Tamely Ramified Towers and Discriminant Bounds for Number Fields

FARSHID HAJIR[1] and CHRISTIAN MAIRE[2]

[1]*Department of Mathematics, UCLA, Los Angeles, CA 90095, U.S.A.*
e-mail: fhajir@math.ucla.edu and Department of Mathematics, California State University,
San Marcos, San Marcos CA 92096, U.S.A. e-mail: fhajir@csusm.edu
[2]*Laboratoire A2X, Université Bordeaux I, Cours de la Libération, 33405 Talence Cedex,*
France. e-mail: maire@math.u-bordeaux.fr

Abstract. The root discriminant of a number field of degree n is the nth root of the absolute value of its discriminant. Let R_{2m} be the minimal root discriminant for totally complex number fields of degree $2m$, and put $\alpha_0 = \liminf_m R_{2m}$. One knows that $\alpha_0 \geqslant 4\pi e^\gamma \approx 22.3$, and, assuming the Generalized Riemann Hypothesis, $\alpha_0 \geqslant 8\pi e^\gamma \approx 44.7$. It is of great interest to know if the latter bound is sharp. In 1978, Martinet constructed an infinite unramified tower of totally complex number fields with small constant root discriminant, demonstrating that $\alpha_0 < 92.4$. For over twenty years, this estimate has not been improved. We introduce two new ideas for bounding asymptotically minimal root discriminants, namely, (1) we allow tame ramification in the tower, and (2) we allow the fields at the bottom of the tower to have large Galois closure. These new ideas allow us to obtain the better estimate $\alpha_0 < 83.9$.

Mathematics Subject Classifications (2000). 11R29, 11R37, 11R21.

Key words. Root discriminant, discriminant bounds, class field towers, Golod–Shafarevich.

1. Introduction

Suppose K is a number field of degree $n = r_1 + 2r_2$ and signature (r_1, r_2), i.e. K has r_1 real, and r_2 pairs of complex conjugate, embeddings. The *root discriminant rd_K* of K is defined by $rd_K = |d_K|^{1/n}$ where d_K is the discriminant of K. This invariant may be thought of as measuring the density of the integer lattice $\mathcal{O}_K$ embedded in $K \otimes \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ in the standard way (under the trace norm).

In 1891, Minkowski [Mi] used his 'geometry of numbers' to give an explicit lower bound for the discriminant of K which is exponential in the degree of K. Minkowski's estimate was substantially improved over the years using refinements of his technique. In 1974, Stark [St] introduced an analytic method (based on a study of the zeros of the Dedekind zeta function) for proving discriminant lower bounds. Stark's approach was refined by Odlyzko [O1], [O2] to improve substantially the estimates obtained from geometry of numbers. Meanwhile, Serre [Se1] introduced a variation based on the Guinand–Weil explicit formulas which was further inves-

tigated by Odlyzko [O3] and Poitou [P], leading to the best known lower bounds today (see the survey paper of Odlyzko [O4] for more details). Naturally, the best bounds are obtained under the assumption of the Generalized Riemann Hypothesis (GRH).

The asymptotic version of these bounds is as follows: If the degree n of K tends to infinity, then

$$rd_K \geqslant A^{2r_2/n} B^{r_1/n} e^{o(1)}; \tag{1}$$

here, unconditionally, we can take $A = 4\pi e^{\gamma} \approx 22.3$, $B = 4\pi e^{1+\gamma} \approx 60.8$, and on GRH, $A = 8\pi e^{\gamma} \approx 44.7$, $B = 8\pi e^{\gamma+\pi/2} \approx 215.3$, where $\gamma = 0.577\cdots$ is Euler's constant (see [O4]).

Lower bounds for discriminants have been found to be very useful in a wide variety of applications, the main one being estimation of class numbers (e.g. [Mas] and [Y2]; many more references can be found in [O4, References D]). For some other applications, see Fontaine [F], Serre [Se2], and Tate [T]. Moreover, the exact (non-asymptotic) versions of the bounds were observed to be quite sharp in low degrees, where the fields of least discriminant and given signature have been tabulated (see [Ma3]).

Thus, given the theoretical as well as practical importance of estimates of type (1), a very interesting question is: what are the best possible values for A and B? A more precise version of the problem, due to Martinet [Ma1], is as follows. Let $I = \mathbb{Q} \cap [0, 1]$. For a number field of signature (r_1, r_2) and degree $n = r_1 + 2r_2$, let $\tau(K) = r_1/n \in I$ be the proportion of its embeddings which are real. Let us call $\tau(K)$ the *infinity type* of K. Number fields of degree $n \geqslant 1$ and infinity type $t \in I$ exist if and only if nt and $n(1-t)/2$ are non-negative integers (see, for example, [ABC]). For such n and t, let $R_{n,t}$ be the minimal root discriminant for number fields of degree n and infinity type t. Define a function α on I by

$$\alpha(t) = \alpha_t = \liminf_{n \to \infty} R_{n,t},$$

where n is restricted to the whole numbers satisfying $nt \in \mathbb{Z}_{\geqslant 0}$, $n(1-t)/2 \in \mathbb{Z}_{\geqslant 0}$.

The problem, in greatest generality, is to determine the function α. The lower bound (1), which reads $\alpha(t) \geqslant A^{1-t}B^t$, is essentially all that is known about α. Some natural (and probably very difficult) questions are: Does α extend to a continuous function on the real unit interval? Indeed, dare one imagine that $\alpha(t) = \alpha_0^{1-t}\alpha_1^t$ for all t?! Does the bound (1) hold with $A = \alpha_0$, $B = \alpha_1$ at least? We expect that α is monotonically increasing, but even this seems (at least to us) to be a non-trivial question.

A more modest aim is to estimate α_0 and α_1. A lower bound is of course obtained from (1). On GRH, we have, for example, that $\alpha_0 > 44.7$ and $\alpha_1 > 215.3$. Thus, what we would like to have is an upper bound for these invariants. Proving an upper bound $\alpha_t \leqslant b$ is tantamount to the demonstration of existence of number fields of arbitrarily large degree and infinity type t with root discriminant bounded by

b. The standard device for doing so is the Hilbert class field tower: Thanks to the work of Golod and Shafarevich [GS], certain number fields can be shown to admit infinite unramified extensions — note that the root discriminant is unchanged in an unramified extension.

In 1978, Martinet [Ma1] constructed infinite Hilbert class field towers with lowest known root discriminant, showing, in particular, that $\alpha_0 < 92.4$ and $\alpha_1 < 1058.6$. For over twenty years, Martinet's examples have not been beaten, despite the compilation of tables of number fields and the advent of number theory packages such as Pari and Kant. Our main aim here is to expand the scope of Martinet's method for finding upper bounds for α_t. We illustrate this by improving the upper estimate for α_0: our main result is that $\alpha_0 < 83.9$.

We now review Martinet's method, then describe our ideas which allow the improvement of the upper bound for α_0. We are hopeful that it will be possible to lower the estimate for α_1 as well, but we limit ourselves to the totally complex case here.

In the Golod–Shafarevich theory, one fixes a prime ℓ and studies the maximal ℓ-extension of a number field K unramified everywhere. Their criterion says that if the ℓ-rank of the ideal class group of K is bounded below by an explicit function of the ℓ-rank of the unit group of K, then this maximal unramified ℓ-extension is infinite. (For background on the arithmetic of ℓ-extensions, see Koch [K] and Maire [M]). Number fields with large ℓ-class rank can be constructed using Gauss' genus theory, suitably generalized; for this, it suffices to have a Galois extension K/k of degree ℓ in which many places are ramified – note that this forces up the discriminant of K. In practice, one usually applies all of this with $\ell = 2$.

