

JOURNAL

de Théorie des Nombres

de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Peter J. CHO et Henry H. KIM

Dihedral and cyclic extensions with large class numbers

Tome 24, n° 3 (2012), p. 583-603.

http://jtnb.cedram.org/item?id=JTNB_2012__24_3_583_0

© Société Arithmétique de Bordeaux, 2012, tous droits réservés.

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://jtnb.cedram.org/legal/>). Toute reproduction en tout ou partie de cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>

Dihedral and cyclic extensions with large class numbers

par PETER J. CHO et HENRY H. KIM

RÉSUMÉ. Cet article est la suite de [2]. Nous construisons inconditionnellement plusieurs familles de corps de nombres ayant un grand nombre de classes. Ce sont des corps de nombres dont la clôture galoisienne a pour groupe de Galois les groupes diédraux D_n , $n = 3, 4, 5$, et les groupes cycliques C_n , $n = 4, 5, 6$. Nous construisons d'abord des familles de corps de nombres à petits régulateurs et, en utilisant la conjecture d'Artin forte et en appliquant une variante du résultat de densité nulle de Kowalski et Michel, nous choisissons des sous-familles telles que les fonctions L correspondantes soient sans zéro près de 1. Pour ces sous-familles, la fonction L prend une valeur extrémale en $s = 1$ et, par la formule du nombre de classes, nous obtenons un grand nombre de classes.

ABSTRACT. This paper is a continuation of [2]. We construct unconditionally several families of number fields with large class numbers. They are number fields whose Galois closures have as the Galois groups, dihedral groups D_n , $n = 3, 4, 5$, and cyclic groups C_n , $n = 4, 5, 6$. We first construct families of number fields with small regulators, and by using the strong Artin conjecture and applying some modification of zero density result of Kowalski-Michel, we choose subfamilies such that the corresponding L -functions are zero free close to 1. For these subfamilies, the L -functions have the extremal value at $s = 1$, and by the class number formula, we obtain large class numbers.

1. Introduction

This paper is a continuation of [2]. Let $\mathfrak{R}(n, G, r_1, r_2)$ be the set of number fields of degree n with signature (r_1, r_2) whose normal closures have G as their Galois group. In [2], we constructed families of number fields with the largest possible class numbers belonging to $\mathfrak{R}(5, S_5, 1, 2)$, $\mathfrak{R}(4, S_4, 2, 1)$,

Manuscrit reçu le 20 juillet 2011.

H. Kim is partially supported by an NSERC grant.

$\mathfrak{K}(4, S_4, 0, 2)$ and $\mathfrak{K}(4, A_4, 0, 2)$. In this paper, we construct families of number fields with large class numbers whose Galois closures have as Galois groups, dihedral groups D_n , $n = 3, 4, 5$, and cyclic groups C_n , $n = 4, 5, 6$.

The idea is the same as in [2]. Namely, we use the class number formula; the class number h_{K_t} for $K_t \in \mathfrak{K}(n, G, r_1, r_2)$ is given by

$$h_{K_t} = \frac{w_{K_t} |d_{K_t}|^{\frac{1}{2}}}{2^{r_1} (2\pi)^{r_2} R_{K_t}} L(1, \rho_t),$$

where w_{K_t} is the number of roots of unity in K_t , d_{K_t} is the discriminant of K_t and R_{K_t} is its regulator and $L(s, \rho_t) = \frac{\zeta_{K_t}(s)}{\zeta(s)}$ is the Artin L-function.

We first construct a family of number fields K_t with small regulators, and then find a subfamily for which $L(1, \rho_t) \gg (\log \log |d_{K_t}|)^{n-1}$. However, in our cases, ρ_t is no longer irreducible, and hence it is no longer attached to a cuspidal automorphic representation. We need to modify the result of [14] to isobaric automorphic representations. See section 3.

In section 4, we use the quintic polynomial considered by Schöpp [22] and Lavallee-Spearman-Williams-Yang [15] who showed that they give rise to number fields whose Galois closures has D_5 as the Galois group, and computed fundamental units when they are of signature (1,2). We prove that they give rise to regular Galois extensions over $\mathbb{Q}(t)$, and we compute regulators and show that they have the largest class numbers.

In section 5, we use the family of quartic polynomials considered by Nakamura [19] who showed that they give rise to number fields whose Galois closures have D_4 as the Galois group, and computed regulators. We prove that they give rise to regular Galois extensions over $\mathbb{Q}(t)$, and show that they have large class numbers. We conjecture that they have the largest possible class numbers.

In section 6, we prove that the cubic extensions considered by Ishida [11] have the largest possible class numbers. This family is different from the one considered by Daileida [5].

In section 7, we consider totally real cyclic extensions. They are sometimes called simplest fields. We prove a very general result that a cyclic extension of prime degree generated by a unit always has the smallest regulator. We use the result in [7] that if the cyclic extension is given by a polynomial $f(x, t)$ of degree p with the constant term ± 1 , then any $p - 1$ roots are multiplicatively independent. However, it is no longer true for composite degree. Cyclic quintic fields were studied by Lehmer [17], Jeanin [12], and Schoof-Washington [21]. We compute the regulators and prove that they have the largest possible class numbers. Cyclic quartic fields were studied by Lazarus [16], and cyclic sextic fields by Gras [9]. They determined fundamental units. We compute the regulators and prove that they have large class numbers.

When $n = 4, 6$, due to the existence of subfields, our regulator bounds are greater than Silverman's bounds [25]. However, we conjecture that in the case of regular Galois extensions, our bounds are sharp. (see Remark 7.3.)

2. Representations of dihedral groups

Let's review irreducible representations of D_n : If n is odd, $D_n = \langle a, x : a^n = x^2 = e, xax = a^{-1} \rangle$. Let $H = \{1, x\}$. Then irreducible representations of D_n are: 2 one-dimensional representations $1, \chi$, and $\frac{n-1}{2}$ two-dimensional representations $\rho_1, \dots, \rho_{\frac{n-1}{2}}$, where χ is the character of H . We have $Ind_H^G 1 = 1 + \rho_1 + \dots + \rho_{\frac{n-1}{2}}$.

If n is even, $D_n = \langle a, x : a^n = x^2 = e, xax = a^{-1} \rangle$. Let $H_1 = \{1, x\}$, $H_2 = \{1, a^{\frac{n}{2}}\}$, $H_3 = \{1, a^{\frac{n}{2}}x\}$ be three order 2 subgroups. Then irreducible representations of D_n are: 4 one-dimensional representations $1, \chi_1, \chi_2, \chi_3$, and $\frac{n-2}{2}$ two-dimensional representations $\rho_1, \dots, \rho_{\frac{n-2}{2}}$, where χ_i is the character of H_i . We have, for each i , $Ind_{H_i}^G 1 = 1 + \chi_i + \rho_1 + \dots + \rho_{\frac{n-2}{2}}$.

Let K/\mathbb{Q} be a degree n extension and \hat{K}/\mathbb{Q} be the Galois closure such that $Gal(\hat{K}/\mathbb{Q}) \simeq D_n$. Then if n is odd,

$$\frac{\zeta_K(s)}{\zeta(s)} = L(s, \rho_1) \cdots L(s, \rho_{\frac{n-1}{2}}).$$

If n is even,

$$\frac{\zeta_K(s)}{\zeta(s)} = L(s, \chi)L(s, \rho_1) \cdots L(s, \rho_{\frac{n-2}{2}}),$$

where $H = Gal(\hat{K}/K)$ is one of the order 2 subgroups of D_n , and χ is the non-trivial character of H .

