x]$ of the form $f(x) = x^d - a$. Although stated only for cubic fields, Heath-Brown's observation holds for pure fields of any odd degree, giving

$$\#\operatorname{Cl}_K[\ell] \ll_{\varepsilon,\ell,d} D_K^{1/2-1/(2(d-1)\ell)+\varepsilon} \tag{1.3}$$

for any $\varepsilon > 0$, and any positive integer ℓ (not just primes).

If $K = \mathbb{Q}(a^{1/d})$ is a pure field of degree d then we can assume

$$a = \prod_{i=1}^{d-1} A_i^i \tag{1.4}$$

where the positive integers $A_1, \dots, A_{d-1}$ are squarefree and pairwise coprime. If k and d are coprime then $(a^k)^{1/d}$ is also a generator of $\mathbb{Q}(a^{1/d})$. Therefore, one can replace[1] A_1 by A_k as we did above whenever helpful.

It is clear that each prime p dividing A_1 must occur with exponent at least $d-1$ in D_K. This shows that $\prod_{(k,d)=1} A_k^{d-1}$ divides D_K.

Each prime $p > d$ divides D_K at most with exponent $d-1$. For primes $p \le d$ we note that the discriminant of the polynomial $x^d - a$ is $\pm d^d a^{d-1}$. Hence, we get

$$\left(\prod_{(k,d)=1} A_k\right)^{d-1} \le D_K \ll_d (A_1 \cdots A_{d-1})^{d-1}. \tag{1.5}$$

Proposition 2 is an immediate consequence of the following result.

Proposition 3. *Let $d > 1$ be odd, and let $K = \mathbb{Q}(a^{1/d})$ be a pure field of degree d. Then we have*

$$\#\operatorname{Cl}_K[\ell] \ll_{\varepsilon,\ell,d} D_K^{1/2+\varepsilon} \left(\min_{\frac{d+1}{2} \le m \le d-1} \prod_{i=1}^{d-1} A_i^{\frac{i\cdot m}{d} - \lfloor \frac{i\cdot m}{d} \rfloor} \right)^{-1/\ell}$$

for any $\varepsilon > 0$, and any positive integer ℓ.

Let us consider two examples. If a is squarefree (i.e., $a = A_1$) then we get

$$\#\operatorname{Cl}_K[\ell] \ll_{\varepsilon,\ell,d} D_K^{1/2-1/(2(d-1)\ell)-1/(2d(d-1)\ell)+\varepsilon},$$

giving a small but significant improvement upon (1.3). If a is cubefree (i.e., $a = A_1A_2^2$), then we get

$$\#\operatorname{Cl}_K[\ell] \ll_{\varepsilon,\ell,d} D_K^{1/2-(d+1)/(2(d-1)\ell)+\varepsilon} A_2^{\frac{d-1}{2d\ell}},$$

or equivalently

$$\#\operatorname{Cl}_K[\ell] \ll_{\varepsilon,\ell,d} D_K^{1/2-1/(2(d-1)\ell)+\varepsilon} \left(\frac{A_2^{d-2}}{A_1}\right)^{1/(2d\ell)},$$

giving an improvement upon (1.3) provided A_1 is sufficiantly large in terms of A_2 and d.

Throughout this article the implied constants in Vinogradov's notation $\ll$ and $\gg$ are absolute unless dependence on further parameters is explicitly mentioned by adding subscripts.

[1]Suppose k is coprime to d. Delete all d-th powers from a^k to get $\phi_k(a)$. Then $\phi_k(a)^{1/d}$ is also a generator of K and we have

$$\phi_k(a) = \prod_{i=1}^{d-1} A_i^{[ik]},$$

where $[ik] \in \{1, 2, \dots, d\}$ with $ik \equiv [ik] \pmod d$.

2. Background and definitions

Let

$$H_K(\alpha) = \prod_{v \in M_K} \max\{1, |\alpha|_v\}^{d_v}$$

be the relative multiplicative Weil height of $\alpha \in K$. Here M_K denotes the set of places of K, and for each place v we choose the unique representative $|\cdot|_v$ that either extends the usual Archimedean absolute value on $\mathbb{Q}$ or a usual p-adic absolute value on $\mathbb{Q}$, and $d_v = [K_v : \mathbb{Q}_v]$ denotes the local degree at v. Note that this is exactly the height in [5, (2.2)] for the principal divisor $(\alpha, (\alpha))$ associated to $\alpha \in K^\times$.