Roughly speaking, then, the problem is to construct a quadratic extension K/k in which many places ramify, but whose root discriminant is not too large. Martinet's idea is to take an extension $k/\mathbb{Q}$ of suitably large degree and a quadratic extension $F/\mathbb{Q}$ such that the ramifying places in $F/\mathbb{Q}$ are highly decomposed in $k/\mathbb{Q}$. By composing the two fields, one obtains a quadratic extension $K = Fk/k$ with many ramifying places. Using this scheme, the calculation of ramification in K/k descends to $F/\mathbb{Q}$ and is therefore much easier to control. Note that, in practice, one had better take k to be Galois (even Abelian) over $\mathbb{Q}$, since we want at least one small prime to split completely in k, and that K is then also Galois (abelian) over $\mathbb{Q}$.

We now describe our ideas. Our first observation is that requiring the set of ramifying primes in K/k to be Galois-stable (over $\mathbb{Q}$) is too restrictive. We found asymmetrical constructions to yield better results. In fact, in our best example (Example C1 of Section 3.2), even the *infinite* places ramifying in K/k do not form a complete set of conjugates over $\mathbb{Q}$. Our second observation is that although *unramified* towers are nice from the point of view that the root discriminant is *constant* all the way up the tower, all that is needed is that the root discriminants remain *bounded*, a property possessed by *tamely ramified* towers. The extra contribution to the root discriminant from allowing ramification is offset handsomely by its effect

on the number of generators and relations of the Galois group in question. Namely, the number of generators is either augmented or unchanged, and (the upper bound on) the number of relations decreases by 1; this is often just enough for the relevant Galois group to pass the Golod–Shafarevich test for infinitude.

Thus far, we have found that *both* of these ideas are required for improving Martinet's records. But already the use of non-Galois extensions is enough to produce dozens of totally complex infinite unramified towers with root discriminant below 100, whereas we know of only six examples with this property constructed strictly with Martinet's technique.

We do not discuss the well-known analogies between the estimation of the least genus of a curve over a finite field with a given number points and the estimation of root discriminants of number fields, but refer the reader to the papers of Serre [Se3], Ihara [I] and Tsfasman–Vladut [TV] (in the latter two, the two cases are treated side by side). We refer also to the recent work of Angles and Maire [AM] where tame towers are used to obtain better estimates for curves over $\mathbb{F}_3$ and $\mathbb{F}_5$.

Let us call a sequence $\mathcal{K} = \{K_j\}$ of pairwise distinct number fields, none of which is $\mathbb{Q}$, a *family*. By taking into account the splitting behavior of primes in an infinite Hilbert class field tower L/K, Ihara [I] gives a refinement of (1) applied to a family $\{K_j\}$ where $K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset L$ is any nested family contained in L/K. Ihara raised the possibility that the addition of this extra term would, in special cases, render the inequality (1) into an *equality*, and for this reason introduced a certain 'deficiency' $\delta_{\mathcal{K}}$ which measures how far the inequality is from being an equality for a family $\mathcal{K}$ arising from an infinite class field tower L/K. Tsfasman and Vladut [TV] have recently extended Ihara's work considerably by treating completely general families. The lowest deficiency given in [TV] results from Martinet's example (Section 3.1, Example 5) with $\delta \leqslant 0.160\cdots$. The deficiencies for the nine towers we construct in Section 3.2 have smaller upper bounds, the best being $\delta \leqslant 0.141\cdots$ (see the last part of Section 3.2).

It was first pointed out by Litsyn and Tsfasman [LT] that any family of number fields with bounded root discriminant gives rise to lattices (the standard integer lattice under the trace norm) of arbitrarily large dimension and bounded packing density; for more details on this topic, see the book by Conway and Sloane [CS, Chapter 8, Section 7]. On GRH, the best asymptotic density obtained from such a construction satisfies (using the notation from [CS]) $(1/n_i)\log_2(\Delta_i) \leqslant -1.695\cdots$ for $i \to \infty$. Once again, the best known packing density obtained in this way has been that obtained from Martinet's example (Section 3.1, Example 5), with asymptotic packing density $(1/n_i)\log_2(\Delta_i) \geqslant -2.217\cdots$ [LT]. Our best example gives a slightly better asymptotic packing density $(1/n_i)\log_2(\Delta_i) \geqslant -2.148\cdots$

We would like to remark that, *once found*, verifying the validity of the examples we describe in this paper can be done by hand. However, the computer package Pari [B], as well as the tables of number fields available online from the Pari ftp site ftp://megrez.math.u-bordeaux.fr/pub/numberfields, were invaluable to us as we searched for strategies to construct these examples.

2. Golod–Shafarevich for Tame Towers

In this section, we describe our construction of infinite towers with bounded root discriminant. We make use of four principal results: the theorem of Golod–Shafarevich (slightly improved by Vinberg and Gaschutz) on presentations of finite groups of prime power order, the theorem of Shafarevich giving an estimate for the number of relations of the Galois group of the maximal unramified-outside-T ℓ-extension of a number field, a standard genus-theory estimate for the ℓ-rank of the class group of an extension of degree ℓ, and finally a calculation of root discriminants in tamely-ramified ℓ-extensions. For the convenience of the reader, we first gather together these results; our main construction is a simple application of them.

Notation. In this section, we fix an arbitrary prime ℓ. In the next section, we will work exclusively with $\ell = 2$. For a finitely generated pro-ℓ group G, we let $d(G) = \dim_{\mathbb{F}_\ell} H^1(G, \mathbb{F}_\ell)$, $r(G) = \dim_{\mathbb{F}_\ell} H^2(G, \mathbb{F}_\ell)$ be its generator and relation rank, respectively. Let K be a number field and T a finite set of primes of K. In an ℓ-extension of K, primes $\mathcal{P}$ such that ℓ does not divide $\mathbb{N}\mathcal{P}(\mathbb{N}\mathcal{P} - 1)$, cannot ramify. Without loss of generality, therefore, we will assume that for evey $\mathcal{P} \in T$, ℓ divides either $\mathbb{N}\mathcal{P}$ or $\mathbb{N}\mathcal{P} - 1$. We say that T is 'away from ℓ' if no primes in T is a divisor of ℓ. For such a T, let $\mathfrak{m}_T = \prod_{\mathcal{P} \in T} \mathcal{P}$ be the corresponding modulus. We let $\mathrm{Cl}(K), \mathrm{Cl}_T(K)$ be the ideal class group and ray class group modulo $\mathfrak{m}_T$ of K, respectively, and write $\rho_K, \rho_{K,T}$ for their respective ℓ-ranks. We write E_K for the unit group of K. Let K_T be the maximal ℓ-extension of K unramified outside T, and put $G_{K,T} = \mathrm{Gal}(K_T/K)$ for its Galois group. Note that, by the Burnside Basis Theorem, and class field theory, $d(G_{K,T}) = \rho_{K,T}$. When T is empty, K_T/K is the Hilbert class field tower of K. We say that an ideal of K is odd if its absolute norm is odd. We let

$$\theta_{K,T} = \begin{cases} 1 & \text{if } T \text{ is empty and } K \text{ contains a primitive } \ell\text{th root of unity} \\ 0 & \text{otherwise.} \end{cases}$$

THEOREM 1 (Golod–Shafarevich). *If G is a non-trivial finite ℓ-group, then $r(G) > d(G)^2/4$.*

    Proof. See, for example, Roquette [R]. $\qquad\square$

THEOREM 2 (Shafarevich). *Suppose K is a number field with signature (r_1, r_2). For a finite set T of prime ideals of K away from ℓ, we have*

$$0 \leqslant r(G_{K,T}) - d(G_{K,T}) \leqslant r_1 + r_2 - 1 + \theta_{K,T}.$$

    Proof. This is immediate by combining Theorems 1 and 5 in [Sh], or Satz 11.5 and Satz 11.8 in [K]. See also [M]. Note that the bound on the right can be interpreted as the ℓ-rank of the subgroup of E_K consisting of units congruent to 1 modulo $\mathfrak{m}_T$. $\qquad\square$

THEOREM 3 (Golod–Shafarevich Criterion). *Suppose K is a number field with signature (r_1, r_2), and T is a finite set of prime ideals of K away from ℓ. If*

$$\rho_{K,T} \geqslant 2 + 2\sqrt{r_1 + r_2 + \theta_{K,T}},$$

then $G_{K,T}$ is infinite.