3. Approximation of $L(1, \rho)$ and zero-free region

We use the following result of Daileda [5] to obtain a bound for $L(1, \rho)$: Let ρ be an l -dimensional complex representation of a Galois group. We assume $L(s, \rho)$ is an entire Artin L-function and N is its conductor. Also $L(s, \rho)$ has a Dirichlet series

$$L(s, \rho) = \sum_{n=1}^{\infty} \lambda(n)n^{-s}.$$

Proposition 3.1. [5] *Let $L(s, \rho)$ and N be as above. Let $\frac{6}{7} < \alpha < 1$. Suppose that $L(s, \rho)$ is zero-free in the rectangle $[\alpha, 1] \times [-(\log N)^2, (\log N)^2]$. If N is sufficiently large, then for any $0 < k < \frac{16}{1-\alpha}$,*

$$\log L(1, \rho) = \sum_{p \leq (\log N)^k} \lambda(p)p^{-1} + O_{l,k,\alpha}(1).$$

This implies immediately that $L(1, \rho) \ll (\log \log N)^l$ since $|\lambda(p)| \leq l$ and $\sum_{p \leq x} \frac{1}{p} \sim \log \log x$.

Due to lack of GRH, we cannot use the above result directly. We extend the result of Kowalski-Michel to isobaric automorphic representations of $GL(n)$.

Let $n = n_1 + \dots + n_r$, and let $S(q)$ be a set of isobaric representations $\pi = \pi_1 \boxplus \pi_2 \cdots \boxplus \pi_r$, where π_j is a cuspidal automorphic representation of $GL(n_j)/\mathbb{Q}$ and satisfies the Ramanujan-Petersson conjecture at the finite places. We assume that for $\pi, \pi' \in S(q)$, $\pi_j \not\cong \pi'_j$ for each j . Moreover, $S(q)$ holds the following conditions:

- (1) There exists $e > 0$ such that for $\pi = \pi_1 \boxplus \pi_2 \cdots \boxplus \pi_r \in S(q)$, $Cond(\pi_1) \cdots Cond(\pi_r) \leq q^e$,
- (2) There exists $d > 0$ such that $|S(q)| \leq q^d$.
- (3) The Γ factors of π_j are of the form $\prod_{k=1}^{n_j} \Gamma(\frac{s}{2} + \alpha_k)$, where $\alpha_k \in \mathbb{R}$.

Let, for $\alpha \geq \frac{3}{4}$, $T \geq 2$,

$$N(\pi; \alpha, T) = |\{\rho : L(\rho, \pi) = 0, Re(\rho) \geq \alpha, |Im(\rho)| \leq T\}|,$$

(zeros counted with multiplicity). Then clearly, $N(\pi; \alpha, T) = N(\pi_1; \alpha, T) + \dots + N(\pi_r; \alpha, T)$.

Theorem 3.1. *For some $B \geq 0$,*

$$\sum_{\pi \in S(q)} N(\pi; \alpha, T) \ll T^B q^{c_0 \frac{1-\alpha}{2\alpha-1}}.$$

One can choose any $c_0 > c'_0$, where $c'_0 = \frac{5n'e}{2} + d$ and $n' = \max\{n_i\}_{1 \leq i \leq r}$.

Proof. Let $S(q)_j$ be the set of the cuspidal automorphic representations consisting of the j -th component of π . Since $\pi_j \not\cong \pi'_j$ for each j , $|S(q)_j| = |S(q)|$ for all $j = 1, 2, \dots, r$. Then clearly, $Cond(\pi_j) \leq q^e$ and $|S(q)_j| \leq q^d$. So

$$\sum_{\pi \in S(q)} N(\pi; \alpha, T) = \sum_{\pi \in S(q)} \sum_{j=1}^r N(\pi_j; \alpha, T) = \sum_{j=1}^r \sum_{\pi_j \in S(q)_j} N(\pi_j; \alpha, T).$$

Now we apply the result of Kowalski-Michel [14] to the inner sum. They assumed that the Gamma factors of π_j are the same. However, the assumption is used only to obtain the convexity bound (Lemma 10 of [14]), and our Γ -factors provide the same convexity bound. Hence our result follows. \square

In the following, we apply the above result to a family of Artin L -functions. In this case, the Γ -factors are a product of $\Gamma(\frac{s}{2})$ and $\Gamma(\frac{s+1}{2})$.

4. D_5 extension with signature (1, 2)

We use a polynomial in [22] for the case of D_5 extension;

$$f(x, t) = x^5 - tx^4 + (2t - 1)x^3 - (t - 2)x^2 - 2x + 1.$$

Its discriminant is $(4t^3 - 28t^2 + 24t - 47)^2$ and the signature is (1, 2) for $t \leq 6$. (There is a minor mistake in [22]. The discriminant of $f(x, t)$ is given by $16(4t^3 - 28t^2 + 24t - 47)^2$ in [22]. But it does not affect his result.) Let θ_t be a root of $f(x, t)$. Schöpp found the fundamental units in the equation order $\mathbb{Z}[\theta_t]$. More precisely, he shows

Theorem 4.1 (Schöpp). *The elements $\theta_t, \theta_t - 1$ form a system of independent units in the order $\mathbb{Z}[\theta_t]$. Moreover, they are fundamental units in $\mathbb{Z}[\theta_t]$ for $t \leq 6$.*

However, Schöpp could not show that $\mathbb{Z}[\theta_t]$ is the maximal order of $\mathbb{Q}(\theta_t)$. Lavallee, Spearman, Williams and Yang [15] found a parametric family of quintics with a power integral basis. The parametric polynomial $F_b(x)$ is given by

$$F_b(x) := x^5 - 2x^4 + (b + 2)x^3 - (2b + 1)x^2 + bx + 1, b \in \mathbb{Z}.$$

and its discriminant is $(4b^3 + 28b^2 + 24b + 47)^2$.

They showed that when $4b^3 + 28b^2 + 24b + 47$ is square-free, then the field $Q(\theta_b)$ generated by a root θ_b of $F_b(x)$ has a power integral basis $\mathbb{Z}[\theta_b]$. Since $x^5 F_{-t}(\frac{1}{x}) = f(x, t)$, this implies that $\theta_t, \theta_t - 1$ are fundamental units of $\mathbb{Q}(\theta_t)$ when $4t^3 - 28t^2 + 24t - 47$ is square-free.

Schöpp found the locations of roots of $f(x, t)$.

Lemma 4.1 (Schöpp). *Let $\theta_t^{(1)}$ be the real root and let $\theta_t^{(2)} = \overline{\theta_t^{(3)}}$, $\theta_t^{(4)} = \overline{\theta_t^{(5)}}$ be the pairs of complex roots of $f(x, t)$. Then we have the following approximations:*

- (i) $-t + 2 + \frac{2}{t} < |\theta_t^{(1)}| < -t + 2 + \frac{1}{t}$ for $t < -4$
- (ii) $-t + 3 + \frac{2}{t} < |\theta_t^{(1)} - 1| < -t + 3 + \frac{1}{t}$ for $t < -4$
- (iii) $\frac{1}{2\sqrt{-t}} < |\theta_t^{(2)}| < \frac{2}{\sqrt{-t}}$ for $t < -4$
- (iv) $\sqrt{1 - \frac{3}{4t}} < |\theta_t^{(2)} - 1| < \sqrt{1 - \frac{6}{5t}}$ for $t < -144$
- (v) $\sqrt{1 + \frac{3}{t}} < |\theta_t^{(4)}| < \sqrt{1 - \frac{1}{t^2}}$ for $t < -174$
- (v) $\sqrt{-\frac{5}{6t}} < |\theta_t^{(4)} - 1| < \sqrt{-\frac{14}{13t}}$ for $t < -139$.

Let K_t be the quintic field by adjoining $\theta_t^{(1)}$ to \mathbb{Q} . Since we know the absolute value of roots, it is easy to show that the regulator R_{K_t} of a quintic field K_t is

$$R_{K_t} \ll (\log d_{K_t})^2.$$

when $4t^3 - 28t^2 + 24t - 47$ is square-free.

We claim that $f(x, t)$ gives rise to a regular D_5 extension over $\mathbb{Q}(t)$, i.e., if we consider $f(x, t)$ as a polynomial over $\mathbb{Q}(t)$ and E is the splitting field, then $E \cap \overline{\mathbb{Q}} = \mathbb{Q}$. This is equivalent to the fact that $Gal(E\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(t)) \simeq Gal(E/\mathbb{Q}(t))$.

