CLASS NUMBERS OF LARGE DEGREE NONABELIAN NUMBER FIELDS

KWANG-SEOB KIM AND JOHN C. MILLER

ABSTRACT. If a number field has a large degree and discriminant, the computation of the class number becomes quite difficult, especially without the assumption of GRH. In this article, we will unconditionally show that a certain nonabelian number field of degree 120 has class number one. This field is the unique $A_5 \times C_2$ extension of the rationals that is ramified only at 653 with ramification index 2. It is the largest degree number field unconditionally proven to have class number 1.

The proof uses the algorithm of Guàrdia, Montes, and Nart to calculate an integral basis and then finds integral elements of small prime power norm to establish an upper bound for the class number; further algebraic arguments prove the class number is 1. It is possible to apply these techniques to other nonabelian number fields as well.

1. INTRODUCTION

One of the problems of algebraic number theory is to get deep knowledge of the Galois groups of various Galois extensions of number fields, especially maximal extensions of number fields with restricted ramification. Such Galois groups can be regarded as étale fundamental groups of spectra of algebraic integer rings punctured at some closed points, and they play essential roles for understanding the arithmetic of number fields, analogous to the role geometric fundamental groups of manifolds do in geometry. In other words, the étale fundamental group $G = \pi_1^{\text{ét}}(\text{Spec } \mathcal{O}_K)$ of the ring of integers $\mathcal{O}_K$ of a number field K is isomorphic to $\text{Gal}(K_{ur}^f/K)$, where K_{ur}^f is the maximal extension of K which is unramified over all finite places. This is one of the motivations for the study of unramified extensions of number fields and their Galois groups. In general, one can know the abelianizations of the étale fundamental group G by examining the ideal class group of $\mathcal{O}_K$. Yamamura's results [17] tell us that $K_{ur}^f = K_l$, where the K's are imaginary quadratic fields with absolute discriminant $|d_K| \leq 420$ and K_l is the top of the class field tower of K. Hence we can find examples of abelian or solvable étale fundamental groups.

However, one can get little information on the structure of G itself via class field theory, especially in the case where G is a nonabelian simple group.

The first author has previously [9] given an example of K with $\text{Gal}(K_{ur}^f/K) \simeq A_5$ under the assumption of the generalized Riemann hypothesis (GRH). Let K be a quadratic number field $\mathbb{Q}(\sqrt{653})$ and let L be a splitting field of

$$(1.1) \qquad\qquad x^5 + 3x^3 + 6x^2 + 2x + 1,$$

©2018 American Mathematical Society

a polynomial that has complex roots. The field L is an A_5-extension of $\mathbb{Q}$ and 653 is the only prime ramified in this field, with ramification index two [3, p. 21]. Moreover, L is the unique such field [1].

By Abhyankar's lemma, the compositum KL is an extension of K which is unramified over all finite places, and KL is the unique $A_5 \times C_2$ extension of $\mathbb{Q}$ ramified only at 653 with ramification index 2. Under the assumption of GRH, the first author proved [9] that the class number of KL is 1 and futhermore that $K_{ur}^f = KL$.

We have the following natural question: Is it possible to show that $K_{ur}^f = KL$ without assuming GRH, thereby proving unconditionally the existence of a non-solvable étale fundamental group?

To do this, the first step is to unconditionally prove that KL has class number one. If a number field has a large degree and discriminant, the computation of the class number becomes quite difficult. The Minkowski bound is too large to be useful, and the root discriminant of KL is too large to be treated by Odlyzko's unconditional discriminant bounds. However, the second author showed [12] that by finding nontrivial lower bounds for sums over prime ideals of the Hilbert class field, upper bounds can be established for class numbers of fields of larger discriminant.

In this paper, we unconditionally prove that KL has class number 1. In fact, KL has degree 120, and it is the largest degree number field proven unconditionally to have class number 1. Previously, among such fields, the one with largest degree, the real cyclotomic field of conductor 151, has degree 75 [13].