Proof. Recall that $\rho_{K,T} = d(G_{K,T})$. Suppose that $G_{K,T}$ is finite. By Theorem 1 and Theorem 2, we have

$$d(G_{K,T})^2/4 - d(G_{K,T}) < r_1 + r_2 - 1 + \theta_{K,T}$$

which implies that

$$d(G_{K,T}) < 2 + 2\sqrt{r_1 + r_2 + \theta_{K,T}}$$

and this contradicts the hypothesis. One can actually show that $G_{K,T}$ is not ℓ-adic analytic, i.e. it is not a Lie group over $\mathbb{Q}_\ell$ (see [H]).   □

Remark. For $\ell = 2$, if we take K to be totally complex of degree 8, the Golod–Shafarevich bound is $\lceil 2 + 2\sqrt{5} \rceil = 7$ for T empty and only $\lceil 2 + 2\sqrt{4} \rceil = 6$ for a non-empty set T consisting of odd primes.

THEOREM 4. (Genus Theory). *Suppose K/k is a Galois extension of degree ℓ. Suppose t places of k ramify in K. Then $\rho_K \geqslant t - 1 - \dim_{\mathbb{F}_\ell} E_k/E_k^\ell$.*

Proof. See any one of the following: [Ma1], [J], [CR], or [S].   □

The next result gives a bound for the root discriminant of number fields contained in a tamely ramified tower.

LEMMA 5. *Suppose T is a finite set of prime ideals of a number field K away from ℓ. Suppose $F \subset K_T$ is a finite ℓ-extension of K unramified outside T. Put $m = [F : K]$ and $\mu = \prod_{\mathcal{P} \in T} \mathbb{N}_{F/\mathbb{Q}}(\mathcal{P})^{1/[K:\mathbb{Q}]}$. Then, $rd_F \leqslant \mu^{1-1/m} \cdot rd_K$, with equality if and only if every $\mathcal{P} \in T$ is totally ramified in F. We have the uniform estimate $rd_F \leqslant \mu \cdot rd_K$.*

Proof. The extension F/K is tamely ramified by assumption. Thus, for each prime ideal $\mathcal{P}$ of K, the $\mathcal{P}$-valuation of the norm in F/K of the different $\mathfrak{D}_{F/K}$ is $m(1 - 1/e_\mathcal{P})$, where $e_\mathcal{P}$ is the ramification index of $\mathcal{P}$ in F/K (e.g. [W, Thm. 3-7-23]). Note that, for each $\mathcal{P}$, $e_\mathcal{P}$ is: a divisor of m, equal to m if and only if $\mathcal{P}$ is totally ramified in F/K, and 1 if $\mathcal{P} \notin T$. Now the discriminant formula $|d_F| = |d_K^m \mathbb{N}_{K/\mathbb{Q}}(\mathfrak{D}_{F/K})|$ (e.g. [W, Prop. 4-8-12]), completes the proof.   □

Given the above calculation, it seems natural to define the following generalization of the root discriminant.

DEFINITION 6. For a number field K and a finite set T of prime ideals of K away from l, define the T-root discriminant of K to be

$$rd_{K,T} = rd_K \prod_{\mathcal{P} \in T} \mathbb{N}_{K/\mathbb{Q}}(\mathcal{P})^{1/[K:\mathbb{Q}]}.$$

Thus, if T is away from ℓ and $F \subset K_T$, then $rd_F \leqslant rd_{K,T}$.

We close this section with a simple consequence of the above Lemma.

PROPOSITION 7. (i) *Let K be a number field. Then for all primes ℓ there exists an infinite ℓ-extension L/K unramified at infinite places of K such that the root discriminant of all number fields contained in L remains bounded.*

(ii) *For each $t \in \mathbb{Q} \cap [0, 1]$, $\alpha(t) < \infty$.*

Proof. By the Cebotarev Density Theorem, there exist infinitely many prime ideals of K with absolute norm congruent to 1 modulo ℓ. If T consists of such prime ideals only, then there is a constant c depending on K but not on T such that $\rho_{K,T} \geqslant |T| - c$ (for example, see [Sh] or, consider composing K with absolutely cyclic degree ℓ extensions ramified at many finite places, and use class field theory). Thus, for all such T of large enough cardinality, $\rho_{K,T}$ surpasses the Golod–Shafarevich bound, giving an infinite T-tamely ramified ℓ-tower K_T/K. By Lemma 5, the root discriminant of subfields of K_T is bounded by $rd_{K,T}$. Note that the infinite places of K are not ramified in K_T, hence all subfields of K_T containing K have the same infinity type as K. Given a rational t in the unit interval and a number field K of infinity type t. We apply part (i) to this K with an appropriate T to obtain $\alpha(t) \leqslant rd_{K,T} < \infty$. $\qquad \square$

Remark. The standard way to show that $\alpha(t) < \infty$ is to take K of infinity type t and compose it with an absolutely cyclic degree ℓ extension in which many primes of $\mathbb{Q}$ (excluding infinity) ramify. The resulting number field has the same infinity type as K and an infinite Hilbert class field tower, thanks to genus theory and the Golod–Shafarevich criterion.

3. Examples of Infinite Towers with Small Root Discriminant

Throughout this section, we let $\ell = 2$. We construct some infinite unramified and tamely ramified 2-towers with root discriminant below 100.

3.1. UNRAMIFIED TOWERS

We first give some examples of Martinet type.

EXAMPLE 1. Let k_0 be the first step in the cyclotomic $\mathbb{Z}_5$-extension of $\mathbb{Q}$, a totally real field of degree 5 and discriminant 5^8. A defining polynomial for it is $x^5 + 5x^4 - 15x^2 - 5x + 7$. Consider $k = k_0(\sqrt{2})$, in which 7 splits completely, and

take $K = k(\sqrt{-7})$. In K/k, ten finite and ten infinite places ramify. By Theorem 4, $\rho_K \geqslant 9$, which implies by Theorem 3 that K has infinite unramified 2-tower. By Lemma 5, the root discriminant of K is $2^{3/2}5^{8/5}7^{1/2} = 98.275\cdots$.

EXAMPLE 2. This time, we start with the degree 9 totally real field $k = \mathbb{Q}(\cos(2\pi/19))$ in which 37 splits completely, and consider the CM extension $K = k(\sqrt{-19 \cdot 37})$. In K/k, there are ten finite and nine infinite ramifying places, hence $\rho_K \geqslant 9$. By the Golod–Shafarevich criterion, K admits an infinite unramified 2-extension; note that every field in the tower is unramified outside $\{19, 37, \infty\}$. By Lemma 5, the root discriminant of K is $19^{17/18}37^{1/2} = 98.132\cdots$.

EXAMPLES 3 and 4. ([Ma2], unpublished). The biquadratic fields

$$\mathbb{Q}(\sqrt{-263}, \sqrt{-35}), \qquad \mathbb{Q}(\sqrt{-607}, \sqrt{-15})$$

admit infinite unramified extensions. A genus theory estimate more refined than Theorem 4 is applied in $k_1(\sqrt{-35})/k_1$ and $k_2(\sqrt{-15})/k_2$ where k_1, k_2 are the Hilbert class fields of $\mathbb{Q}(\sqrt{-263})$, $\mathbb{Q}(\sqrt{-607})$, respectively. Since the details are interesting but lengthy, we give them in an appendix. The root discriminants are respectively, $95.942\cdots$, $95.420\cdots$.

EXAMPLE 5 ([Ma1]). We let $k = \mathbb{Q}(\cos(2\pi/11), \sqrt{2})$, a totally real field of degree 10 in which 23 splits completely. In the CM extension $K = k(\sqrt{-23})/k$, there are ten finite and ten infinite ramifying primes. Just as in Example 1, genus theory and Golod–Shafarevich together show that K has an infinite unramified 2-tower. The root discriminant is $11^{4/5}2^{3/2}23^{1/2} = 92.368\cdots$ all the way up the tower. No number field of smaller root discriminant has been shown to admit an infinite unramified extension.

