Contemporary Mathematics

Points of low height on $\mathbb{P}^1$ over number fields and bounds for torsion in class groups

Jordan S. Ellenberg

1. Introduction

Let K be a number field and ℓ a positive integer. The main theorem of [**3**] gives an upper bound for the order of the ℓ-torsion subgroup in the ideal class group Cl_K of K under the Generalized Riemann Hypothesis, which can be made unconditional in certain special cases (e.g. when $K/\mathbb{Q}$ is a quadratic extension and $\ell = 3$.) The main idea is to show that there are many ideal classes which are *not* ℓ-torsion. This is accomplished by showing that there are many ideals $I_1, I_2, \ldots, I_s$ of small height (in a sense which will be made precise below) but that there are no *principal* ideals of small height; this implies that $\ell I_1 - \ell I_2$, which also has small height, is non-principal, which shows that $I_1, I_2, \ldots, I_s$ represent distinct classes of $\mathrm{Cl}_K/\ell\mathrm{Cl}_K$. This shows that $\mathrm{Cl}_K[\ell]$ cannot be too large.

The aim of this note is to make the observation that the bounds of [**3**] could be improved if one had good bounds on the *number* of principal ideals of height at most X, when X is large enough that this number is nonzero. We are led to precise questions about the distribution of points of low height on $\mathbb{P}^1(K)$, which do not seem to have been well-investigated either theoretically or experimentally. Any nontrivial progress on these questions would lead to an improvement of the results of [**3**].

We remark that one expects to have $|\mathrm{Cl}_K[\ell]| \ll_{d,\epsilon} \Delta_K^\epsilon$, so one should be aware that the results proved here, which bound the order of $\mathrm{Cl}_K[\ell]$ below a positive power of Δ_K, are not expected to be anywhere close to sharp.

2. Ideals and heights

As in [**3**], we will need to work in the group of Arakelov divisors. Much of the discussion that follows is copied word-for-word from [**3**, §2].

Notation: Let K be a number field of degree d over $\mathbb{Q}$. Let I_K be the (free abelian) group of fractional ideals of K, let M_K be the set of infinite places of K, and let Δ_K be the absolute value of the discriminant of $K/\mathbb{Q}$. Write K_∞ for $K \otimes_{\mathbb{Q}} \mathbb{R}$.

2000 Mathematics Subject Classification. Primary: 11R29. Secondary: 11G50

This work was supported in part by NSF-CAREER Grant DMS-0448750 and a Sloan Research Fellowship.

Now write $\widetilde{\mathrm{Div}}_K^0$ for the group

$$\{(x, J) \in K_\infty^\times \times \mathrm{I}_K : \mathrm{Norm}(x) = \mathrm{Norm}(J)\}.$$

Then $K^\times$ is diagonally embedded in $\widetilde{\mathrm{Div}}_K^0$. We define the *Arakelov class group* $\widetilde{\mathrm{Cl}}_K$ to be $\widetilde{\mathrm{Div}}_K^0/K^\times$. This group carries a natural measure induced from (arbitrarily) chosen Haar measures on $\mathbb{R}^*$ and $\mathbb{C}^*$.

There is a natural notion of *height* on $\widetilde{\mathrm{Div}}_K^0$. Namely, for each (x, J) we define

$$H(x, J) = \prod_{\sigma \in M_K} \max(|\sigma(x)|^{\deg(\sigma)}, 1) \prod_{\mathfrak{p}} \max(\mathrm{Norm}(\mathfrak{p})^{-v_\mathfrak{p}(J)}, 1).$$

Then if (x, J) is the principal Arakelov divisor associated to some $y \in K^\times$, the height of (x, J) is precisely the usual height of y (considered as the point $(y : 1) \in \mathbb{P}^1(K)$. Note that if d_1, d_2 are elements of $\widetilde{\mathrm{Div}}_K^0$, we have $H(d_1, d_2) \ll_d H(d_1)H(d_2)$.

3. Bounds on torsion in class groups

Notation: the integers ℓ and d are fixed from now on, and all implicit constants are allowed to depend on ℓ, d, and any ϵ that is present. The important thing is that they are uniform in K.

For any positive real number X, denote by $N_K(X)$ the number of points in $\mathbb{P}^1(K)$ (that is, the number of principal Arakelov divisors) of height at most X.