Theorem 1.1. *The unique $A_5 \times C_2$ extension of $\mathbb{Q}$ ramified only at 653 with ramification index 2 has class number 1.*

2. Remark on the maximal unramified extension of $\mathbb{Q}(\sqrt{p})$

The first author proved [9] that if the class number of KL is less than 16, then the class number of KL is 1. Using discriminant lower bounds, it was further proved, *under the assumption of GRH*, that the class number of KL is indeed less than 16 (and therefore is 1), and also that the maximal unramified extension of K is KL.

Theorem 2.1 (Main theorem of [9])**.** *Let K be a real quadratic field $\mathbb{Q}(\sqrt{p})$ with narrow class number 1, where p is a prime congruent to 1 $\mod 4$ and $p \neq 5$. Suppose that there exists a totally imaginary A_5-extension L over $\mathbb{Q}$ and p is the only prime ramified in this field with ramification index 2. If $\sqrt{p} < B(1920, 0, 960)$, then the class number of KL is one and $K_{ur}^f = KL$.*

($B(n, r_1, r_2)$ is defined as an infimum of $|d_F|^{1/n_F}$ over all number fields F satisfying $n_F \geq n$ and $\frac{r_1(F)}{n_F} = \frac{r_1}{n}$ (resp. $\frac{r_2(F)}{n_F} = \frac{r_2}{n}$), where $r_1(F)$ (resp. $r_2(F)$) is the number of real (resp. complex) places of a number field F.)

In $B(1920, 0, 960)$, the number 1920 represents

$$16 \times \text{ the degree of } KL.$$

In particular, the proof of Theorem 2.1 has the following consequence.

Corollary 1. *With the notation and conditions the same as above, if the class number of KL is smaller than 16, then the class number of KL is exactly one.*

Here we briefly sketch the main elements of the proof, the details of which are given in [9].

Proof. Let M denote the Hilbert class field of KL, and let $M^{(q)}$ denote the Hilbert q-class field for a prime q. Every automorphism group of an abelian group of order less than 16 does not contain a subgroup isomorphic to A_5, so $\mathrm{Gal}(M^{(q)}/K)$ is a central extension of A_5 by $\mathrm{Gal}(M^{(q)}/KL)$. If q is odd, $\mathrm{Gal}(M^{(q)}/K)$ has a nontrivial abelian quotient [9, Cor. 2.2], contradicting that the narrow class number of K is 1. Thus the q-class group of KL is trivial for odd q.

Similarly, $\mathrm{Gal}(M^{(2)}/K)$ has a nontrivial abelian quotient if $\mathrm{Gal}(M^{(2)}/KL)$ has order greater than 2 [9, Cor. 2.3]. Also, if $\mathrm{Gal}(M^{(2)}/KL)$ is trivial, then we are done. Otherwise, we have $\mathrm{Gal}(M^{(2)}/K)$ is isomorphic to $A_5 \times C_2$ or $\mathrm{SL}_2(\mathbb{F}_5)$ [9, Cor. 2.3]. However, $\mathrm{Gal}(M^{(2)}/K)$ cannot be isomorphic to $A_5 \times C_2$ because K has narrow class number 1. Finally, it has been shown [9, pp. 116–118] that $\mathrm{Gal}(M^{(2)}/K) \simeq \mathrm{SL}_2(\mathbb{F}_5)$ also leads to a contradiction. $\qquad\square$

To prove unconditionally that KL has class number 1, it remains to show that the class number is less than 16.

3. UPPER BOUNDS ON CLASS NUMBERS OF TOTALLY COMPLEX FIELDS

The root discriminant $|d_{KL}|^{1/120}$ of KL is approximately 25.5539. If we assume the generalized Riemann hypothesis, we can use discriminant lower bounds [11, 14] to show that any totally complex field with degree 480 or larger must have root discriminant larger than 26.48. But the root discriminant of KL is equal to the root discriminant of its Hilbert class field, so under GRH the class number of KL must be less than 4.

However, without the assumption of GRH, this method fails for totally complex fields with root discriminant above $4\pi e^\gamma \approx 22.3816$. To make further progress, we must find another approach that can handle large root discriminants. Such a method was introduced in [12] for totally real fields. By finding sufficiently many integral elements with small prime norm, an upper bound for class numbers could be established even for fields of large discriminant.