Since $\max\{1, |\alpha\beta|_v\} \le \max\{1, |\alpha|_v\} \max\{1, |\beta|_v\}$ we conclude that

$$H_K(\alpha\beta) \le H_K(\alpha) H_K(\beta)$$

for all $\alpha, \beta \in K$. We write $\eta(K)$ for the minimal height of a primitive element[2]

$$\eta(K) = \inf\{H_K(\alpha); K = \mathbb{Q}(\alpha)\}.$$

First we recall Ellenberg and Venkatesh's Key-Lemma [5, Lemma 2.3]. Recall from [5] that a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is said to be an extension of a prime ideal from a subfield $K_0 \subsetneq K$ if there exists a prime ideal $\mathfrak{p}_0$ of $\mathcal{O}_{K_0}$ such that $\mathfrak{p} = \mathfrak{p}_\circ \mathcal{O}_K$. For such a prime ideal $\mathfrak{p}$ the residue degree $f(\mathfrak{p}/p)$ is necessarily larger than 1.

If $\mathfrak{p}$ and $\mathfrak{p}_0$ are non-zero prime ideals in $\mathcal{O}_K$ and $\mathcal{O}_{K_0}$ respectively and $\mathfrak{p} \mid \mathfrak{p}_0 \mathcal{O}_K$ then we say $\mathfrak{p}$ is unramified in K/K_0 if $\mathfrak{p}^2 \nmid \mathfrak{p}_0 \mathcal{O}_K$.

Lemma 1 (Ellenberg and Venkatesh)**.** *Suppose K is a number field of degree $d > 1$, $\delta < 1/(2\ell(d-1))$, and $\varepsilon > 0$. Moreover, suppose $\mathfrak{p}_1, \dots, \mathfrak{p}_M$ are M prime ideals in $\mathcal{O}_K$ of norm $N(\mathfrak{p}_i) \le D_K^\delta$ that are unramified in $K/\mathbb{Q}$ and are not extensions of prime ideals from any proper subfield of K. Then we have*

$$\#\operatorname{Cl}_K[\ell] \ll_{d,\ell,\gamma,\varepsilon} D_K^{1/2+\varepsilon} M^{-1}.$$

Here the hypothesis $\delta < 1/(2\ell(d-1))$ can be replaced by $\delta < \gamma/\ell$ as long as $\eta(K) > D_K^\gamma$. This fact will be used for the proof of Proposition 2.

It turns out that for a "typical" K one expects $\eta(K)$ to be much larger than $D_K^{1/(2(d-1))}$ and this led to improvements for the average $\#\operatorname{Cl}_K[\ell]$ over various families (see [17, 6, 7]).

Writing $N'_K(X)$ for the number of primitive elements in K of (relative) height less than X, Ellenberg [4, Proposition 1] pointed out that the proof of [5, Lemma 2.3] even provides the stronger conclusion

$$\#\operatorname{Cl}_K[\ell] \ll_{d,\ell,\varepsilon} D_K^{1/2+\varepsilon} X^{-1/\ell+\varepsilon}(1 + N'_K(X)), \tag{2.6}$$

provided there are $\gg_{d,\ell,\varepsilon} X^{1/\ell-\varepsilon}$ prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$ of norm $N(\mathfrak{p}) < X^{1/\ell}$ that are unramified in $K/\mathbb{Q}$ and are not extensions of prime ideals from any proper subfield of K. Following Ellenberg we define

$$M_{K,\ell} := \inf_X (X^{-1/\ell}(1 + N'_K(X))).$$

It is well-known (cf. [14, Theorem 2] or [13, Lemma 2]) that $\eta(K) > (1/2) D_K^{1/(2(d-1))}$, so that $N'_K(X) = 0$ whenever $X \le (1/2) D_K^{1/(2(d-1))}$. Hence,

$$M_{K,\ell} = \inf_{X \ge (1/2) D_K^{1/(2(d-1))}} (X^{-1/\ell}(1 + N'_K(X))) \le 2 D_K^{-1/(2\ell(d-1))},$$

and thus

$$f(\ell, d) := \liminf_{\substack{K \\ [K:\mathbb{Q}]=d}} \frac{-\log M_{K,\ell}}{\log D_K} \ge \frac{1}{2\ell(d-1)}. \tag{2.7}$$