Let $G = \widetilde{\mathrm{Div}}_K^0$, and let H be the subgroup of principal divisors. It is easy to check that $\mathrm{vol}(G/H) = h_K R_K$, where $h = |Cl_K|$ and R_K is the regulator of K. In particular, $\log \mathrm{vol}(G/H) \sim (1/2) \log \Delta_K$.

Write H_ℓ for the subgroup $\ell G + H$. Then G/H_ℓ is the maximal abelian quotient of Cl_K with exponent ℓ. One may show that $|G/H_\ell|$ is small by showing that H_ℓ/H has large volume.

Under the Generalized Riemann Hypothesis there are $\gg_{d,\epsilon} Y^{1-\epsilon}$ primes of $\mathbb{Q}$ less than Y which split completely in K, by the theorem of Lagarias and Odlyzko [**4**]. In particular, there are split primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_M$ of K which have norm at most $X^{1/\ell}$, with $M \gg_{d,\epsilon} X^{1/\ell-\epsilon}$. For each i between 1 and M, consider a small ball in G consisting of all pairs $(x, \mathfrak{p}_i)$ such that x satisfies

$$(1/2)|\mathrm{Norm}(\mathfrak{p}_i)|^{\deg(\sigma)/d} \le x_\sigma \le 2|\mathrm{Norm}(\mathfrak{p}_i)|^{\deg(\sigma)/d}.$$

for all archimedean valuations σ.

Let B be the set of points of the form b^ℓ, where b is an element of one of these balls. Note that each ball has volume bounded below by a constant, since it is a translate of a fixed region in $K_\infty^\times$. So B is a subset of H_ℓ whose volume is $\gg X^{1/\ell-\epsilon}$.

Let $\pi : B \to H_\ell/H$ be the natural map. If $\pi(x) = \pi(y)$, then x/y is an element of K^* of height $\ll X$. Suppose x/y lies in a proper subfield L of K. Then the valuation of x/y at every prime of K pulled back from L is trivial, since such primes are not totally split in $K/\mathbb{Q}$ and thus do not occur among the $\mathfrak{p}_i$. Thus x/y lies in $\mathscr{O}_L^*$, and in particular $i = j$. It follows that the image of x/y in $K \otimes \mathbb{R}$ lies in a compact neighborhood of 1 which is independent of K; it follows that the number of possibilities for x/y in $\mathscr{O}_L$ is bounded, since there are only finitely many algebraic integers with bounded degree and bounded archimedean absolute values.

Write $N'_K(X)$ for the number of elements of $\mathbb{P}^1(K)$ of height less than X which are *not* defined over any proper subfield of K. Then we have shown above that the size of each fiber of π is at most $c + N'_K(X)$. We conclude that

$$\mathrm{vol}|H_\ell/H| \geq \mathrm{vol}(B)(c + N'_K(X))^{-1} \gg X^{1/\ell-\epsilon}(c + N'_K(X))^{-1}.$$

and thus that

$$|\mathrm{Cl}_K[\ell]| \ll \Delta_K^{1/2+\epsilon} X^{-1/\ell+\epsilon}(c + N'_K(X)).$$

The content of Lemma 2.2 of [**3**] is that, when $X \ll \Delta_K^{\frac{1}{2(d-1)}}$, the only principal divisors of height less than X are the ones attached to points of $\mathbb{P}^1(L)$ for some proper subfield $L \subset K$. (We note that this is *not* quite a direct consequence of Minkowski's theorem, because we are looking for low-height points in K^*, not in the integer lattice $\mathscr{O}_K$.) In particular, one has $N'_K(X) = 0$ in this case, and this yields Proposition 3.1 of [**3**], which asserts that, assuming GRH,

$$|\mathrm{Cl}_K[\ell]| \ll \Delta_K^{1/2-1/2\ell(d-1)+\epsilon}.$$

But we have in fact proven the following a priori stronger proposition.

PROPOSITION 1. *For each number field K of degree d, define*

$$M(K) = \min_X (X^{-1/\ell}(c + N'_K(X)))$$

Then, assuming GRH, $|\mathrm{Cl}_K[\ell]| \ll \Delta_K^{1/2+\epsilon} M(K)$.

One could prove results without reliance on GRH in cases where K, ℓ satisfy the conditions of Proposition 3.6 of [**3**], for instance when $\ell = 3$ and $K/\mathbb{Q}$ is an extension of even degree disjoint from $\mathbb{Q}(\zeta_3)$.