We prove a similar result for totally complex fields.

Theorem 3.1. *Let K be a totally complex Galois number field of degree n, and let*

$$F(x) = \frac{e^{-(x/c)^2}}{\cosh \frac{x}{2}}$$

for some positive constant c. Suppose S is a subset of the prime integers which are unramified in K and factor into principal prime ideals of K of degree f_p. Let

$$B = \gamma + \log 8\pi - \log \mathrm{rd}(K) - \int_0^\infty \frac{1 - F(x)}{2 \sinh \frac{x}{2}}\, dx + 2 \sum_{p \in S} \sum_{m=1}^\infty \frac{\log p}{p^{f_p m/2}} F(f_p m \log p),$$

where γ is Euler's constant. If $B > 0$, then we have an upper bound for the class number h of K,

$$h < \frac{2c\sqrt{\pi}}{nB}.$$

Proof. The proof is a modification of the argument in [12]. We apply Poitou's version [15] of Weil's "explicit formula" for the Dedekind zeta function of the Hilbert

class field $H(K)$ of K:

$$\log d(H(K)) = hr_1\frac{\pi}{2} + hn(\gamma + \log 8\pi) - hn\int_0^\infty \frac{1-F(x)}{2\sinh\frac{x}{2}}\,dx$$
$$- hr_1\int_0^\infty \frac{1-F(x)}{2\cosh\frac{x}{2}}\,dx - 4\int_0^\infty F(x)\cosh\frac{x}{2}\,dx$$
$$+ \sum_\rho \Phi(\rho) + 2\sum_{\mathfrak{P}}\sum_{m=1}^\infty \frac{\log N\mathfrak{P}}{N\mathfrak{P}^{m/2}}F(m\log N\mathfrak{P}),$$

where γ is Euler's constant and $r_1 = 0$ since K is totally complex. The first sum is over the nontrivial zeros of the Dedekind zeta function of $H(K)$, the second sum is over the prime ideals of $H(K)$, and Φ is defined by

$$\Phi(s) = \int_{-\infty}^\infty F(x)e^{(s-1/2)x}\,dx.$$

By our choice of F, the real part of $\Phi(s)$ is nonnegative everywhere in the critical strip. Indeed, on the boundary of the critical strip, the real part

$$\operatorname{Re}\Phi(s) = \operatorname{Re}\int_{-\infty}^\infty \frac{e^{-(x/c)^2}}{\cosh\frac{x}{2}}e^{(s-1/2)x}\,dx$$
$$= \int_{-\infty}^\infty e^{-(x/c)^2}\cos(x\operatorname{Im}s)\,dx = c\sqrt{\pi}e^{-(c\operatorname{Im}s/2)^2} > 0$$

is positive, and $\operatorname{Re}\Phi(s) \to 0$ as $|\operatorname{Im}s| \to \infty$, so by the maximum modulus principle for harmonic functions, $\operatorname{Re}\Phi(s)$ cannot be negative anywhere in the critical strip.

Since the root discriminant $\operatorname{rd}(K)$ of K equals the root discriminant of $H(K)$, we have

$$\log d(H(K)) = hn\log\operatorname{rd}(H(K)) = hn\log\operatorname{rd}(K),$$

and also

$$4\int_0^\infty F(x)\cosh\frac{x}{2}\,dx = 2c\sqrt{\pi}.$$

We therefore get the expression

$$hn\log\operatorname{rd}(K) = hn(\gamma + \log 8\pi) - hn\int_0^\infty \frac{1-F(x)}{2\sinh\frac{x}{2}}\,dx$$
$$- 2c\sqrt{\pi} + \sum_\rho \Phi(\rho) + 2\sum_{\mathfrak{P}}\sum_{m=1}^\infty \frac{\log N\mathfrak{P}}{N\mathfrak{P}^{m/2}}F(m\log N\mathfrak{P}).$$