3. A lower bound for $M_{K,\ell}$

To prove Proposition 1 we need a sufficently good lower bound for $M_{K,\ell}$. And for this in turn we need to have a good lower bound on the number of small generators

$$N'_K(X) = \#\{\gamma \in K; K = \mathbb{Q}(\gamma), H_K(\gamma) < X\}.$$

Surprisingly, it suffices to consider rational multiples of a minimal generator, and this gives us the next lemma.

Lemma 2. *Let K be a number field of degree $d > 1$, and let $\delta > 0$. Then $N'_K(\eta(K) D_K^\delta) \gg D_K^{2\delta/d}$.*

[2] By Northcott's Theorem such a minimal element exists.

Proof. Let $\alpha \in K$ with $H_K(\alpha) = \eta(K)$ and $\mathbb{Q}(\alpha) = K$. Now consider the primitive elements $\alpha\beta$ with nonzero $\beta \in \mathbb{Q}$ and $H_K(\beta) < D_K^{\delta/d}$. Note that $H_K(\beta) = H_{\mathbb{Q}}(\beta)^d$. Writing $\beta = b_1/b_0$ with coprime integers $b_0 > 0$ and b_1 it follows from the product formula that $H_{\mathbb{Q}}(\beta) = \max\{b_0, |b_1|\}$. Hence, there are $\gg T^2$ non-zero elements $\beta \in \mathbb{Q}$ with $H_{\mathbb{Q}}(\beta) < T$ if $T > 1$. Applying this with $T = D_K^{\delta/d} > 1$ we conclude that there are $\gg D_K^{2\delta/d}$ of these elements $\beta \in \mathbb{Q}$. Using the trivial estimate $H_K(\alpha\beta) \le H_K(\alpha)H_K(\beta)$ we conclude that $N'_K(\eta(K)D_K^{\delta}) \gg D_K^{2\delta/d}$. □

Now we can prove a lower bound for $M_{K,\ell}$.

Lemma 3. *Let K be a number field of degree $d > 1$ and suppose $\ell \ge d/2$. Then*

$$M_{K,\ell} \gg \eta(K)^{-1/\ell}.$$

Proof. If $X \le \eta(K)$ then $N'_K(X) = 0$. Hence,

$$\inf_{X \le \eta(K)} (X^{-1/\ell}(1 + N'_K(X))) = \eta(K)^{-1/\ell}. \tag{3.8}$$

If $X > \eta(K)$ then we can write $X = \eta(K)D_K^{\delta}$ for some $\delta > 0$, and thus

$$\inf_{X > \eta(K)} (X^{-1/\ell}(1 + N'_K(X))) = \inf_{\delta > 0} \left((\eta(K)D_K^{\delta})^{-1/\ell}(1 + N'_K(\eta(K)D_K^{\delta})) \right). \tag{3.9}$$

Plugging the bound from Lemma 2 into (3.9) shows that

$$\inf_{X > \eta(K)} (X^{-1/\ell}(1 + N'_K(X))) \gg \inf_{\delta > 0} ((\eta(K)D_K^{\delta})^{-1/\ell} D_K^{2\delta/d}) = \eta(K)^{-1/\ell} \inf_{\delta > 0} D_K^{\delta(2/d - 1/\ell)}.$$

Since $\ell \ge d/2$ we have $\inf_{\delta > 0} D_K^{\delta(2/d-1/\ell)} = 1$, and thus

$$\inf_{X > \eta(K)} (X^{-1/\ell}(1 + N'_K(X))) \gg \eta(K)^{-1/\ell}. \tag{3.10}$$

Combining (3.8) and (3.10) proves Lemma 3. □

4. proof of Proposition 1

We have already seen that $f(\ell, d) \ge 1/(2\ell(d-1))$. Let us now suppose that $\ell \le d/2$. From Proposition 3 we know that $-\log M_{K,\ell} \le \frac{1}{\ell}\log \eta(K) - \log C$ for some absolute constant $C > 0$. Hence,

$$f(\ell, d) = \liminf_{\substack{K \\ [K:\mathbb{Q}]=d}} \frac{-\log M_{K,\ell}}{\log D_K} \le \liminf_{\substack{K \\ [K:\mathbb{Q}]=d}} \frac{\log \eta(K)}{\ell \log D_K}. \tag{4.11}$$