3.2. TAMELY RAMIFIED TOWERS

We now use tamely ramified towers to improve Martinet's estimate $\alpha_0 \leqslant 92.368\cdots$ to $\alpha_0 \leqslant 83.885\cdots$. We first describe the general scheme. Taking the Remark following Theorem 3 to heart, we begin with a degree 4 field k and consider a totally complex quadratic extension K of it. In the first type of example (labeled $A\bullet$), four infinite and seven finite places of k are ramified in K, so $\rho_K \geqslant 6$. We then take T to consist of a single odd prime of K and find the T-ramified 2-tower of K to be infinite. In the second type (labeled $B\bullet$), four infinite and six finite places of k are ramified in K; by Theorem 4, $\rho_K \geqslant 5$. We then take a set T of primes of K such that $\rho_{K,T} \geqslant 6$, ensuring that K has an infinite T-ramified 2-tower. Finally, for the third type (labeled $C\bullet$), the quartic field we take at the outset has signature $(2, 1)$; both real infinite places as well as seven finite places of k ramify in K, giving $\rho_K \geqslant 5$. We then take a set T of primes of K such that $\rho_{K,T} \geqslant 6$, and again find

that K has an infinite T-ramified 2-tower. In all the examples presented here, 2 is unramified in $K/\mathbb{Q}$.

To verify our examples, one needs to check that the different of K/k is indeed what we claim it is and that this ideal has the stated number of prime factors. A computer program such as Pari is ideal for this task. Additionally, in each case, we give a defining polynomial for the field K of degree 8; thus, using Pari, one may calculate, in a matter of seconds, the root discriminant and the structure of the appropriate ray class group.

At the same time, we would like to present the examples in such a way that a reader armed with an ordinary hand-held calculator can easily check the validity of the construction. Since calculations in number fields of degree greater than two quickly become laborious — we are essentially doing quadratic Kummer theory in quartic number fields — we provide (at the cost of lengthening the presentation) much supplementary data and a method for verifying each step in the reasoning. We also provide some data (such as Galois group, class number, generators for the unit group) whose validity need not be verified but which would aid the reader who wishes to check our claims independently. For each example, the two calculations which need to be verified are the 2-rank of the ray class group and the root discriminant of K.

The path we provide for verification of these examples is as follows. We wish to do arithmetic in a number field k of degree 4. We give a monic integral defining polynomial f for k and approximate roots $\xi^{(j)}$, $j = 1, 2, 3, 4$, accurate to 25 decimal places (which more than suffices!). The reader may begin by plugging in the given values to see that they are indeed good approximations to the roots of f. Since we are working with algebraic *integers*, if an integral algebraic expression in ξ (an abstract root of f) is 0 (to sufficient accuracy) when one plugs in each of the four roots, then one has a proof that the expression is exactly 0. For example, suppose we say the discriminant of $f = x^4 - x^3 - 4x^2 + 2x + 1$ is 3981. If, by plugging in the four roots provided into $\prod_{i<j}(\xi^{(i)} - \xi^{(j)})^2$, one finds the value $3981.000\cdots$, then the discriminant must indeed be 3981 (by continuity, since one knows that the discriminant is an *integer*). As another example, if we claim that, for a root ξ of f, the minimal polynomial of $h(\xi) = \xi^3 - \xi^2 - 5\xi + 1$ is $x^4 - 3x^3 - 11x^2 - 21x + 37$, then this can be verified by checking that the latter polynomial vanishes, to the given accuracy, on the four numbers $h(\xi^{(j)})$, $j = 1, 2, 3, 4$, because we know that the minimal polynomial of $h(\xi)$ has integer coefficients. This is one way to show that $(h(\xi))$ is a prime ideal of absolute norm 37. Another way (which involves no approximations, and is pleasant for a reader who enjoys taking determinants) would be to calculate the absolute value of the resultant of h and f. Of course, a reader with access to Pari can verify our claims by using its resources for working in algebraic number fields.

We discuss in detail the best examples of each type that we have been able to find, and present six further examples in Table 1 at the end of this section. Each of these nine examples gives a root discriminant lower than that of Martinet's tower

(Example 5, Section 3.1). The notation of the table follows exactly the notation in the detailed examples.

EXAMPLE A1. Let $k = \mathbb{Q}(\xi)$ where ξ is a root of $f = x^4 - x^3 - 4x^2 + 2x + 1$. The discriminant of f is $3981 = 3 \cdot 1327$; thus, this is also the discriminant of k, and $\mathcal{O}_k = \mathbb{Z}[\xi]$. The roots of f are

$$\xi^{(1)} = -1.75080042206091586958004 0466 \cdots$$

$$\xi^{(2)} = -0.31845889657472074084575 93350 \cdots$$

$$\xi^{(3)} = 0.78526144849356535849285 16638 \cdots$$

$$\xi^{(4)} = 2.28399787014207125193294 8137 \cdots.$$

Thus, k is a totally real field. Since d_k is a quadratic discriminant, it follows (see [Ko]) that the Galois group of f is S_4 (the Galois closure of k is an unramified A_4-extension of $\mathbb{Q}(\sqrt{3981})$). The narrow class number of k is 1. The unit group of k is generated by $\{\xi, \xi - 1, \xi^2 + \xi - 1, -1\}$.

Generators for some $\mathcal{O}_k$-ideals of small norm are listed in the table below; here, $\pi_r = a_3\xi^3 + a_2\xi^2 + a_1\xi + a_0$ generates a prime ideal $\pi_r\mathcal{O}_k$ of norm r. We also give h_{π_r}, the minimal polynomial of π_r so that the reader can verify, by the method discussed above, that each of the algebraic integers listed has the claimed norm. (Instead of writing out the polynomial in full, we give a list of its coefficients in order of descending powers of x. For example the coefficient list $1, 2, 3, 4, 5$ represents the polynomial $x^4 + 2x^3 + 3x^2 + 4x + 5$).

π_r	a_3, a_2, a_1, a_0	h_{π_r}
π_3	$0, 1, 1, 0$	$1, -10, 20, -9, -3$
π_5	$1, -1, -3, 1$	$1, 1, -5, -3, 5$
π_9	$0, 1, 0, -2$	$1, -1, -8, 0, 9$
π_{13}	$1, -1, -4, 0$	$1, 6, 8, -7, -13$
π_{23}	$2, -2, -7, 2$	$1, 3, -14, -48, -23$
π_{37}	$-3, 2, 9, -6$	$1, 18, 67, -114, 37$
π_{41}	$1, 0, -5, 1$	$1, -6, 1, 36, -41$

Note that $3\mathcal{O}_K$ has two prime factors of residue degree 1 and 2, as can be seen, for instance, from the factorization of f over $\mathbb{F}_3$: $f(x) \equiv (x^2 + 1)(x + 1)^2 \bmod 3$. To see that π_3 and π_9 generate different prime ideals, note, for example, that $\pi_3(-\xi^3 + \xi^2 + 4\xi - 2) = (\xi + 1)$ and $\pi_9(\xi^2 - \xi - 1) = \xi^2 + 1$. Alternatively, one can check that the minimal polynomial of π_3^2/π_9 is not integral, hence π_3^2 and π_9 are not associates.