We rearrange this to get the identity

$$(3.1)\qquad h = \frac{2c\sqrt{\pi}}{n\left[\gamma + \log 8\pi - \mathcal{G}(F) - \log\operatorname{rd}(K) + \frac{1}{hn}\sum_\rho \Phi(\rho) + \frac{2}{hn}\sum_{\mathfrak{P}}\sum_{m=1}^\infty \frac{\log N\mathfrak{P}}{N\mathfrak{P}^{m/2}}F(m\log N\mathfrak{P})\right]},$$

where

$$\mathcal{G}(F) = \int_0^\infty \frac{1-F(x)}{2\sinh\frac{x}{2}}\,dx.$$

To get an upper bound for the class number h, we need to bound from below the sum over the zeros and the sum over the primes. The sum $\sum_\rho \Phi(\rho)$ over the critical zeros is nonnegative since the real part of $\Phi(s)$ is nonnegative on the critical strip. We note that principal ideals in K totally split in the Hilbert class field of K. To find a nontrivial lower bound for the sum over prime ideals of the Hilbert class field,

we consider the contribution of the hn/f_p prime ideals $\mathfrak{P}$ of degree f_p that lie over some unramified rational prime p:

$$\frac{2}{hn} \sum_{\mathfrak{P}|p} \sum_{m=1}^{\infty} \frac{\log N\mathfrak{P}}{N\mathfrak{P}^{m/2}} F(m \log N\mathfrak{P}) = 2 \sum_{m=1}^{\infty} \frac{\log p}{p^{f_p m/2}} F(f_p m \log p).$$

Summing this contribution over an arbitrary set S of unramified primes gives a lower bound for the sum over the prime ideals, proving the theorem. $\square$

4. An integral basis for KL

In order to apply Theorem 3.1, we must find sufficiently many integral elements of small prime power norm. To do this, we first must compute a basis of the ring of integers $\mathcal{O}_{KL}$ of KL.

In general, it is difficult to compute an integral basis for a number field with such large degree and takes an unfeasibly long time using the commonly implemented algorithms. Fortunately, Jordi Guàrdia, Jesús Montes, and Enric Nart studied and recently implemented an algorithm that allows for fast computation of an integral basis. (The detailed algorithms are described in [4], [5], and [6].) The "Montes package" is available at their homepage [7].

To use the Montes package, we must find a polynomial $f(x)$ defining our field KL. From the work of Basmaji and Kiming [1], it is known that there is a unique A_5-extension of $\mathbb{Q}$ which is ramified only at 653 with ramification index 2, and so there is a unique $A_5 \times C_2$-extension of $\mathbb{Q}$ ramified only at 653 with ramification index 2. We can also check that the splitting field of

(4.1) $$x^{12} - 2x^{10} + x^8 - 3x^6 + 2x^4 + 4x^2 + 1$$

(see [8]) is an $A_5 \times C_2$-extension of $\mathbb{Q}$, and ramified only at 653 with ramification two. Therefore the splitting field of (4.1) is isomorphic to KL, and we find that the defining polynomial $f(x)$ of the splitting field has reasonably-sized coefficients.

The polynomial $f(x)$ is too long to write here. Instead, we upload this polynomial $f(x)$ in a file with the arXiv submission of this paper.

Now let a be a zero of the polynomial $f(x)$, i.e., $KL = \mathbb{Q}(a)$. We can get an integral basis

$$\mathcal{B} = (b_1, b_2, \ldots, b_{120})$$

for KL by using the Montes package and Magma software, where each $b_i \in \mathbb{Q}[a]$. The basis is included as an ancillary file with the arXiv submission of this paper.

4.1. **Finding a better integral basis for KL.** Let $\sigma_1, \bar{\sigma}_1, \sigma_2, \bar{\sigma}_2, \ldots, \sigma_{60}, \bar{\sigma}_{60}$ be the 60 conjugate pairs of embeddings of LK into the complex numbers. We have the usual embedding ι of KL into $\mathbb{R}^{120}$,

$$\iota : KL \hookrightarrow \mathbb{R}^{120}$$
$$x \longmapsto (\operatorname{Re}\sigma_1(x), \operatorname{Im}\sigma_1(x), \ldots, \operatorname{Re}\sigma_{60}(x), \operatorname{Im}\sigma_{60}(x)).$$

Under this map, the ring of integers $\mathcal{O}_{KL}$ is embedded as a lattice in $\mathbb{R}^{120}$.