The family of degree d-fields $K = \mathbb{Q}(a^{1/d})$ as in (1.5) with $a = A_1 A_{d-1}^{d-1}$ and $A_{d-1} \le A_1 \le 2A_{d-1}$ have a generator $\alpha = (A_1/A_{d-1})^{1/d}$ of height

$$\eta(K) \le H_K(\alpha) = A_1 \le \sqrt{2A_1 A_{d-1}} \le \sqrt{2} D_K^{1/(2(d-1))}.$$

Plugging the above estimate into (4.11) for this infinite family of fields shows that $f(\ell, d) \le 1/(2\ell(d-1))$. This completes the proof of Proposition 1.

5. Constructing suitable primes

The following lemma was observed by Heath-Brown (and possibly others including Jiuya Wang) but stated only for $d = 3$. For the convenience of the reader we give all details for general odd d.

Lemma 4. *Let $\delta > \varepsilon > 0$. Then there are $\gg_{\varepsilon,d} D_K^{\delta-\varepsilon}$ many prime ideals $\mathfrak{p}|p$ in $\mathcal{O}_K$ of degree $f(\mathfrak{p}/p) = 1$, ramification index $e(\mathfrak{p}/p) = 1$, and norm $N(\mathfrak{p}) < D_K^{\delta}$.*

Proof. Let K be a pure field of odd degree d. Hence there is a non-zero integer m, free of d-th powers, such that $f(x) = x^d - m$ is irreducible in $\mathbb{Z}[x]$, $K = \mathbb{Q}(\theta)$ and $f(\theta) = 0$.

Note that the discriminant of f has modulus $|\Delta_f| = d^d m^{d-1}$. Let $p|m$ be a prime divisor and p^a the maximal power dividing m. Thus $1 \le a \le d-1$. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal above p. Since $m = \theta^d$ it follows that $\mathfrak{p}|(\theta)$ and therefore $\mathfrak{p}^d|p^a$. Hence, $d \le a \cdot e(\mathfrak{p}/p)$. This shows that p ramifies in K.

The total number of primes p that ramify in K is $\omega(D_K) \ll_{\varepsilon} D_K^{\varepsilon}$. Next we show that for any unramified prime $p \equiv 2 \pmod d$ there exists a prime ideal $\mathfrak{p}|p$ in $\mathcal{O}_K$ of degree $f(\mathfrak{p}/p) = 1$, so that the claim follows from Dirichlet's prime number theorem.

So let p be a prime with $p \equiv 2 \pmod d$ and $p \nmid m$. Let g be a generator of the cyclic group $\mathbb{F}_p^{\times}$. Reducing the polynomial f modulo p gives $\overline{f}(x) = x^d - g^t$ for some integer t. Hence $\overline{f}$ has a root g^s in $\mathbb{F}_p^{\times}$ if and only if $sd \equiv t \pmod{p-1}$. The latter has a solution s if and only if $(d, p-1)|t$ which is true as $p \equiv 2 \pmod d$. Noting that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$ and applying Dedekind's factorisation theorem completes the proof. □

6. A height lower bound for generators of pure fields and proof of Proposition 3

Ellenberg and Venkatesh used Silverman's classical lower bound for generators α of K

$$H_K(\alpha) \gg_d D_K^{1/(2(d-1))} \tag{6.12}$$

to get (1.1). Dubickas [3, Theorem 1] has improved (6.12) for pure fields $K = \mathbb{Q}(a^{1/d})$ of odd degree d, provided a is prime. Following his proof and implementing the obvious minor modifications provides a lower bound for general a that improves (6.12) in some new cases, e.g., when a is squarefree.

For the next result let $K = \mathbb{Q}(a^{1/d})$ be a pure field of odd degree $d \geq 3$ with $a > 1$. Recall that we can assume

$$a = \prod_{i=1}^{d-1} A_i^i$$

where the positive integers $A_1, \ldots, A_{d-1}$ are squarefree and pairwise coprime.