By [13], page 41, the Weber sextic resolvent of $f(x, t)$ is

$$G(z) = (z^3 + b_4z^2 + b_2z + b_0)^2 - 2^{10}(4t^3 - 28t^2 + 24t - 47)^2z,$$

where $b_4 = -4t^2 - 4t + 37, b_2 = 64t^3 - 312t^2 + 328t + 115, b_0 = 64t^3 - 2884t^2 + 4348t - 249$. It factors as

$$\begin{aligned} G(z) &= (z - 4t^2 + 12t - 9) \\ &\quad \times (z^5 - (4t^2 + 20t - 83)z^4 \\ &\quad + (128t^3 - 368t^2 - 816t + 2346)z^3 \\ &\quad - (1024t^4 - 7040t^3 + 16536t^2 + 3448t - 29126)z^2 \\ &\quad + (2048t^4 + 51072t^3 - 201328t^2 + 18640t + 256933)z \\ &\quad - (1024t^4 - 89216t^3 + 1948548t^2 - 231404t + 6889)). \end{aligned}$$

Therefore, the Galois group of $f(x, t)$ over $\mathbb{Q}(t)$ and $\overline{\mathbb{Q}}(t)$ is either D_5 or C_5 . In order to distinguish it, we use the criterion in [13], page 42. Namely, the Galois group is C_5 if and only if the resolvent $R(x_1 - x_2, f(x, t))(X)$ factors into irreducible polynomials of degree 5. Here

$$\begin{aligned} &R(x_1 - x_2, f(x, t))(X) \\ &= X^{-5}Res(f(Y - X, t), f(Y, t)) \\ &= (X^{10} + X^8(-2t^2 + 12t - 8) + X^6(t^4 - 12t^3 + 46t^2 - 56t - 4) \\ &\quad + X^4(-2t^4 + 16t^3 - 8t^2 - 112t + 127) \\ &\quad + X^2(t^4 - 60t^2 + 128t + 6) - 4t^3 + 28t^2 - 24t + 47) \\ &\quad \times (X^{10} + X^8(-2t^2 + 8t - 2) + X^6(t^4 - 8t^3 + 20t^2 - 4t + 7) \\ &\quad + X^4(-2t^4 + 36t^2 - 4t + 41) \\ &\quad + X^2(t^4 - 4t^3 + 66t^2 - 36t + 103) - 4t^3 + 28t^2 - 24t + 47) \end{aligned}$$

It is clear that the above factors cannot be factored into irreducible polynomials of degree 5. Hence the Galois group of $f(x, t)$ over both $\mathbb{Q}(t)$ and $\overline{\mathbb{Q}}(t)$ is D_5 .

From now on, we replace t by $-t$ in $f(x, t)$ because we want that t varies in positive integers. Then the discriminant of $f(x, t)$ become $(4t^3 + 28t^2 + 24t + 47)^2$. Let \hat{K}_t be the Galois closure of K_t and $Gal(\hat{K}_t/\mathbb{Q}) \simeq D_5$. Then

$$\frac{\zeta_{K_t}(s)}{\zeta(s)} = L(s, \rho_t) = L(s, \sigma_{t,1})L(s, \sigma_{t,2}),$$

where $\rho_t = \sigma_{t,1} \oplus \sigma_{t,2}$ and $\sigma_{1,t}$ and $\sigma_{2,t}$ are the 2-dimensional representations of D_5 . Now D_5 has the cyclic subgroup C_5 of order 5 and let M_t be the fixed field by C_5 . Then $\sigma_{1,t}, \sigma_{2,t}$ are induced by non-trivial characters for \widehat{K}_t/M_t . Hence the Artin conductors of σ_1 and σ_2 equal $|d_{M_t}|N_{M_t/\mathbb{Q}}(\mathfrak{b}_t)$ where \mathfrak{b}_t is the Artin conductor of nontrivial characters of C_5 . Since $d_{K_t} = (4t^3 + 28t^2 + 24t + 47)^2 = (|d_{M_t}|N_{M_t/\mathbb{Q}}(\mathfrak{b}_t))^2$ for $4t^3 + 28t^2 + 24t + 47$ square-free, the Artin conductors of $\sigma_{1,t}, \sigma_{2,t}$ are both $4t^3 + 28t^2 + 24t + 47$. Hence, the Hypotheses of Theorem 3.1 are satisfied.

By Serre’s observation (see p.45 in [23]), there exists a constant c_f depending only on f such that for every prime $q \geq c_f$, there is an integer t_q with q splits completely in K_t for all $t \equiv t_q \pmod q$.

Now for given $X \gg 1$, define $y = \frac{\log X}{\log \log X}$ and $M = \prod_{c_f \leq q \leq y} q$. Let t_M be an integer such that $t_M \equiv t_q \pmod q$ for all $c_f \leq q \leq y$. Here $\log M \sim y$, and hence $M \ll X^\epsilon$ for any $\epsilon > 0$.

Since discriminant $discf(x, t)$ of $f(x, t)$ is a polynomial of degree 6, there is a constant $C > 0$ such that $discf(x, t) < Ct^6$. Now we define a set $L(X)$ of square-free integers,

$$L(X) = \left\{ \frac{X}{2} < t < X \mid 4t^3 + 28t^2 + 24t + 47 \text{ square-free, } t \equiv t_M \pmod M \right\}.$$

Let $t = Mm + t_M$, and let $h(m) = 4(Mm + t_M)^3 + 28(Mm + t_M)^2 + 24(Mm + t_M) + 47$. It is a cubic polynomial. By [10], page 69, $|L(X)| = \beta \frac{X}{2M} + O\left(\frac{X}{M(\log \frac{X}{M})^{\frac{1}{2}}}\right)$ for some constant β . Hence $|L(X)| \gg X^{1-\epsilon}$. By the construction of $L(X)$, every $t \in L(X)$ gives rise to a distinct automorphic L -function $L(s, \rho_t) = \sum_{n=1}^\infty \lambda_t(n)n^{-s}$ of $GL(4)/\mathbb{Q}$ with $\lambda_t(q) = 4$ for all $c_f \leq q \leq y$.

By the above argument, we have

$$X^{1-\epsilon} \ll |L(X)| \ll X.$$

We apply Theorem 3.1 to the family $L(X)$ with $n' = 2$, $T = (\log CX^6)^2$, $e = 6$ and $d = 1$. Let $c_0 = 31$. Choose α with $c_0 \frac{1-\alpha}{2\alpha-1} < \frac{98}{100}$. Then every $L(s, \rho_t)$ in $L(X)$ excluding exceptional $O(X^{98/100})$ L -functions is zero free in the rectangle $[\alpha, 1] \times [-(\log d_{K_t})^2, (\log d_{K_t})^2]$. Applying Proposition 3.1 to $L(s, \rho_t)$, we have

$$\begin{aligned} \log L(1, \rho_t) &= \sum_{q \leq (\log d_{K_t})^{1/2}} \lambda(q)q^{-1} + O(1) \\ &= \sum_{c_f \leq q \leq (\log d_{K_t})^{1/2}} 4q^{-1} + O(1) = 4 \log \log \log d_{K_t} + O(1), \end{aligned}$$

where we used the fact that $(\log d_{K_t})^{1/2} \leq y = \frac{\log X}{\log \log X}$ for large X . So we have $L(1, \rho_t) \gg (\log \log d_{K_t})^4$. By the class number formula and the size of

regulator R_{K_t} , we have the required result

$$h_{K_t} \gg d_{K_t}^{1/2} \frac{(\log \log d_{K_t})^4}{(\log d_{K_t})^2}.$$

We summarize our result as follows:

Theorem 4.2. *There is a constant $c > 0$ such that there exist $K \in \mathfrak{K}(5, D_5, 1, 2)$ with arbitrarily large discriminant d_K for which*

$$h_K > cd_K^{1/2} \frac{(\log \log d_K)^4}{(\log d_K)^2}.$$

Remark 4.1. When $t > 7$, $f(x, t) = x^5 - tx^4 + (2t - 1)x^3 - (t - 2)x^2 - 2x + 1$ gives rise to a totally real extension K_t whose Galois closure has D_5 as the Galois group. In this case, numerical calculation shows that the regulator of K_t is quite large: If $t = 10^3$, $R_{K_t} \sim 8 \times 10^7$; if $t = 10^4$, $R_{K_t} \sim 2.3 \times 10^{10}$; if $t = 10^5$, $R_{K_t} \sim 9.3 \times 10^{13}$.