In order to find an upper bound for the class number of KL, we must find sufficiently many integral elements with small multiplicative norm. For this purpose, we desire a "nice" integral basis for $\mathcal{O}_{KL}$. We thereby encounter the classical problem of lattice basis reduction. We can apply the Lenstra-Lenstra-Lovász (LLL)

TABLE 1. Generators of some small degree 1 primes in $\mathcal{O}_{KL}$

Element	Norm	Element	Norm
$c_2 + c_{17} + c_{46}$	3571	$c_{71} + c_{74}$	43787
$c_3 - c_9 + c_{48}$	5477	$c_{30} + c_{62}$	44879
$c_{14} - c_{41}$	7499	$c_1 - c_{17} + c_{77}$	45361
$c_1 - c_{48} + c_{64}$	8867	c_{95}	46271
$c_{11} + c_{75}$	15679	$c_2 - c_{28} - c_{62}$	48341
$c_2 - c_{54} + c_{70}$	17203	$c_{23} - c_{53} + c_{85}$	54311
$c_3 + c_{12} - c_{100}$	20047	$c_2 + c_{31} + c_{76}$	95327
$c_{23} + c_{104}$	25343	$c_{36} + c_{49}$	111611
$c_{25} - c_{74}$	31477	$c_3 + c_{22} + c_{66}$	113081
$c_{10} - c_{21} + c_{97}$	34613	$c_{23} - c_{62}$	137927
$c_{49} - c_{80}$	35537	$c_7 - c_{89}$	139999

TABLE 2. Generators of some small degree 2 and degree 3 primes in $\mathcal{O}_{KL}$

Element	Norm	Element	Norm
$c_9 + c_{62}$	13^2	c_{69}	229^2
c_{71}	83^2	$c_{22} + c_{25}$	251^2
c_{94}	89^2	$c_{24} - c_{75}$	383^2
$c_4 + c_{17} - c_{76}$	137^2	$c_7 + c_{42}$	433^2
$c_8 - c_{62}$	227^2	$c_1 - c_7 + c_{68}$	11^3

algorithm [10]. Then we applied the LLL-algorithm repeatedly (in fact, 279 times) until we obtained another basis

$$\mathcal{C} = (c_1, c_2, \ldots, c_{120}), \quad c_i \in \mathbb{R}^{120},$$

that has sufficiently short c_i. The inverse of change of basis matrix to get from $\iota(\mathcal{B})$ to $\mathcal{C}$ can be found as an ancillary file with the arXiv submission of this paper.

5. FINDING ELEMENTS OF $\mathcal{O}_{KL}$ WITH SMALL MULTIPLICATIVE NORM

Our next step is to find integral elements of our number field KL with small multiplicative norm. Then we can apply the theorem from [12] to establish an upper bound for the class number. To find such elements of small norm, we will search over "sparse" vectors, i.e., vectors where almost all the coefficients are zero with respect to the basis (c_j).

Table 1 lists the elements of small prime norm that are found by searching over "sparse" vectors. These prime integers generate principal ideals which totally split in KL into 120 principal prime ideals, each of which is generated by the given element or one of its Galois conjugates. Therefore we can include the primes given in Table 1 as degree 1 primes in the set S used by Theorem 3.1.

Table 2 lists some elements which have norms of small prime power. Each of these primes can be included in the set S as degree 2 primes, except for 11 which