If one defines

$$f(\ell, d) := \liminf_{K|[K:\mathbb{Q}]=d} (-\log M(K)/\log \Delta_K)$$

then one has, assuming GRH,

$$\mathrm{Cl}_K[\ell] \ll \Delta_K^{1/2-f(\ell,d)+\epsilon}.$$

But at present it is not at all clear how to bound $M(K)$ 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 $f(\ell, d) = \frac{1}{2\ell(d-1)}$ and no improvement would be made on the results of [**3**]. In fact, Lecoanet [**5**] 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.

A few final remarks and suggestions regarding $M(K)$ follow.

4. Guesses about $M(K)$

We first observe that one good way to make a guess about $M(K)$ would be numerical experimentation. At present, Lecoanet's work on cubic fields is the only investigation of this kind. The function field heuristics below suggest that there is some reason for optimism in higher degree, despite the negative flavor of Lecoanet's results with $d = 3$.

In the same vein, it would be interesting to investigate numerically the values of $g(d, \alpha) := \liminf_{K|[K:\mathbb{Q}]=d} \log N'_K(\Delta_K^\alpha)$ for various choices of α.

Another heuristic approach is to consider an analogous problem over function fields. Consider the set of all curves $C/\mathbb{F}_q$ endowed with a degree-d map $\pi : C \to \mathbb{P}^1$; such curves are called *d-gonal*. (Here $\mathbb{P}^1/\mathbb{F}_q$ is standing in for $\mathbb{Q}$; philosophically, any choice of a fixed base curve in place of $\mathbb{P}^1$ should do just as well.) Then the points of height at most q^n on $\mathbb{P}^1(\mathbb{F}_q(C))$ are just the morphisms of degree at most n from C to $\mathbb{P}^1$. Write $N_C(q^n)$ for the number of such morphisms, and write $N'_C(q^n)$ for the number of such morphisms ϕ such that $\phi \times \pi : C \to \mathbb{P}^1 \times \mathbb{P}^1$ is birational onto its image. Write Δ for the norm of the discriminant of π. If g is the genus of C, one has by the Riemann-Hurwitz formula that $g = (1/2)\log_q \Delta + O(1)$.

By Theorem 2.6 of [**1**], one knows that for the *general* n-gonal curve C, one has $N'_C(q^n) = 0$ for all $n < (g/2)+1$. In other words, $N'_C(X) = 0$ whenever $X \ll \Delta^{1/4}$. Once $d > 3$, this is stronger than the analogue of Lemma 2.2 of [**3**], which shows that for *all* d-gonal curves, $N'_C(X) = 0$ for $X \ll \Delta^{1/2(d-1)}$. In particular, this suggests that for a "typical" number field K, one might hope to have $M(K) \ll \Delta_K^{-1/(4\ell)}$.

The problem of bounding $N'_C(q^n)$ for an arbitrary, as opposed to generic, genus g d-gonal curve seems difficult. Indeed, even the problem of bounding the dimension of the space of degree-n maps from C to $\mathbb{P}^1$ is not well-understood; this amounts to understanding the dimension of the space of basepoint-free g^r_n's on C. This problem seems not to be well-understood at present, though see [**6**] for the $d = 3$ case and [**2**] for some results in the general case.

References

[1] E. Arbarello and M. Cornalba. Footnotes to a Paper of Beniamino Segrre. *Math. Ann.* 256 (1981) 341–362.

[2] E. Ballico and C. Fontanari. Linear series on k-gonal curves. *Ann. Univ. Ferrara Sez. VII (N.S.)* 47 (2001), 1–8.

[3] J.S. Ellenberg and A. Venkatesh. Reflection principles and bounds for class group torsion. To appear, *Internat. Math. Res. Not.*

[4] J. Lagarias and A. Odlyzko. Effective versions of the Chebotarev density theorem. Algebraic number fields: L-functions and Galois properties, 409–464, *Proc. Sympos., Univ. Durham, Durham, 1975.*

[5] D. Lecoanet. Report on undergraduate research project: elements of low height in cubic fields.

[6] G. Martens and F.-O. Schreyer. Line bundles and syzygies of trigonal curves. *Abh. Math. Sem. Univ. Hamburg* 56 (1986), 169–189.

Department of Mathematics, University of Wisconsin-Madison, 480 Lincoln Drive, Madison, WI, 53705

E-mail address: ellenber@math.wisc.edu