5. D_4 extension

Nakamura [19] constructed quartic fields with small regulators whose Galois closures have D_4 as the Galois group. We prove that Nakamura's family of quartic fields have large class numbers. We conjecture that they have the largest possible class numbers. (See Remark 7.3.) Nakamura uses a polynomial with 3 parameters

$$f = x^4 - sx^3 + (t + 2u)x^2 - usx + 1$$

where $(s, t, u) \in \mathbb{N} \times \mathbb{Z} \times \{\pm 1\}$, $(s, t, u) \neq (1, -1, 1)$.

The discriminant D_f of f is given by

$$D_f = D_1^2 D_2 \text{ with } D_1 = s^2 - 4t, \quad D_2 = (t + 4u)^2 - 4us^2.$$

For a zero ϵ of f with $|\epsilon| \geq 1$, we define $\alpha := \epsilon + u\epsilon^{-1}$. Put

$$K = \mathbb{Q}(\epsilon), \quad F = \mathbb{Q}(\sqrt{D_1}), \quad L = \mathbb{Q}(\sqrt{D_2}), \quad M = \mathbb{Q}(\sqrt{D_1 D_2})$$

Then $F = \mathbb{Q}(\alpha) \subseteq K = F(\epsilon) = F(\sqrt{\alpha^2 - 4u})$.

With signs of D_1 and D_2 we can determine the signature of K . More precisely,

Lemma 5.1. [19] *Assume $F \neq \mathbb{Q}$ and $L \neq \mathbb{Q}$. Then K is a non-CM quartic field with a quadratic subfield F , and $|\epsilon| > 1$. If $F = L$, then K is cyclic over \mathbb{Q} . If $F \neq L$, then K is non-Galois over \mathbb{Q} , and the composite MK is dihedral over \mathbb{Q} and cyclic over M . Moreover*

$$\begin{cases} (r_1, r_2) = (0, 2) & \text{if } D_1 < 0 \\ (r_1, r_2) = (2, 1) & \text{if } D_2 < 0 \\ (r_1, r_2) = (4, 0) & \text{otherwise.} \end{cases}$$

Moreover, if $F \neq L$, $d_F = D_1$ and $d_L = D_2$, then $d_K = D_f$.

Note that if K is not totally complex, the quadratic subfield F is real.

Let $\widehat{K} = MK$ be the Galois closure of K and $G = Gal(\widehat{K}/\mathbb{Q})$ is isomorphic to D_4 . Then G has a subgroup H isomorphic to C_2 such that $\widehat{K}^H = K$. Let $Ind_H^G 1_H = 1 + \rho$ be the induced representation of G by the trivial representation of H where ρ is a 3-dimensional representation of D_4 . Here ρ is no longer irreducible but a sum of the non-trivial 1-dimensional representation χ and the 2-dimensional representation ψ of D_4 . Since ψ is modular, ρ is modular. We can check easily that the Artin conductor of χ is the absolute value of discriminant d_F of the quadratic subfield F of K and the Artin conductor of ρ equals to $\left| \frac{d_K}{d_F} \right|$.

Then

$$L(s, \rho) = L(s, \chi)L(s, \psi) = \frac{\zeta_K(s)}{\zeta(s)}.$$

5.1. D_4 extension with the signature (0,2). We specify that $s = u = 1$. Then we have, for positive integer t ,

$$f(x, t) = x^4 - x^3 + (t + 2)x^2 - x + 1$$

with $D_1 = 1 - 4t$, $D_2 = t^2 + 8t + 12$. If D_1, D_2 are square-free for odd integer t , D_K equals $(1 - 4t)^2(t + 2)(t + 6)$. For a positive integer t , D_1 is negative, by Lemma 5.1, $(r_1, r_2) = (0, 2)$ and MK/\mathbb{Q} is a D_4 Galois extension.

Nakamura estimated the regulator R_K of the field K .

$$R_K = \frac{1}{4} \log \frac{d_K}{16} + o(1) \text{ as } d_K \rightarrow \infty.$$

To show that $f(x, t)$ gives rise to a regular D_4 extension, we briefly recall how to determine the Galois group of a quartic polynomial over an arbitrary field F in [3], page 358. We write a quartic polynomial f in the form

$$f = x^4 - c_1x^3 + c_2x^2 - c_3x + c_4$$

and we define the Ferrari resolvent of f to be

$$\theta_f(y) = y^3 - c_2y^2 + (c_1c_3 - 4c_4)y - c_3^2 - c_1^2c_4 + 4c_2c_4.$$

Theorem 5.1. *Let F have characteristic $\neq 2$, and $f \in F[x]$ be monic and irreducible of degree 4. Then Galois group of f over F is determined as follows:*

(a) *If $\theta_f(y)$ is irreducible over F , then*

$$G = \begin{cases} S_4, & \text{if } disc(f) \notin F^2 \\ A_4, & \text{if } disc(f) \in F^2 \end{cases}$$

(b) *If $\theta_f(y)$ splits completely over F , then $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

(c) If $\theta_f(y)$ has a unique root β in F , then G is isomorphic to

$$\begin{cases} D_4, & \text{if } 4\beta + c_1^2 - 4c_2 \neq 0 \text{ and } \text{disc}(f)(4\beta + c_1^2 - 4c_2) \notin (F^*)^2 \\ & \text{or } 4\beta + c_1^2 - 4c_2 = 0 \text{ and } \text{disc}(f)(\beta^2 - 4c_4) \notin (F^*)^2 \\ C_4, & \text{otherwise.} \end{cases}$$

The Ferrari resolvent of $f(x, t)$ is

$$y^3 - (t + 2)y^2 - 3y + 4t + 6 = (y - 2)(y^2 - ty - (2t + 3)).$$

Then $\text{disc}(f(x, t))(4\beta + c_1^2 - 4c_2) = (1 - 4t)^3(t + 2)(t + 6) \notin (\overline{\mathbb{Q}}(t)^*)^2$ and $(\mathbb{Q}(t)^*)^2$. By Theorem 5.1, the Galois group of $f(x, t)$ over both $\overline{\mathbb{Q}}(t)$ and $\mathbb{Q}(t)$ is D_4 . Hence $f(x, t)$ gives rise to a D_4 regular extension over $\mathbb{Q}(t)$.

Hence as in the case of D_5 extension, we can define M, t_M and a set $L(X)$ of square-free integers

$$L(X) = \left\{ \frac{X}{2} < t < X \mid (1 - 4t)(t + 2)(t + 6) \text{ square-free, } t \equiv t_M \pmod{M} \right\}.$$

For $t \in L(X)$, $|1 - 4t|$ is the Artin conductor of the one-dimensional representation and $|(t + 2)(t + 6)(1 - 4t)|$ is the Artin conductor of the two-dimensional representation. Hence we can apply Theorem 3.1 to $L(X)$.

To estimate $|L(X)|$, we introduce Nair’s work [18]. For an polynomial $f(x) \in \mathbb{Z}[x]$ of degree d , we define,

$$N_k(f, x, h) = N_k(x, h) = |\{n : x < n \leq x + h \mid f(n) : k\text{-free}\}|.$$

He showed

Theorem 5.2 (Nair). *If*

$$f(x) = \prod_{i=1}^m (a_i x - b_i)^{\alpha_i} \text{ and } \alpha = \max_i \alpha_i,$$

then

$$N_k(x, h) = \prod_p \left(1 - \frac{\rho(p^2)}{p^2} \right) h + O\left(\frac{h}{(\log h)^{k-1}} \right)$$

for $h = x^{(\alpha/2k)+\epsilon}$ if $k > \alpha$ and $\epsilon > 0$.