TABLE 3. Generators of some composite ideals in $\mathcal{O}_{KL}$

Element	Norm	Element	Norm
$c_2 + c_{65}$	$13^2 * 19^2$	$c_{24} - c_{80}$	$13^2 * 19963$
$c_9 - c_{89}$	$13^2 * 7^3$	$c_1 + c_{65} + c_{77}$	$19^2 * 23431$
$c_{24} - c_{70}$	$13^2 * 6361$	$c_{53} - c_{89}$	$19^2 * 23531$
$c_{35} + c_{91}$	$13^2 * 10753$	$c4 + c_{25} - c_{61}$	$13^2 * 32309$
$c_{68} + c_{93}$	$13^2 * 11681$	c_{80}	$31147 * 33403$
$c_{18} + c_{91}$	$13^2 * 109^2$	$c_{15} + c_{100}$	$13^2 * 41621$
$c_3 + c_{39} - c_{74}$	$13^2 * 23^3$	$c_1 - c_{24} + c_{72}$	$13^2 * 48179$
$c_1 + c_{68} + c_{78}$	$19^2 * 12619$	$c_{61} + c_{79}$	$13^2 * 56359$
$c_2 - c_{21} + c_{44}$	$13^2 * 16561$	$c_{56} - c_{71}$	$13^2 * 58601$

is included as degree 3. However, we have still not found enough principal prime ideals to establish a sufficiently strong upper bound for the class number of KL. Table 3 lists some integral elements and their norms. Consider, for example, the element $c_2 + c_{65}$, which has norm $13^2 \cdot 19^2$. Since we also know that $c_9 + c_{62}$ generates a degree 2 prime ideal of norm 13^2, we can divide $c_2 + c_{65}$ by the appropriate Galois conjugate of $c_9 + c_{62}$ to find an integral element of norm 19^2. Since 19 does not totally split in KL, we know that 19 factors into degree 2 principal prime ideals. By this way, we can show that the following primes totally split in KL into degree 1 principal prime ideals:

$$6361, 10753, 11681, 12619, 16561, 19963, 23431,$$

$$23531, 32309, 33403, 41621, 48179, 56359, 58601.$$

6. AN UPPER BOUND FOR THE CLASS NUMBER OF KL

We are now in a position to prove our main result by applying Theorem 3.1 and Corollary 1.

Proof of Theorem 1.1. By searching for elements of small norm, and taking quotients where necessary, we find a number of primes that can be included in the set S of unramified primes that factor into principal prime ideals. In particular, the following 36 primes totally split into degree 1 principal primes in KL:

3571, 5477, 6361, 7499, 8867, 10753, 11681, 12619, 15679, 16561, 17203, 19963, 20047,

23431, 23531, 25343, 31477, 32309, 33403, 34613, 35537, 41621, 43787, 44879, 45361,

46271, 48179, 48341, 54311, 56359, 58601, 95327, 111611, 113081, 137927, 139999.

Also, the following 11 primes factor into degree 2 principal primes in KL:

$$13, 19, 83, 89, 109, 137, 227, 229, 251, 383, 433.$$

Finally, the following three primes factor into degree 3 principal primes in KL:

$$7, 11, 23.$$

If we include these primes in our set S and set $c = 24.5$, we find that

$$2 \sum_{p \in S} \sum_{m=1}^{\infty} \frac{\log p}{p^{f_p m/2}} F(f_p m \log p) > 0.18797.$$

We can numerically calculate the integral and find that

$$\int_0^\infty \frac{1 - F(x)}{2 \sinh \frac{x}{2}}\, dx < 0.70010.$$

Since the root discriminant of KL is $\sqrt{653}$, we have

$$B = \gamma + \log 8\pi - \log \operatorname{rd}(KL) - \int_0^\infty \frac{1 - F(x)}{2 \sinh \frac{x}{2}}\, dx + 2 \sum_{p \in S} \sum_{m=1}^\infty \frac{\log p}{p^{f_p m/2}} F(f_p m \log p)$$

$$> 0.57721 + 3.22417 - 3.24079 - 0.70010 + 0.18797 = 0.04846.$$

Therefore, by Theorem 3.1, we get an upper bound for the class number of KL:

$$h_{KL} < \frac{2c\sqrt{\pi}}{nB} < \frac{2 \times 24.5\sqrt{\pi}}{120 \times 0.04846} < 14.94.$$

Since the class number is an integer, we determine that

$$h_{KL} \leq 14.$$

Applying Corollary 1, we conclude that the class number of KL is 1. $\qquad\square$

7. Summary of results and concluding remarks

We have shown unconditionally that the class number of KL is 1. Thus we know that KL does not have any solvable unramified extensions. To prove unconditionally that the étale fundamental group of $K = \mathbb{Q}(\sqrt{653})$ is A_5, the remaining task is to show that KL does not have a nonabelian simple unramified extension.