The element $\eta = -29\xi^3 - 23\xi^2 + 25\xi - 65 \in \mathcal{O}_k$ is totally negative. Its minimal polynomial is $g(y) = y^4 + 645y^3 + 90201y^2 + 4375521y + 61233705$. The $\mathcal{O}_k$-ideal it generates factors into seven prime ideals of $\mathcal{O}_k$; in fact, one can check that $\eta = \pi_3\pi_5\pi_9\pi_{13}\pi_{23}\pi_{37}\pi_{41}$. We let $K = k(\sqrt{\eta})$, a totally complex field of degree 8. A defining polynomial for K is $g(y^2)$. We note that η is congruent to a square modulo

$4\mathcal{O}_K$; explicitly, $\eta = \beta^2 - 4\gamma$ with $\beta = \xi^3$ and $\gamma = 9\xi^3 + 10\xi^2 - 9\xi + 15$. Thus, K/k is ramified at the infinite places and at the seven primes dividing η and nowhere else. By Lemma 5, the root discriminant of K is $rd_K = 3981^{1/4}(3 \cdot 5 \cdot 9 \cdot 13 \cdot 23 \cdot 37 \cdot 41)^{1/8} = 74.708\cdots$. By Theorem 4, the 2-rank of the ideal class group of K is at least 6. (This is confirmed by a Pari calculation, which finds that $\mathrm{Cl}(K) = (22, 2, 2, 2, 2, 2)$.) Since $\pi_3\mathcal{O}_k$ ramifies in K, $\mathcal{O}_K$ has an ideal $\mathfrak{P}_3$ of absolute norm 3; we let $T = \{\mathfrak{P}_3\}$. (Incidentally, $\mathrm{Cl}_T(K) = \mathrm{Cl}(K)$, according to a Pari calculation). By Theorem 3, K admits an infinite T-tamely ramified 2-tower. By Lemma 5, the root discriminant of the fields in this tower are bounded by $rd_{K,T} = rd_K 3^{1/8} = 85.706\cdots$.

EXAMPLE B1. Let $k = \mathbb{Q}(\xi)$ where ξ is a root of $f = x^4 - 2x^3 - 4x^2 + 3x + 3$. The discriminant of f (hence also that of k) is $7053 = 3 \cdot 2351$; we have $\mathcal{O}_k = \mathbb{Z}[\xi]$. The roots of f are

$$\xi^{(1)} = -1.36360863740202443352905825\ 0\cdots$$
$$\xi^{(2)} = -0.66942604022407781354949966\ 76\cdots$$
$$\xi^{(3)} = 1.13341035061593398846461718\ 2\cdots$$
$$\xi^{(4)} = 2.89962432701016825861394073\ 5\cdots.$$

Again, k is totally real. The Galois group of f is S_4 (the Galois closure of k is an unramified A_4-extension of $\mathbb{Q}(\sqrt{7053})$). The narrow class number of k is 1. The unit group of k is generated by $\{\xi + 1, \xi - 1, \xi^2 - 2\xi - 2, -1\}$.

Generators for some $\mathcal{O}_k$-ideals of small norm are listed in Table I, with the same notation as in Example A1.

Note that $3\mathcal{O}_K$ has two prime factors of residue degree 1 and 2, as can be seen, for instance, from the factorization $f(x) \equiv x^2(x^2 + x - 1) \bmod 3$. We can verify that π_3 and π_9 generate different prime ideals of norm 3 and 9, respectively, by noting that $\pi_3(\xi^3 - 2\xi^2 - 3\xi + 1) = \xi$ and $\pi_9(\xi + 1) = \xi^2 + \xi - 1$. Similarly, $f(x) \equiv (x + 7)(x + 2)(x^2 + 2x + 3) \bmod 13$ and $\pi_{13}(3\xi^3 - 7\xi^2 - 6\xi + 4) = \xi + 7$, $\pi'_{13}(\xi + 1) = \xi + 2$ collectively imply that π_{13}, π'_{13} generate different prime ideals of norm 13. Alternatively, one can check that π_3^2/π_9 and π_{13}/π'_{13} are not algebraic integers.

Table I

π_r	a_3, a_2, a_1, a_0	h_{π_r}
π_3	$-1, 0, 1, 0$	$1, 21, -11, -15, -3$
π_7	$-1, 2, 3, 1$	$1, -11, 38, -44, 7$
π_9	$-1, 3, 2, -4$	$1, -1, -11, 21, -9$
π_{13}	$1, -1, -2, 1$	$1, -11, -4, 22, 13$
π'_{13}	$1, -3, -1, 5$	$1, -5, 1, 15, -13$
π_{17}	$1, -2, -2, 2$	$1, -3, -7, 11, 17$
π_{31}	$1, -2, -4, 2$	$1, 1, -15, -11, 31$

The element $\eta = -25\xi^3 - 8\xi^2 + 30\xi - 17 \in \mathcal{O}_k$ is totally negative. Its minimal polynomial is $g(y) = y^4 + 679y^3 + 45406y^2 + 964704y + 5610969$. The $\mathcal{O}_k$-ideal it generates factors into six prime ideals of $\mathcal{O}_k$; in fact, one can check that $\eta = \pi_7\pi_9\pi_{13}\pi'_{13}\pi_{17}\pi_{31}$. We let $K = k(\sqrt{\eta})$, a totally complex field of degree 8. A defining polynomial for K is $g(y^2)$. Since $\eta = \beta^2 - 4\gamma$ with $\beta = \xi^3 + \xi + 1$ and $\gamma = 13\xi^3 + 10\xi^2 - 16\xi - 3$, K/k is ramified at the infinite places and at the six primes dividing η but nowhere else. By Lemma 5, the root discriminant of K is $rd_K = 7053^{1/4}(9 \cdot 7 \cdot 13^2 \cdot 17 \cdot 31)^{1/8} = 63.93\cdots$. By Theorem 4, the 2-rank of the ideal class group of K is at least 5. In K, the ideal $\pi_3\mathcal{O}_K$ has absolute norm 9. We let T be the set of primes of K dividing $\pi_3\mathcal{O}_K$. (It is not needed, but one can check that $|T| = 2$). We note that $\pi_3 = (\xi^3 + \xi^2 + \xi + 1)^2 - 4(12\xi^3 + 12\xi^2 - 14\xi - 11)$, so that $k(\sqrt{\pi_3})/k$ is ramified at (π_3) and at no other finite place. Since (π_3) is *unramified* in K/k, it follows that $K(\sqrt{\pi_3})$ is a *ramified* quadratic extension of K ramified at T and nowhere else. Thus, by class field theory, the 2-rank of the ray class group of K modulo $\pi_3\mathcal{O}_K$, is at least 6. (This is confirmed by a Pari calculation, which finds that $\mathrm{Cl}(K) = (28, 2, 2, 2, 2)$ and $\mathrm{Cl}_T(K) = (28, 2, 2, 2, 2, 2)$.) By Theorem 3, K admits an infinite T-tamely ramified 2-tower. By Lemma 5, the root discriminants of the fields in this tower are bounded by $rd_{K,T} = rd_K 9^{1/8} = 84.140\cdots$.

EXAMPLE C1. Let $k = \mathbb{Q}(\xi)$ where ξ is a root of $f = x^4 - x^3 + x^2 + x - 1$. The discriminant of f (hence also that of k) is -331 and $\mathcal{O}_k = \mathbb{Z}[\xi]$. Since the discriminant is negative, the signature of k must be $(2, 1)$. Indeed, the roots of f are

$$\xi^{(1)} = -0.848374895731953217105620467 7\cdots$$
$$\xi^{(2)} = 0.6609925318901199786139741268\cdots$$
$$\xi^{(3)} = 0.59369118192091661924582317 04 +$$
$$\quad + 1.196158336070944997927456045i\cdots$$
$$\xi^{(4)} = 0.59369118192091661924582317 04 -$$
$$\quad - 1.196158336070944997927456045i\cdots.$$

The Galois group of f is S_4; the Galois closure of k is an unramified A_4-extension of $\mathbb{Q}(\sqrt{-331})$ – it gives rise to a 2-dimensional octahedral Galois representation of small prime conductor. The narrow class number of k is 1. The unit group of k is generated by $\{\xi, \xi^3 - \xi^2 + \xi, -1\}$.

Generators for some $\mathcal{O}_k$-ideals of small norm are listed in Table II. The notation is as in the previous examples.