Theorem 5.2 implies

$$|L(X)| = \prod_{p \nmid M} \left(1 - \frac{\rho(p^2)}{p^2} \right) \frac{X}{2M} + O\left(\frac{X}{M(\log \frac{X}{M})} \right) \gg X^{1-\epsilon}.$$

Let $c_0 = 21$. Choose α with $c_0 \frac{1-\alpha}{2\alpha-1} < \frac{98}{100}$. By applying Theorem 3.1 to $L(X)$ with $e = 4, d = 1$ and $T = (\log CX^4)^2$, every automorphic L -function excluding exceptional $O(X^{98/100})$ L -functions has a zero-free region $[\alpha, 1] \times$

$[-(\log |d_{K_t}|)^2, (\log |d_{K_t}|)^2]$. Applying Proposition 3.1 to $L(s, \rho_t)$ having the desired zero-free region, we have

$$\begin{aligned} \log L(1, \rho_t) &= \sum_{q \leq (\log d_{K_t})^{1/2}} \lambda(q)q^{-1} + O(1) \\ &= \sum_{c_f \leq q \leq (\log d_{K_t})^{1/2}} 3q^{-1} + O(1) = 3 \log \log \log d_{K_t} + O(1), \end{aligned}$$

where we used the fact that $(\log d_{K_t})^{1/2} \leq y = \frac{\log X}{\log \log X}$ for large X . So we have $L(1, \rho_t) \gg (\log \log d_{K_t})^3$.

By the class number formula and the size of regulator R_{K_t} , we have the required result

$$h_{K_t} \gg d_{K_t}^{1/2} \frac{(\log \log d_{K_t})^3}{(\log d_{K_t})}.$$

We summarize as follows:

Theorem 5.3. *There is a constant $c > 0$ such that there exist $K \in \mathfrak{K}(4, D_4, 0, 2)$ with arbitrarily large discriminant d_K for which*

$$h_K > cd_K^{1/2} \frac{(\log \log d_K)^3}{(\log d_K)}.$$

5.2. D_4 extension with the signature $(2, 1)$. We specify that $u = 1, t = 1$. Then we have $f(x, s) = x^4 - sx^3 + 3x^2 - sx + 1$ and $D_1 = s^2 - 4$ and $D_2 = 25 - 4s^2 = (5 + 2s)(5 - 2s)$. Assume that D_1 and D_2 are square-free for odd integers s . Then $d_F = D_1, d_L = D_2$ and by Lemma 5.1 we have $d_K = D_f = (s^2 - 4)^2(5 + 2s)(5 - 2s)$. For a positive integer s bigger than 3, D_1 is positive and D_2 is negative, by Lemma 5.1, $(r_1, r_2) = (2, 1)$ and MK/\mathbb{Q} is a D_4 Galois extension.

Nakamura showed for the field generated by $f(x, t)$,

$$\begin{aligned} \frac{QR_K}{R_F} &= \frac{1}{3} \log \frac{|d_K|}{4} + o(1), \\ R_F &= \frac{1}{2} \log d_F + o(1) \end{aligned}$$

as $|d_K|$ and $d_F \rightarrow \infty$. Here Q is 1 or 2 depending on K and F . Hence $R_K \ll (\log |d_K|)^2$.

The Ferrari resolvent of $f(x, s)$ is

$$y^3 - 3y^2 + (s^2 - 4)y - 2(s^2 - 6) = (y - 2)(y^2 - y + (s^2 - 6)).$$

Then $\text{disc}(f(x, s))(4\beta + c_1^2 - 4c_2) = (s^2 - 4)^3(5 + 2s)(5 - 2s) \notin (\overline{\mathbb{Q}}(s)^*)^2$ and $(\mathbb{Q}(s)^*)^2$. Hence $f(x, s)$ gives rise to a D_4 regular extension over $\mathbb{Q}(s)$. So we can define M, s_M and a set $L(X)$ of square-free integers:

$$L(X) = \left\{ \frac{X}{2} < s < X \mid (s^2 - 4)(25 - 4s^2) \text{ square-free, } s \equiv s_M \pmod{M} \right\}.$$

For $s \in L(X)$, $s^2 - 4$ is the Artin conductor of the one-dimensional representation and $|(s^2 - 4)(25 - 4s^2)|$ is the Artin conductor of the two-dimensional representation. Hence we can apply Theorem 3.1 to $L(X)$.

Theorem 5.2 implies

$$|L(X)| = \prod_{p \nmid M} \left(1 - \frac{\rho(p^2)}{p^2}\right) \frac{X}{2M} + O\left(\frac{X}{M(\log \frac{X}{M})}\right) \gg X^{1-\epsilon},$$

and we have

Theorem 5.4. *There is a constant $c > 0$ such that there exist $K \in \mathfrak{K}(4, D_4, 2, 1)$ with arbitrarily large discriminant d_K for which*

$$h_K > cd_K^{1/2} \frac{(\log \log |d_K|)^3}{(\log |d_K|)^2}.$$

5.3. D_4 extension with the signature (4,0). we specify that $u = -1, t = 1$ and $s > 6$. Then we have $f(x, s) = x^4 - sx^3 - x^2 + sx + 1$ and $D_1 = s^2 - 4$ and $D_2 = 9 + 4s^2$. Assume that D_1 and D_2 are square-free for odd integer s . Then $d_F = D_1, d_L = D_2$ and by Lemma 5.1 we have $d_K = D_f = (s^2 - 4)^2(9 + 4s^2)$. For square-free $s^2 - 4$ and $4s^2 + 9, K, L$ are always distinct. Hence, by Lemma 5.1, $(r_1, r_2) = (4, 0)$ and MK/\mathbb{Q} is a D_4 Galois extension.

Nakamura showed for the field generated by $f(x, t)$,

$$\begin{aligned} \frac{QR_K}{R_F} &= \frac{1}{18} \log \frac{d_K}{4} \log \frac{d_F}{2^{10}} + o(1) \\ R_F &= \frac{1}{2} \log d_F + o(1) \end{aligned}$$

as d_K and $d_F \rightarrow \infty$. Here Q is 1 or 2 depending on K and F .

Hence $R_K \ll (\log |d_K|)^3$. The Ferrari resolvent of $f(x, s)$ is

$$y^3 + y^2 - (s^2 + 4)y - 2(s^2 + 2) = (y + 2)(y^2 - y - (s^2 + 2)).$$

Then $\text{disc}(f(x, s))(4\beta + c_1^2 - 4c_2) = (s^2 - 4)^3(9 + 4s^2) \notin (\overline{\mathbb{Q}}(s)^*)^2$ and $(\mathbb{Q}(s)^*)^2$. Hence $f(x, s)$ gives rise to a D_4 regular extension over $\mathbb{Q}(s)$. We can define M, s_M a set $L(X)$ of square-free integers:

$$L(X) = \left\{ \frac{X}{2} < s < X \mid (s^2 - 4)(4s^2 + 9) \text{ square-free, } s \equiv s_M \pmod{M} \right\}.$$

Since $4s^2 + 9$ is irreducible, we cannot apply Theorem 5.2 to $L(X)$. Nair also showed

Theorem 5.5 (Nair). *If $f(x) = \prod_{i=1}^m (f_i(x))^{\alpha_i} \in \mathbb{Z}[x]$, where each f_i is irreducible, $\alpha = \max_i \alpha_i$ and $\deg f_i(x) = g_i$, then*

$$N_k(x, h) = \prod_p \left(1 - \frac{\rho(p^k)}{p^k}\right) h + O\left(\frac{h}{(\log h)^{k-1}}\right)$$

for $h = x^\theta$ where $0 < \theta < 1$ and $k \geq \max_i \{\lambda g_i \alpha_i\}$, ($\lambda = \sqrt{2} - 1/2$) provided that at least one $g_i \geq 2$.