How might we rule out such nonabelian simple unramified extensions? There are at least two possible approaches: One is to gain sufficient knowledge of the prime ideals of the unramified extension in order to bound the degree of the extension, similar to our approach for bounding the degree of Hilbert class field. But this is difficult: We do not have access to a class field theory for nonabelian extensions as we have in the abelian case. A possible alternative approach may be to use the theory of Galois representations to attempt to rule out possible nonabelian unramified extensions of KL.

Acknowledgments

References

[1] J. Basmaji and I. Kiming, *A table of A_5-fields*, On Artin's Conjecture for Odd 2-dimensional Representations, Lecture Notes in Math., vol. 1585, Springer, Berlin, 1994, pp. 37–46, 122–141. MR1322317

[2] W. Bosma, J. Cannon, and C. Playout, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. MR1484478

[3] B. Cais, *Serre's Conjectures* (2005, revised 2009), http://math.arizona.edu/~cais/Papers/Expos/Serre05.pdf.

[4] J. Guàrdia, J. Montes, and E. Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, J. Théor. Nombres Bordeaux **23** (2011), no. 3, 667–696. MR2861080

[5] J. Guàrdia, J. Montes, and E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. **364** (2012), no. 1, 361–416. MR2833586

[6] J. Guàrdia, J. Montes, and E. Nart, *Higher Newton polygons and integral bases*, J. Number Theory **147** (2015), 549–589. MR3276340

[7] J. Guàrdia, J. Montes, and E. Nart, *The Montes Package Web Page*. `http://www-ma4.upc.edu/~guardia/MontesAlgorithm.html`

[8] J. Klüners and G. Malle, *A Database for Number Fields*. `http://galoisdb.math.upb.de/home`

[9] K.-S. Kim, *A construction of nonabelian simple étale fundamental groups*, Ramanujan J. **35** (2014), no. 1, 111–120. MR3258601

[10] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 515–534. MR682664

[11] J. Martinet, *Petits discriminants des corps de nombres*, Number Theory Days, 1980 (Exeter, 1980), London Math. Soc. Lecture Note Ser., vol. 56, Cambridge Univ. Press, Cambridge-New York, 1982, pp. 151–193. MR697261

[12] J. C. Miller, *Class numbers of totally real fields and applications to the Weber class number problem*, Acta Arith. **164** (2014), no. 4, 381–398. MR3244941

[13] J. C. Miller, *Real cyclotomic fields of prime conductor and their class numbers*, Math. Comp. **84** (2015), no. 295, 2459–2469. MR3356035

[14] A. M. Odlyzko, *Table 3: GRH bounds for discriminants*, `http://www.dtc.umn.edu/~odlyzko/unpublished/discr.bound.table3`

[15] G. Poitou, *Sur les petits discriminants*, Séminaire Delange-Pisot-Poitou, 18e année: (1976/77), Théorie des nombres, Fasc. 1 (French), Secrétariat Math., Paris, 1977, Exp. No. 6, 18pp. MR551335

[16] J.-P. Serre, *Modular forms of weight one and Galois representations*, Algebraic Number Fields: *L*-functions and Galois Properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 193–268. MR0450201

[17] K. Yamamura, *Maximal unramified extensions of imaginary quadratic number fields of small conductors*, J. Théor. Nombres Bordeaux **9** (1997), no. 2, 405–448. MR1617407

DEPARTMENT OF MATHEMATICS, CHOSUN UNIVERISTY, GWANGJU 501-759, KOREA
Email address: `kwang12@chosun.ac.kr`

DEPARTMENT OF APPLIED MATHEMATICS & STATISTICS, JOHNS HOPKINS UNIVERSITY, 100 WHITEHEAD HALL, 3400 NORTH CHARLES STREET, BALTIMORE, MARYLAND 21218
Email address: `jmill268@jhu.edu`