To confirm that these numbers all give rise to different prime ideals, it is enough to observe the following facts: $f(x) \equiv (x - 2)(x - 3)(x^2 + 4x + 2) \bmod 13$, $\xi - 3 = \pi_{13}(-\xi^2 - 1)$, $\xi - 2 = \pi'_{13}(\xi^2 - \xi + 1)$, and $f(x) \equiv (x - 5)(x + 6)(x^2 - 2x + 10) \bmod 23$, $\xi + 6 = \pi_{23}(\xi^3 - \xi^2 + 3\xi + 2)$, $\xi - 5 = \pi'_{23}(-3\xi^3 + 4\xi^2 - 5\xi + 1)$.

The element $\eta = -127\xi^3 - 139\xi^2 - 181\xi - 146 \in \mathcal{O}_k$ is totally negative. Its minimal polynomial is $g(y) = y^4 - 9y^3 + 24182y^2 + 60281988y + 895172213$. The $\mathcal{O}_k$-

Table II

π_r	a_3, a_2, a_1, a_0	h_{π_r}
π_5	$0, -1, 0, -1$	$1, 3, 4, 6, 5$
π_{13}	$1, 0, -1, 2$	$1, -2, 0, -7, 13$
π'_{13}	$-1, -1, 0, -1$	$1, -2, -5, 10, 13$
π_{17}	$1, 1, 0, 2$	$1, -2, -5, 2, 17$
π_{19}	$1, 0, 2, 0$	$1, 3, 3, -5, -19$
π_{23}	$1, -2, 2, 1$	$1, -3, -4, 24, -23$
π'_{23}	$1, 1, 2, 1$	$1, 0, 5, -36, -23$
π_{31}	$2, 0, 3, 3$	$1, -5, 4, -34, -31$

ideal it generates factors into seven prime ideals of $\mathcal{O}_k$; in fact, one can check that $\eta = \pi_{13}\pi'_{13}\pi_{17}\pi_{19}\pi_{23}\pi'_{23}\pi_{31}$. We let $K = k(\sqrt{\eta})$, a totally complex field of degree 8. A defining polynomial for K is $g(y^2)$. We find $\eta = \beta^2 - 4\gamma$ with $\beta = \xi^2 + 1$ and $\gamma = 32\xi^3 + 35\xi^2 + 45\xi + 37$. Thus, K/k is ramified at the two real infinite places and at the seven primes dividing η and nowhere else. By Lemma 5, the root discriminant of K is $rd_K = 331^{1/4}(13^2 \cdot 17 \cdot 19 \cdot 23^2 \cdot 31)^{1/8} = 56.097\cdots$. By Theorem 4, the 2-rank of the ideal class group of K is at least 5. In K, the ideal $\pi_5\mathcal{O}_K$ has absolute norm 25. We let T be the set of primes of K dividing $\pi_5\mathcal{O}_K$. (It is not needed, but one can check that $|T| = 2$). Now, the ray class group of k mod (π_5) is trivial, but K admits a quadratic extension ramified at $\pi_5\mathcal{O}_K$ and nowhere else. To verify the latter claim, it is enough to observe that $\pi_5\pi_{13} = \xi - 3 = (\xi^3 + 1)^2 - 4$, so that $k(\sqrt{\pi_5\pi_{13}})/k$ is ramified at (π_5) and at (π_{13}) but at no other finite place. Since K/k is ramified at (π_{13}) and unramified at (π_5), it follows that $K(\sqrt{\pi_5\pi_{13}})$ is a ramified quadratic extension of K contained in its ray class field modulo $\pi_5\mathcal{O}_K$. By class field theory, then, the 2-rank of the ray class group of K modulo $\pi_5\mathcal{O}_K$, which equals $\rho_{K,T}$, is at least 6. (This is confirmed by a Pari calculation, which finds that $\mathrm{Cl}(K) = (12, 2, 2, 2, 2)$ and $\mathrm{Cl}_T(K) = (12, 2, 2, 2, 2, 2)$). By Theorem 3, K admits an infinite T-tamely ramified 2-tower. By Lemma 5, the root discriminant of the fields in this tower are bounded by $rd_{K,T} = rd_K 25^{1/8} = 83.885\cdots$. This gives $\alpha_0 \leqslant 5^{1/4}13^{1/4}17^{1/8}19^{1/8}23^{1/4}31^{1/8} 331^{1/4} = 83.885\cdots$, as promised in the introduction.

To fulfill another promise made there, we now describe how our examples lead to families with small Ihara–Tsfasman–Vladut deficiency δ. We recall its definition [TV]. If F is any number field, let $(r_1(F), r_2(F))$ be its signature, and let $N_q(F)$ be the number of places of F of absolute norm q. For a family $\mathcal{K} = \{K_j\}$ of number fields, consider the quantities

$$\phi_{\mathbb{R}} = \lim_j \frac{2r_1(K_j)}{\log|d_{K_j}|}, \qquad \phi_{\mathbb{C}} = \lim_j \frac{2r_2(K_j)}{\log|d_{K_j}|}, \qquad \phi(q) = \lim_j \frac{2N_q(K_j)}{\log|d_{K_j}|}.$$

Note that

$$\phi_{\mathbb{R}} = \lim_j \frac{2\tau(K_j)}{\log rd_{K_j}}, \qquad \phi_{\mathbb{C}} = \lim_j \frac{1 - \tau(K_j)}{\log rd_{K_j}}.$$

The family $\mathcal{K}$ is said to be *asymptotically exact* if these limits exist. For a nested family $\mathcal{K} = \{K_j\}$, $K_0 \subset K_1 \subset K_2 \subset \cdots$, $\tau(K_j)$ is non-increasing and rd_{K_j} is non-decreasing, so $\phi_{\mathbb{R}}$ and $\phi_{\mathbb{C}}$ exist. A similar argument shows that $\phi(q)$ exists in this case, so a nested family is always asymptotically exact ([TV], Lemma 2.3). Define the deficiency $\delta_{\mathcal{K}}$ of an asymptotically exact family $\mathcal{K}$ to be

$$\delta_{\mathcal{K}} = 1 - \sum_q \frac{\phi(q)\log q}{\sqrt{q}-1} - \phi_{\mathbb{R}}\left(\log\sqrt{8\pi} + \frac{\pi}{4} + \frac{\gamma}{2}\right) - \phi_{\mathbb{C}}(\log 8\pi + \gamma).$$

Here, $\gamma = 0.577\cdots$ is Euler's constant, and the sum is over all rational prime powers q.

On GRH, we have, for any family $\mathcal{K}$, $\delta_{\mathcal{K}} \geqslant 0$ ([TV, GRH Theorem 3.1]). For a nested family, this represents a refinement of the inequality (1), thanks to the term involving the norms of almost completely split primes in the tower. We would like to know how small $\delta_{\mathcal{K}}$ can be. In [TV], it is shown that if $\mathcal{K} = \{K_j\}$ is any nested family of fields contained in the Hilbert class field tower of Martinet's best example (our Example 5 in Section 3.1 above), then $\delta_{\mathcal{K}} \leqslant 0.160\cdots$. This has remained the smallest known deficiency for some time. (Yamamura's examples in [Y1] are not valid; see the author's forthcoming Correction as well as [TV, Section 6.2]). By Lemma 5, we find for any nested family $\mathcal{K}$ of subfields of the infinite tower K_T/K of our example C1 that

$$\delta_{\mathcal{K}} \leqslant 1 - \frac{\gamma + \log(8\pi)}{\log(rd_{K,T})} = 0.141\cdots.$$

It is conceivable that some nested family $\mathcal{K}$ of subfields of K_T/K satisfies either $\phi(q) > 0$ for some small q or $\lim_j rd_{K_j} < rd_{K,T}$, conditions which would give improved deficiencies, but these would appear to be difficult to establish. While the first condition is a possibility also for Hilbert class field towers, the second one is a potentially fruitful new feature of the use of tame towers for bounding α_t and for finding small deficiencies. The Question of the next section is related to this.