Theorem 5.5 implies that $|L(X)| \gg X^{1-\epsilon}$. For $s \in L(X)$, $s^2 - 4$ is the Artin conductor of the one-dimensional representation and $(s^2 - 4)(4s^2 + 9)$ is the Artin conductor of the two-dimensional representation. Hence we can apply Theorem 3.1 to $L(X)$. We have

Theorem 5.6. *There is a constant $c > 0$ such that there exist $K \in \mathfrak{R}(4, D_4, 4, 0)$ with arbitrarily large discriminant d_K for which*

$$h_K > cd_K^{1/2} \frac{(\log \log d_K)^3}{(\log d_K)^3}.$$

6. D_3 extensions with signature (1, 1)

We consider a family of non-abelian cubic fields with signature (1, 1) with the largest possible class numbers. This is different from the one considered in [5]. Our family is the one considered by Ishida [11].

Theorem 6.1 (Ishida). *Let $K_t = \mathbb{Q}(\eta)$ be the cubic field of signature (1, 1), where η is the real root of the cubic equation*

$$x^3 + tx - 1 = 0, \quad (t \in \mathbb{Z}, t \geq 2).$$

If $4t^3 + 27$ is square-free or $t = 3m$ and $4m^3 + 1$ is square-free, then η is the fundamental unit of K .

It is easy to show that the real root η is located between $-\frac{1+\epsilon}{t}$ and $-\frac{1}{t}$ for any $\epsilon > 0$. Hence for t with square-free $4t^3 + 27$, the regulator R_{K_t} is

$$\log t < R_{K_t} < (1 + \epsilon) \log t.$$

Since $d_{K_t} = -(4t^3 + 27)$, $R_{K_t} \ll \log |d_{K_t}|$.

Also it is clear that $x^3 + tx - 1$ gives rise to a regular $D_3 (= S_3)$ extension over $\mathbb{Q}(t)$. Hence we can define t_M and M similarly as before. Define

$$L(X) = \left\{ \frac{X}{2} < t < X \mid 4t^3 + 27 \text{ square-free and } t \equiv t_M \pmod{M} \right\}$$

By the work of Hooley as in section 4, we have $X^{1-\epsilon} \ll |L(X)| \ll X$. Hence we have

Theorem 6.2. *There is a constant $c > 0$ such that there exist $K \in \mathfrak{R}(3, D_3, 1, 1)$ with arbitrarily large discriminant d_K for which*

$$h_K > cd_K^{1/2} \frac{(\log \log d_K)^2}{(\log d_K)}.$$

7. Cyclic extensions

Let $f(x, t) = x^n + a_1(t)x^{n-1} + \dots + a_{n-1}(t)x \pm 1$ be an irreducible polynomial over $\mathbb{Q}(t)$ such that $a_i(t) \in \mathbb{Z}[t]$. Suppose $f(x, t)$ gives rise to a cyclic extension over $\mathbb{Q}(t)$, and if $t \in \mathbb{Z}$, it gives rise to a totally real extension over \mathbb{Q} . For each integer $t > 0$, let K_t be the cyclic extension over \mathbb{Q} . Let $Gal(K_t/\mathbb{Q}) = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$. Let θ be a root of $f(x, t)$. Then $\theta, \sigma(\theta), \dots, \sigma^{n-1}(\theta)$ are roots of $f(x, t)$.

We show that if $n = p$ is a prime, $\sigma(\theta), \dots, \sigma^{p-1}(\theta)$ form independent units, and the regulator of K_t is small. By definition, the regulator of $\mathbb{Z}[\theta]$ is

$$R = |\det(\log |\sigma^{i+j}(\theta)|)_{1 \leq i, j \leq p-1}|.$$

Theorem 7.1. (1) $R \neq 0$, and (2) $R \ll (\log t)^{p-1}$.

Proof. By Lemma 5.26 in [26], we have

$$R = \frac{1}{p} \prod_{\chi \neq 1} \left(\sum_{i=0}^{p-1} \chi(\sigma^i) \log |\sigma^i(\theta)| \right),$$

where the product runs over the nontrivial characters of $Gal(K_t/\mathbb{Q})$.

Since $t^{-c} \ll \sigma^i(\theta) \ll t^d$ for some $c, d > 0$ depending only on $f(x, t)$, $|\log |\sigma^i(\theta)|| \ll \log t$. Hence (2) follows.

Since $\theta \cdot \sigma(\theta) \cdots \sigma^{p-1}(\theta) = \pm 1$,

$$\log |\theta| + \log |\sigma(\theta)| + \dots + \log |\sigma^{p-1}(\theta)| = 0.$$

Hence we write

$$\sum_{i=0}^{p-1} \chi(\sigma^i) \log |\sigma^i(\theta)| = \sum_{i=1}^{p-1} (\chi(\sigma^i) - 1) \log |\sigma^i(\theta)|.$$

Since p is a prime, by [7], $\sigma(\theta), \dots, \sigma^{p-1}(\theta)$ are multiplicatively independent. Hence $\log |\sigma(\theta)|, \dots, \log |\sigma^{p-1}(\theta)|$ are linearly independent over \mathbb{Q} . By Baker's theorem [1], they are linearly independent over $\overline{\mathbb{Q}}$.

Since $\chi(\sigma^i)$ are roots of unity and $\chi \neq 1$, one of $\chi(\sigma^i) - 1$ is not zero. Hence

$$\sum_{i=1}^{p-1} (\chi(\sigma^i) - 1) \log |\sigma^i(\theta)| \neq 0.$$

□

Remark 7.1. If n is not a prime, we still have $R \ll (\log t)^{n-1}$. However, $R = 0$ for a composite number n . We show this for simplest quartic and sextic fields. Duke [4] proved that cyclic cubic fields given by $f(x, t) = x^3 - tx^2 - (t + 3)x - 1$ (studied by D. Shanks) have the smallest possible regulators.

7.1. Cyclic quartic fields. Consider totally real cyclic quartic fields K_t generated by a root of

$$f(x, t) = x^4 - tx^3 - 6x^2 + tx + 1, \quad t \in \mathbb{Z}^+.$$

Here $\text{Disc}(f(x, t)) = 4(t^2 + 16)^3$.

We can express the 4 roots of $f(x, t)$ explicitly.

$$\theta_{1,2,3,4} = \pm \frac{\sqrt[4]{t^2 + 16} \sqrt{\sqrt{t^2 + 16} \pm t}}{2\sqrt{2}} \pm \frac{\sqrt{t^2 + 16}}{4} + \frac{t}{4}, \quad t \neq 0, 3$$

where the second and third ambiguous signs agree.

Let θ_1 be the largest root by choosing $+$ for all signs. The Galois group action on the roots is given by

$$\sigma : \theta_j \mapsto \frac{\theta_j - 1}{\theta_j + 1} = \theta_{j+1}, \quad j = 1, 2, 3, 4.$$

Now $\theta_1, \theta_2 = \sigma(\theta_1)$ and $\theta_3 = \sigma^2(\theta_1)$ are not multiplicatively independent. The regulator

$$R = \frac{1}{4} \prod_{\chi \neq 1} \left(\sum_{i=0}^3 \chi(\sigma^i) \log |\sigma^i(\theta)| \right)$$

vanishes because the term corresponding to $\chi(\sigma) = e^{\pi i}$ is zero.

It is known that θ_1, θ_2 and ϵ_t are independent units where ϵ_t is the fundamental units of $\mathbb{Q}(\sqrt{t^2 + 16})$ (See p.10 in [16]). When t is even, we can find ϵ_t .

Proposition 7.1 (Lazarus). *When t is even, ϵ_t is given by*

$$\epsilon_t = \begin{cases} \frac{t/2 + \sqrt{(t/2)^2 + 4}}{2}, & t \equiv 2 \pmod{4} \\ \frac{1 + \sqrt{5}}{2}, & t = 8 \\ (t/4) + \sqrt{(t/4)^2 + 1}, & \text{otherwise.} \end{cases}$$

We replace t in $f(x, t)$ by $2t$ because it is convenient to consider only even t . Then

$$f(x, t) = x^4 - 2tx^3 - 6x^2 + 2tx + 1$$

with $\text{disc}(f(x, t)) = 2^8(t^2 + 4)^3$. When $t^2 + 4$ is square-free, the field discriminant d_{K_t} equals $2^4(t^2 + 4)^3$, and K_t has the unique quadratic subfield $M_t = \mathbb{Q}(\sqrt{t^2 + 4})$. Let $H \simeq C_2$ be the unique subgroup of order 2 in C_4 . Then $\text{Ind}_H^{C_4} 1_H = 1 + \chi^2$ where χ the generator of the group of characters for C_4 . Hence the Artin conductor $f(\chi^2)$ of χ^2 equals $t^2 + 4$ when $t^2 + 4$ is square-free. Since $d_{K_t} = f(\chi)f(\chi^2)f(\chi^3)$ and $\chi^3 = \bar{\chi}$, we have $f(\chi) = f(\chi^3) = 2^2(t^2 + 4)$.