Proposition 4 (Dubickas, 2023)**.** *Suppose $\alpha \in K$ and $K = \mathbb{Q}(\alpha)$. Then*

$$H_K(\alpha) > C_d \min_{\frac{d+1}{2} \leq m \leq d-1} \left(\prod_{i=1}^{d-1} A_i^{\frac{i\cdot m}{d} - \lfloor \frac{i\cdot m}{d} \rfloor} \right). \tag{6.13}$$

One can take $C_d = d^{-(2d-1)}$

Proof. For the convenience of the reader we reproduce Dubickas' proof [3, 4. Proof of Theorem 1] with the necessary slight modification in the final step. Let

$$\alpha = b_0 + b_1 a^{1/d} + \cdots + b_m a^{m/d}$$

where $m \in \{1, 2, \ldots, d-1\}$, $b_0, \ldots, b_m \in \mathbb{Q}$ and $b_m \neq 0$. Replacing α by α^{-1} (which does not change the height), we can assume that $m \geq (d+1)/2$ (see line after (4.3) in [3]). Let T be the leading coefficient of the minimal polynomial of α in $\mathbb{Z}[x]$ so that for $1 \leq j \leq d$ the conjugates α_j satisfy

$$\alpha_j = \sum_{k=0}^{m} b_k a^{k/d} \zeta^{(j-1)k}$$

where $\zeta = e^{2\pi i/d}$. By [3, Lemma 7] there are $X_1, \ldots, X_{m+1} \in F = \mathbb{Q}(\zeta)$ with $d^m X_j \in \mathcal{O}_F$, and

$$X_1\alpha_1 + \cdots + X_{m+1}\alpha_{m+1} = b_m a^{m/d} \tag{6.14}$$

and moreover,

$$|X_j| \leq \frac{1}{(2\sin(\pi/d))^m} \quad (1 \leq j \leq m+1). \tag{6.15}$$

We consider the X_j and the conjugates α_i as complex numbers and $|\cdot|$ denotes the standard absolute value on $\mathbb{C}$. Note that $T\alpha_j$ and $d^m X_j$ are algebraic integers and therefore also

$$d^m T(X_1\alpha_1 + \cdots + X_{m+1}\alpha_{m+1}) = d^m T b_m a^{m/d}$$

is an algebraic integer. Now $d^m T b_m$ is a non-zero rational number, say D_0/D with $(D_0, D) = 1$ and $D \geq 1$.

Combining (6.14) and (6.15) gives

$$a^{m/d}/D \leq d^m T|b_m| a^{m/d} \leq \frac{(m+1)d^m T \max_{1\leq j\leq m+1} |\alpha_j|}{(2\sin(\pi/d))^m}.$$

Since the height $H_K(\alpha)$ is equal to the Mahler measure of the minimal polynomial of α (see [1, Proposition 1.6.6]) we get

$$H_K(\alpha) = T\prod_{j=1}^{d} \max\{1, |\alpha_j|\} \geq T \max_{1\leq j\leq m+1} |\alpha_j| \geq \frac{(2\sin(\pi/d))^m}{(m+1)d^m} \cdot \frac{a^{m/d}}{D} > C_d \cdot \frac{a^{m/d}}{D}.$$

Next we claim that

$$D \leq \prod_{p|a} p^{\lfloor \frac{m\cdot \mathrm{ord}_p(a)}{d} \rfloor}.$$

Now $D_0 a^{m/d}/D$ and $a^{(d-m)/d}$ are both algebraic integers. Therefore, also their product aD_0/D is an algebraic integer. Since D_0 and D are coprime it follows that each prime divisor p of D must also divide a. Taking d-th powers and recalling that $D_0 a^{m/d}/D$ is an algebraic integer implies $d\cdot \mathrm{ord}_p(D) \leq m \cdot \mathrm{ord}_p(a)$, proving the claim.