Finally, we leave to the reader the verification of the asymptotic packing density for this tower, which was given in the introduction.

We present examples A1, B1, C1 and six others, sorted according to increasing $rd_{K,T}$ in Table III. The notation is exactly as in the above examples.

4. A Question

We close by posing a natural question:

Question. Does every infinite tamely ramified ℓ-extension contain a number field (of finite degree) admitting an infinite *unramified* ℓ-extension?

Table III

name	f	d_k	rd_K
g	η	T	$rd_{K,T}$
C1	$1, -1, 1, 1, -1$	-331	$56.097\cdots$
$1, -9, 24182, 60281988, 895172213$	$-127, -139, -181, -146$	$\{\mathfrak{P}_5, \mathfrak{P}'_5\}$	$83.885\cdots$
B1	$1, -2, -4, 3, 3$	$3 \cdot 2351$	$63.932\cdots$
$1, 679, 45406, 964704, 5610969$	$-25, -8, 30, -17$	$\{\mathfrak{P}_3, \mathfrak{P}'_3\}$	$84.140\cdots$
C2	$1, -1, -1, 3, 1$	$-7 \cdot 293$	$64.682\cdots$
$1, 392, 55986, 3415104, 728377653$	$-16, 36, -8, -143$	$\{\mathfrak{P}_3, \mathfrak{P}'_3\}$	$85.126\cdots$
A1	$1, -1, -4, 2, 1$	$3 \cdot 1327$	$74.708\cdots$
$1, 645, 90201, 4375521, 61233705$	$-29, -23, 25, -65$	$\{\mathfrak{P}_3\}$	$85.706\cdots$
B2	$1, -2, -4, 5, 5$	$5^2 \cdot 101$	$58.274\cdots$
$1, 953, 133401, 5013085, 20861005$	$143, -71, -578, -344$	$\{\mathfrak{P}_5, \mathfrak{P}'_5\}$	$87.141\cdots$
B3	$1, -2, -4, 3, 3$	$3 \cdot 2351$	$66.481\cdots$
$1, 307, 30262, 1041840, 7671573$	$21, -70, -13, 19$	$\{\mathfrak{P}_3, \mathfrak{P}'_3\}$	$87.495\cdots$
C3	$1, -1, -1, 3, -3$	$-3 \cdot 953$	$66.976\cdots$
$1, 220, 10342, 818844, 49539105$	$-24, -16, 88, -95$	$\{\mathfrak{P}_3, \mathfrak{P}'_3\}$	$88.145\cdots$
B4	$1, -1, -5, 1, 1$	$13^2 \cdot 53$	$67.133\cdots$
$1, 221, 17277, 542997, 5142501$	$4, 1, -12, -68$	$\{\mathfrak{P}_3, \mathfrak{P}'_3\}$	$88.352\cdots$
A2	$1, -1, -7, 3, 9$	$5^2 \cdot 181$	$75.001\cdots$
$1, 810, 91575, 3651750, 48901725$	$39, -123, -24, 138$	$\{\mathfrak{P}_5\}$	$91.715\cdots$

It is easy to construct examples of number fields having: (a) finite Hilbert class field tower; (b) an infinite tamely ramified ray class field tower; (c) an extension of small degree in the ray class field tower which passes the Golod–Shafarevich test (for infinitude of its Hilbert class field tower). In [HM], we investigate this question and other conjectural links between tamely ramified and unramified class field towers, along lines suggested by the Fontaine–Mazur conjecture [FM].

The importance of the question for the estimation of α_t is clear. Thus, in all the infinite ramified towers constructed here, there is the potential of finding a number field admitting an infinite unramified extension; this would lower the upper estimate for α_0 by a possibly substantial amount. For instance, consider Example C1 once more. The field K has root discriminant approximately 56. It already admits an unramified extension of degree 2^6 (its 2-Hilbert class field). A 2-extension where the ramifying primes $\mathfrak{P}_5, \mathfrak{P}'_5$ both have ramification index $e = 1, 2, 4, 8, 16, \ldots$ would have root discriminant approximately $56, 69, 76, 80, 82, \ldots$, respectively.

One interpretation of the significance of the above question is as follows. The difficulty in finding good upper estimates for α_t is that it is difficult to access number fields of large degree. A positive answer to Question 1 would be saying, in effect, that a good place to look for number fields of small root discriminant admitting infinite *Hilbert* class field towers is inside (the first few stages of) infinite *ray* class field towers.

Appendix

Here we give a proof for the claims made in Examples 3 and 4 of Section 3.1. All of the arguments presented in this appendix are based on [Ma2] and are due to Martinet. We thank him for allowing us to include them here.

We will need a refinement of the genus theory estimate of Theorem 4.

PROPOSITION 8. *Suppose K/k is a Galois extension of degree ℓ, and let t be the number of places of k ramified in K. Then, $\rho_K \geqslant t - 1 - \dim_{\mathbb{F}_\ell}(E_k/E_k \cap \mathbb{N}_{K/k}U_K)$, where U_K is the group of idele units of K.*

Proof. A proof can be found, for example, in Schoof [S].   □

Note that the calculation of $E_k/E_k \cap \mathbb{N}_{K/k}U_K$ reduces to local considerations. The following Proposition, which is a variation on a construction of Schoof [S], will illustrate this point.

PROPOSITION 9. *Let F_1 be an imaginary quadratic field with class number $h \geqslant 13$. Suppose F_2 is another quadratic field such that two primes p_1, p_2 which ramify in F_2 are inert in F_1. Then, the biquadratic field $F = F_1F_2$ has infinite Hilbert class field tower.*

Proof. Let $\ell = 2$. Let k be the Hilbert class field of F_1 and put $K = kF_2$. It is clear that K is contained in the Hilbert class field of F, so it suffices to show that K has an infinite 2-class field tower. Since p_1, p_2 are inert (hence principal) in F_1, each of them splits into h primes in k, which then all ramify in K/k. Thus, for the number t of ramified primes in K/k, we have $t \geqslant 2h$. For $h \geqslant 14$, the crude estimate of Theorem 4 suffices, in conjunction with Theorem 3, to show that K has an infinite 2-class field tower. We therefore assume that $h = 13$, which implies, by classical genus theory, that $|d_{F_1}|$ is and odd prime. By replacing F_2 with a third quadratic subfield of F, if necessary, we may assume that d_{F_1} and d_{F_2} are relatively prime. If some prime other than p_1, p_2 is ramified in $F_2/\mathbb{Q}$, then $t \geqslant 2h + 1 = 27$ and again Theorem 4 together with Theorem 3 suffices. So now we have arrived at the interesting case where the only prime divisors of d_{F_2} are p_1 and p_2.

We claim that $-1 \in \mathbb{N}_{K/k}U_K$. To do this, it is sufficient to show that -1 is a norm in F/F_1. There one only has to look at the two prime ideals (p_1) and (p_2) of F_1, and by the product formula it is sufficient to look at only one of them. In particular, we may assume without loss of generality that p_1 is odd. It is enough to show that -1 is a square in the completion of F_1 at (p_1). Since p_1 is odd, Hensel's Lemma reduces this to checking that -1 is a square in the residue field $\mathcal{O}_{F_1}/(p_1)$, but this is clear since this residue field is $\mathbb{F}_{p_1^2}$, thus the claim is proved. Since $d_k = d_{F_1}^{13}$ is odd, -1 is not a square in k. Consequently, $d(E_k/E_k \cap \mathbb{N}_{K/k}U_K) \leqslant 12$. We now apply Proposition 8, with $\ell = 2$, to find

$$\rho_K \geqslant 26 - 1 - d(E_k/E_k \cap \mathbb{N}_{K/k}U_K) \geqslant 13 > 2 + 2\sqrt{27},$$

so we are done by Theorem 3.   □

EXAMPLES. If we take $F_1 = \mathbb{Q}(\sqrt{-263})$, $F_2 = \mathbb{Q}(\sqrt{-35})$ or $F_1 = \mathbb{Q}(\sqrt{-607})$, $F_2 = \mathbb{Q}(\sqrt{-15})$, the hypotheses of Proposition 9 are satisfied (with $h = 13$), verifying the claims made in Examples 3 and 4 of Section 3.1. Note, as an interesting consequence, that the real quadratic fields $L_1 = \mathbb{Q}(\sqrt{9205})$, and $L_2 = \mathbb{Q}(\sqrt{9105})$ admit infinite unramified-outside-infinity extensions, but, on GRH, their maximal everywhere unramified extension is of finite degree. Unconditionally, their Hilbert class field towers stop at $L_j(\sqrt{5})$, since it is easy to show that these fields have class number 1.