Hence by Proposition 7.1, when $t^2 + 4$ is square-free, the regulator R_{K_t} is given by $R_{K_t} \ll \log^3 t$. Since $d_{K_t} = 2^4(t^2 + 4)^3$,

$$R_{K_t} \ll (\log d_{K_t})^3.$$

From the root formula for $f(x, t)$, it is clear that $f(x, t)$ gives rise to a C_4 regular extension over $\mathbb{Q}(t)$.

Let

$$L(X) = \left\{ \frac{X}{2} < t < X \mid t^2 + 4 \text{ square-free, } t \equiv t_M \pmod{M} \right\}$$

where t_M and M are defined similarly as before. Then we have $X^{1-\epsilon} \ll |L(X)| \ll X$. Since the Artin conductors of the characters for the simplest quartic fields are increasing functions in t , they satisfy the hypothesis in Theorem 3.1. Hence we have

Theorem 7.2. *There is a constant $c > 0$ such that there exist $K \in \mathfrak{K}(4, C_4, 4, 0)$ with arbitrarily large discriminant d_K for which*

$$h_K > cd_K^{\frac{1}{2}} \frac{(\log \log d_K)^3}{(\log d_K)^3}.$$

7.2. Cyclic quintic fields. Emma Lehmer [17] introduced a family of quintic polynomials $f(x, t)$ for $t \in \mathbb{Z}$:

$$f(x, t) = x^5 + t^2x^4 - (2t^3 + 6t^2 + 10t + 10)x^3 + (t^4 + 5t^3 + 11t^2 + 15t + 5)x^2 + (t^3 + 4t^2 + 10t + 10)x + 1.$$

It is easy to show that $f(x, t)$ is irreducible for all $t \in \mathbb{Z}$ when we observe it modulo 2. And it is also known that the zeros of $f(x, t)$ generate a cyclic extension K_t of degree 5 over \mathbb{Q} . Here $Disc(f(x, t)) = (t^3 + 5t^2 + 10t + 7)^2(t^4 + 5t^3 + 15t^2 + 25t + 25)^4$.

Let $G = Gal(K_t/\mathbb{Q})$ be the Galois group and σ be a generator of G given by

$$\sigma(\theta) = \frac{(t + 2) + t\theta - \theta^2}{1 + (t + 2)\theta}$$

for a root θ of $f(x, t)$. For the details, we refer to [21]. Also it is obvious that the Galois groups of $f(x, t)$ over $\mathbb{Q}(t)$ and over $\overline{\mathbb{Q}}(t)$ are both C_5 generated by σ . Hence $f(x, t)$ gives rise to a regular C_5 extension over $\mathbb{Q}(t)$.

Schoof and Washington studied these simplest quintic fields when $P_t = t^4 + 5t^3 + 15t^2 + 25t + 25$ is a prime number. When P_t is a prime, then the zeros of $f(x, t)$ form a fundamental system of units in K_t . Gaál and Pohst extended this result for square-free P_t (see the proof of Theorem 3.5 in [21]).

In this case, by Theorem 7.1, $R_{K_t} \ll (\log t)^4$. It also follows from [21]: Let U denote the group of units generated by the zeros modulo $\{\pm 1\}$. Define $i_\theta = [O_{K_t}^*/\{\pm 1\} : U]$. Schoof and Washington [21] showed that $i_\theta \leq 11$ if $|t + 1| \geq 20$ and

$$R = |\det(\log |\sigma^{i+j}(\theta)|)_{1 \leq i, j \leq 4}| \leq \left(71 + \frac{36}{\log |t + 1|} \right) \log^4 |t + 1|.$$

Jeannin [12] found the prime factorization of P_t .

Theorem 7.3 (Jeannin). *The number P_t is written in a unique way: $P_t = 5^c q^5 \prod_{i=1}^n p_i^{x_i}$, $c \in \{0, 2\}$, $q \in \mathbb{N}$, p_i distinct primes, $x_i \in [1, 4]$. So the conductor of K_t is $f_t = 5^c \prod_{i=1}^n p_i$.*

Especially if P_t is cube-free, then $P_t = 5^c \prod_{i=1}^n p_i^{x_i}$ and $x_1 = 1$ or 2 and

$$t^4 \ll P_t \leq 5^c \left(\prod_{i=1}^n p_i\right)^2 \leq d_{K_t}$$

since $d_{K_t} = f_t^4$. Hence for cube-free P_t , when we combine all these arguments, we have

$$R_{K_t} \ll \log^4(d_{K_t}).$$

Let $L(X)$ be a finite set given by

$$L(X) = \left\{ \frac{X}{2} < t < X \mid P_t \text{ cube-free and } t \equiv t_M \pmod{M} \right\}.$$

Then by [10], page 69, we have $X^{1-\epsilon} \ll |L(X)| \ll X$.

For cyclic extensions of prime degree, the conductor of a cyclic extension equals the Artin conductors of characters for the extension. We showed that the product of prime divisors of $P_t = t^4 + 5t^3 + 15t^2 + 25t + 25$ is the conductor. But it would be possible that the sets of distinct prime divisors of P_t coincide for different t 's. Let $\nu(n)$ is the number of distinct prime divisors of n . For each t , the number of possible repetition is bounded by $2^{\nu(P_t)}$ because we assume that P_t is cube-free. It is known that $\nu(n) \ll \frac{\log n}{\log \log n}$. (See page 167 in [20]) Hence, for all $t < X$, $2^{\nu(P_t)} \ll 2^{\frac{\log X}{\log \log X}} \ll X^\epsilon$. After removing the possible repetition, we can say that the Artin conductors are distinct.

Hence we have

Theorem 7.4. *There is a constant $c > 0$ such that there exist $K \in \mathfrak{K}(5, C_5, 5, 0)$ with arbitrarily large discriminant d_K for which*

$$h_K > cd_K^{1/2} \frac{(\log \log d_K)^4}{(\log d_K)^4}.$$

7.3. Cyclic sextic fields. It was Gras [9] who introduced the simplest sextic polynomial $f(x, t)$ first, given by

$$f(x, t) = x^6 - \frac{t-6}{2}x^5 - 5\frac{t+6}{4}x^4 - 20x^3 + 5\frac{t-6}{4}x^2 + \frac{t+6}{2}x + 1$$

and discriminant of $f(x, t)$ is $\frac{3^6}{2^{14}}(t^2 + 108)^5$.

Let $K_t = \mathbb{Q}(\theta)$, where θ is a root of $f(x, t)$. She showed the following properties:

- (1) If $t \in \mathbb{Z} - \{0, \pm 6, \pm 26\}$, then $f(x, t)$ is irreducible in $\mathbb{Q}[X]$, and K_t is a real cyclic sextic field; a generator σ of its Galois group is characterized by the relation $\sigma(\theta) = (\theta - 1)/(\theta + 2)$. We have $K_{-t} = K_t$ for all $t \in \mathbb{Z}$, and we can suppose that $t \in \mathbb{N} - \{0, 6, 26\}$.
- (2) The quadratic subfield of K_t is $k_2 = \mathbb{Q}(\sqrt{t^2 + 108})$.
- (3) The cubic field of K_t is $k_3 = \mathbb{Q}(\phi)$, where

$$\phi = \theta^{-1-\sigma^3} = -\frac{2\theta + 1}{\theta(\theta + 2)}$$

and

$$\text{Irr}(\phi, \mathbb{Q}) = x^3 - \frac{t-6}{4}x^2 - \frac{t+6}{4}x - 1;$$

the discriminant of this polynomial is $((t^2 + 108)/16)^2$. If $t \equiv 2 \pmod{4}$, k_3 is the simplest cubic field.