Finally, we note that for $p|A_i$ we have $\mathrm{ord}_p(A_i) = i$, and hence,

$$\frac{a^{m/d}}{D} \geq \prod_{p|a} p^{\frac{m\cdot \mathrm{ord}_p(a)}{d} - \lfloor \frac{m\cdot \mathrm{ord}_p(a)}{d} \rfloor} \geq \prod_{i=1}^{d-1} A_i^{\frac{i\cdot m}{d} - \lfloor \frac{i\cdot m}{d} \rfloor}.$$

Recalling that $(d+1)/2 \le m \le d-1$ this completes the proof of the lemma. □

Using (6.12) to lower bound $\eta(K)$ and applying Lemma 4 yields (1.3). To prove Proposition 2 we use (6.13) instead of (6.12). We apply the stronger form of the Key-Lemma (Lemma 1), using the invariant $\eta(K)$, so that we can replace the hypothesis $\delta < 1/(2\ell(d-1))$ by $\delta < \gamma/\ell$ as long as $\eta(K) > D_K^{\gamma}$.

We set

$$\mathcal{A} := C_d \min_{\frac{d+1}{2} \le m \le d-1} \left(\prod_{i=1}^{d-1} A_i^{\frac{i\cdot m}{d} - \lfloor \frac{i\cdot m}{d} \rfloor} \right).$$

Define γ by $\mathcal{A} = D_K^{\gamma}$ so that $\eta(K) > D_K^{\gamma}$ by Proposition 4. We can assume $\gamma > 1/(2(d-1))$ as we already have (1.3). Next let $0 < \varepsilon < \gamma/\ell$ and set $\delta = \gamma/\ell - \varepsilon$. Applying the Key-Lemma (Lemma 1) and using Lemma 4 gives

$$\#\operatorname{Cl}_K[\ell] \ll_{\varepsilon,\ell,d} D_K^{1/2+\varepsilon} D_K^{-(\delta-\varepsilon)} = D_K^{1/2+3\varepsilon} \mathcal{A}^{-1/\ell}.$$

This concludes the proof.

References

1. E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.
2. S. Chan and P. Koymans, *A new pointwise bound for 3-torsion of class groups*, 2025.
3. Artūras Dubickas, *Minimal Mahler measures for generators of some fields*, Rev. Mat. Iberoam. **39** (2023), no. 1, 269–282. MR 4571605
4. J. Ellenberg, *Points of low height on $\mathbb{P}^1$ over number fields and bounds for torsion in class groups*, Computational arithmetic geometry, Contemporary Mathematics, vol. 463, Amer. Math. Soc., Providence, RI, 2008, 45–48.
5. J. Ellenberg and A. Venkatesh, *Reflection principles and bounds for class group torsion*, Int. Math. Res. Not. **no.1, Art. ID rnm002** (2007).
6. C. Frei and M. Widmer, *Average bounds for the ℓ-torsion in class groups of cyclic extensions*, Res. Number Theory **4:34** (2018).
7. ———, *Average bounds and higher moments for the ℓ-torsion in class groups*, Math. Ann. **379** (2021), 1205–1229.
8. Frank Gerth, III, *Ranks of 3-class groups of non-Galois cubic fields*, Acta Arith. **30** (1976), no. 4, 307–322. MR 422198
9. D. R. Heath-Brown and L. B. Pierce, *Averages and moments associated to class numbers of imaginary quadratic fields*, Compositio Math. **153 (11)** (2017), 2287–2309.
10. D.R. Heath-Brown, *ℓ-Torsion in Class Groups via Dirichlet L-functions*, arXiv:2412.07701v2 (2025).
11. P. Koymans and J. Thorner, *Bounds for moments of ℓ-torsion in class groups*, Math. Ann. **390** (2024), 3221–3237.
12. D. Lecoanet, *Report on undergraduate research project: elements of low height in cubic fields*, (2008).
13. D. Roy and J. L. Thunder, *A note on Siegel's lemma over number fields*, Monatsh. Math. **120** (1995), 307–318.
14. J. Silverman, *Lower bounds for height functions*, Duke Math. J. **51** (1984), 395–403.
15. J. Wang, *Pointwise bound for ℓ-torsion in class groups II: Nilpotent extensions*, 2020.
16. ———, *Pointwise bound for ℓ-torsion in class groups: elementary abelian extensions*, J. Reine Angew. Math. **773** (2021), 129–151. MR 4237969
17. M. Widmer, *Bounds for the ℓ-torsion in class groups*, Bull. London Math. Soc. **50** (2018), no. 1, 124–131.

TU Graz, Institute of Analysis and Number Theory, Steyrergasse 30/II, 8010 Graz, Austria
Email address: martin.widmer@tugraz.at