Acknowledgements

References

[ABC]   Ankeny, N.C., Brauer, R. and Chowla, S.: A note on the class numbers of algebraic number fields, *Amer. J. Math.* **78** (1956), 51–61.

[AM]   Angles, B. and Maire, C.: A note on tamely ramified towers of global function fields, Preprint, 1999.

[B]   Batut, C., Belabas, K., Bernardi, D., Cohen, H. and Olivier, M.: GP/PARI 2.0.7, ftp://megrez.math.u-bordeaux.fr/pub/pari.

[CR]   Cornell, G. and Rosen, M.: A cohomological investigation of the class Group extension problem, In: P. Ribenboim (ed.), *Proc. Queen's Number Theory Conference*, Queen's Papers in Pure and Appl. Math. 54, Queen's University Press, 1980, pp. 287–308.

[CS]   Conway, J. and Sloane, N.: *Sphere Packings, Lattices and Groups*, Springer, New York, 1988.

[F]   Fontaine, J.-M.: Il n'y a pas de variété abelienne sur $\mathbb{Z}$, *Invent. Math.* **81** (1985), 515–538.

[FM]   Fontaine, J.-M. and Mazur, B.: Geometric Galois representations, In: *Elliptic Curves, Modular Forms, and Fermat's Last Theorem (Hong Kong, 1993)*, Ser. Number Theory I, Internat. Press, Cambridge, MA, 1995, pp. 41–78.

[GS]   Golod, E. and Shafarevich, I.: On class field towers, *Izv. Akad. Nauk SSSR* **28** (1964), 261–272 [In Russian]; English transl. in *Amer. Math. Soc. Transl.* 48. Amer. Math. Soc., Providence, RI, 1965, pp. 91–102.

[H]   Hajir, F.: On the growth of *p*-class groups in *p*-class field towers, *J. Algebra* **188** (1997), 256–271.

[HM]   Hajir, F. and Maire, C.: Unramified subextensions of ray class field towers, Preprint 2001.

[I]   Ihara, Y.: How many primes decompose completely in an infinite unramified Galois extension of a global field? *J. Math. Soc. Japan* **35** (1983), 693–709.

[J]   Jehne, W.: On knots in algebraic number theory, *J. Reine Angew. Math.* **311/312** (1979), 215–254.

[K]   Koch, H.: *Galoissche Theorie der p-Erweiterungen*, VFB Deutscher Verlag der Wissenschaften, Berlin, 1970.

[Ko]   Kondo, T.: Algebraic number fields with the discriminant equal to that of a quadratic number field, *J. Math. Soc. Japan* **47**(1) (1995), 31–36.

[LT]   Litsyn, S. N. and Tsfasman, M. A.: Constructive high-dimensional sphere packings, *Duke Math. J.* **54**(1) (1987), 147–161.

[M]   Maire, C.: Extensions *T*-ramifiées modérées, *S*-décomposées, Thesis, Besançon (1995).

[Ma1]   Martinet, J.: Tours de corps de classes et estimations de discriminants, *Invent. Math.* **44** (1978), 65–73.

[Ma2]   Martinet, J.: Les tours de corps de classes, unpublished manuscript, 1984.

[Ma3]   Martinet, J.: Petits Discriminants, *Ann. Inst. Fourier (Grenoble)* **29**(1) (1979), 159–170.

[Mas]   Masley, J. M.: Odlyzko bounds and class number problems, In: A. Fröhlich (ed.), *Algebraic Number Fields (Proc. Durham Symp. 1975)*, Academic Press, New York, 1977, pp. 465–474,

[Mi]   Minkowski, H.: Théorèmes arithmétiques, *C. R. Acad. Sci. Paris* **112** (1891), 209–212. Reprinted in Ges. Abh. I, pp. 261–263, Chelsea, 1967.

[O1]   Odlyzko, A. M.: Some analytic estimates of class numbers and discriminants, *Invent. Math.* **29** (1975), 275–286.

[O2]   Odlyzko, A. M.: Lower bounds for discriminants of number fields, *Acta Arith.* **29** (1976), 275–297.

[O3]   Odlyzko, A. M.: Lower bounds for discriminants of number fields II, *Tokoku Math. J.* **29** (1977), 209–216.

[O4]   Odlyzko, A. M.: Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results, *Sém. de Théorie des Nombres, Bordeaux* **2** (1990), 119–141.

[P]   Poitou, G.: Minorations de discriminants (d'après A. M. Odlyzko), *Séminaire Bourbaki, Vol. 1975/76*, 28ème année, Exp. No. 479, pp. 136–153, Lecture Notes in Math. 567, Springer, New York, 1977.

[R]   Roquette, P.: On class field towers, In: J. Cassels and A. Fröhlich (eds), *Algebraic Number Theory*, Academic Press, New York, 1980.

[S]   Schoof, R.: Infinite class field towers of quadratic fields, *J. Reine Angew. Math.* **372** (1986), 209–220.

[Se1]   Serre, J.-P.: Minorations de discriminants, note of October 1975, In: *Collected Papers of Jean-Pierre Serre*, Vol. 3, Springer, New York, 1986, pp. 240–243.

[Se2]   Serre, J.-P.: In: *Collected Papers of Jean-Pierre Serre*, Vol. 3, Springer, New York, 1986, p. 710.

[Se3]   Serre, J.-P.: Sur le nombre des points rationnels d' une courbe algébrique sur un corps fini, *C.R. Acad. Sci. Paris* **296** (1983), ser. I, 397–402. Reprinted in *Collected Papers of Jean-Pierre Serre*, Vol. 3, Springer, New York, 1986.

[Sh] Shafarevich, I.: Extensions with prescribed ramification points, *Publ. Math. I.H.E.S.* **18** (1964), 71–95 [In Russian]; English transl. In: *Amer. Math. Soc. Transl.* 59. American Math Soc., Providence, RI, 1966, pp. 128–149.

[St] Stark, H. M.: Some effective cases of the Brauer–Siegel theorem, *Invent. Math.* **23** (1974), 135–152.

[T] Tate, J. T.: The non-existence of certain Galois extensions of $\mathbb{Q}$ unramified outside 2. *Arithmetic Geometry (Tempe, AZ, 1993)*, Contemp. Math. 174, Amer. Math. Soc., Providence, RI, 1994, pp. 153–156.

[TV] Tsfasman, M. A. and Vladut, S. G.: Asymptotic properties of global fields and generalized Brauer–Siegel theorem, Prétirage 98–35, Institut Mathématiques de Luminy, 1998.

[W] Weiss, E.: *Algebraic Number Theory*, Reprint of the 1963 original, Dover Publications, Mineola, NY, 1998.

[Y1] Yamamura, K.: On infinite unramified Galois extensions of algebraic number fields with many primes decomposing almost completely, *J. Math. Soc. Japan* **38** (1986), 599–605. Correction, to appear.

[Y2] Yamamura, K.: Maximal unramified extensions of imaginary quadratic number fields of small conductor, *J. Théor. Nombres Bordeaux* **9**(2) (1997), 405–448.

Note added in proof: In a forthcoming work, we prove $\alpha_0 < 82.2$ and $\alpha_1 < 954.3$. Also, in an article to appear in the Proceedings of the 2000 European Congress, we exhibit an unramified infinite tower with root discriminant less than 84.4.