- (4) The conductor f of K_t is given by the following procedure: Let m be the product of primes, different from 2 and 3, dividing $t^2 + 108$ with an exponent not congruent to 0 modulo 6. Then $f = 4^k 3^l m$, where

$$k = \begin{cases} 0, & t \equiv 1 \pmod{2} \text{ or } t \equiv \pm 6 \pmod{16} \\ 1, & \text{otherwise} \end{cases}, \quad l = \begin{cases} 0, & t \equiv 1 \pmod{3} \\ 1, & t \equiv 0 \pmod{27} \\ 2, & \text{otherwise} \end{cases}$$

As in the case of simplest quartic fields, $\theta, \sigma(\theta), \sigma^2(\theta), \sigma^3(\theta)$ and $\sigma^4(\theta)$ do not form independent units. The regulator

$$R = \frac{1}{6} \prod_{\chi \neq 1} \left(\sum_{i=0}^5 \chi(\sigma^i) \log |\sigma^i(\theta)| \right)$$

vanishes because the term corresponding to $\chi(\sigma) = e^{\pi i}$ is zero.

Let

$$S(X) = \left\{ 0 < r < X \mid (3r^2 + 3r + 1)(12r^2 + 12r + 7) \text{ square-free} \right\}.$$

For all $r \in S(X)$, let $t = (6r + 3)(36r^2 + 36r + 18)$ and we consider fields $L_r = K_t = \mathbb{Q}(w)$ where $w = \theta^{1-\sigma^3} = -\frac{\theta(2\theta+1)}{\theta+2}$. We note that $t^2 + 108 = 432(12r^2 + 12r + 7)(3r^2 + 3r + 1)^2$. Then there exists a unit v such that $w = v^{1+\sigma}$. Hence $v = \frac{(w+1)-\sqrt{(w+1)^2-8w}}{2}$. Gras showed that if $r \in S(X)$, then the conductor of k_2 is $f_2 = 36r^2 + 36r + 21$, and the fundamental unit of k_2 is

$$\epsilon_2 = \frac{(12r^2 + 12r + 5) + (2r + 1)\sqrt{36r^2 + 36r + 21}}{2}.$$

By Proposition 1 in [27], the conductor of k_3 is $(3r^2 + 3r + 1)(12r^2 + 12r + 7)$. By the above property (4), if $r \in S(X)$, the conductor f_6 of K_t is $3(12r^2 + 12r + 7)(3r^2 + 3r + 1)$.

Let σ be the generator of $Gal(K_t/\mathbb{Q}) \simeq C_6$, $k_3 = K_t^{\langle \sigma^3 \rangle}$ and $k_2 = K_t^{\langle \sigma^2 \rangle}$. Let χ be the generator of the group of characters for $Gal(K_t/\mathbb{Q})$ with $\chi(\sigma) = e^{2\pi i/6}$. Then $Ind_{\langle \sigma^2 \rangle}^{\langle \sigma \rangle} 1_{\langle \sigma^2 \rangle} = 1_{\langle \sigma \rangle} + \chi^3$, $Ind_{\langle \sigma^3 \rangle}^{\langle \sigma \rangle} 1_{\langle \sigma^3 \rangle} = 1_{\langle \sigma \rangle} + \chi^2 + \chi^4$ and $Ind_{\langle \sigma^3 \rangle}^{\langle \sigma \rangle} \varphi = 1_{\langle \sigma \rangle} + \chi + \chi^5$ where φ is the non-trivial character for $\langle \sigma^3 \rangle$. Hence the Artin conductor of χ^3 equals the field discriminant of k_2 , which is $3(12r^2 + 12r + 7)$, and the Artin conductors of χ^2 and χ^4 are both $(3r^2 + 3r + 1)(12r^2 + 12r + 7)$. The Artin conductors of χ and χ^5 equals $(3r^2 + 3r + 1)(12r^2 + 12r + 7)\sqrt{N(\mathfrak{b})}$ where \mathfrak{b} is the Artin conductor of φ . Since the Artin conductors of χ and χ^5 are divisors of f_6 , $\sqrt{N(\mathfrak{b})}$ is at most 3. Hence we verified that the hypothesis of Theorem 3.1 is satisfied.

Since $t = (6r + 3)(36r^2 + 36r + 18) \equiv 2 \pmod 4$, the field k_3 is a simplest cubic field. Hence for $r \in S$, we have an explicit system of fundamental units:

$$\{\epsilon_2, \tau, \tau^\sigma, v, v^\sigma\}$$

where τ is a root of $x^3 - \frac{t-6}{4}x^2 - \frac{t+6}{4}x - 1$. Hence for $t = (6r + 3)(36r^2 + 36r + 18)$ with $r \in S(X)$, the regulator $R_{K_t} \ll (\log d_{K_t})^5$.

Now we show that $f(x, (6r + 3)(36r^2 + 36r + 18))$ gives rise to a regular C_6 extension over $\mathbb{Q}(r)$. If θ_r is a root of $f(x, (6r + 3)(36r^2 + 36r + 18))$, then it is clear $\mathbb{Q}(r)(\theta_r)$ is the splitting field of $f(x, (6r + 3)(36r^2 + 36r + 18))$ over $\mathbb{Q}(r)$ with Galois group $C_6 = \langle \sigma \rangle$. By the same argument, the Galois group of $f(x, (6r + 3)(36r^2 + 36r + 18))$ over $\overline{\mathbb{Q}}(t)$ is also $C_6 = \langle \sigma \rangle$. Hence the claim follows.

Now define

$$L(X) = \left\{ \frac{X}{2} < r < X \mid \begin{array}{l} (3r^2 + 3r + 1)(12r^2 + 12r + 7) \text{ square-free,} \\ r \equiv r_M \pmod M \end{array} \right\}$$

where r_M and M are defined similarly as before and we can show that $X^{1-\epsilon} \ll |L(X)| \ll X$. Hence we have

Theorem 7.5. *There is a constant $c > 0$ such that there exist $K \in \mathfrak{K}(6, C_6, 6, 0)$ with arbitraril large discriminant d_K for which*

$$h_K > cd_K^{1/2} \frac{(\log \log d_K)^5}{(\log d_K)^5}.$$

Remark 7.2. We could not find in the literature a family of polynomials of degree 7, $f(x, t) = x^7 + a_1(t)x^6 + \dots + a_6(t)x \pm 1$, where $a_i(t) \in \mathbb{Z}[t]$ which generate cyclic extensions of degree 7. By Theorem 7.1, such a family would provide a family of cyclic extensions of degree 7 with the largest possible class numbers.

Remark 7.3. Silverman [25] obtained a lower bound of regulator R_K of number fields K : $R_K \gg (\log |d_K|)^{r-r_0}$, where $r = r_1 + r_2 - 1$ and r_0 is the maximum of unit ranks of subfields of K . However, in the above examples

where $f(x, t)$ gives rise a regular Galois extension over $\mathbb{Q}(t)$, the regulator R_{K_t} satisfies

$$R_{K_t} \gg (\log |d_{K_t}|)^r.$$

We conjecture that this is always sharp in the case of regular Galois extensions. The CM field $K_t = \mathbb{Q}(\sqrt{\alpha - t})$, where α is an algebraic integer, given in [6], does not give rise to a regular Galois extension over $\mathbb{Q}(t)$, since $\mathbb{Q}(\alpha) \subset K_t$.

Remark 7.4. Shen [24] considered a parametric polynomial $f(x, t)$ generating real cyclic octic fields:

$$f(x, t) = x^8 - 8tx^7 - 28x^6 + 56tx^5 + 70x^4 - 56tx^3 - 28x^2 + 8tx + 1.$$

However, this polynomial does not give rise to a regular extension over $\mathbb{Q}(t)$, since $\mathbb{Q}(\sqrt{2}) \subset K_t$, where K_t is the splitting field of $f(x, t)$ (See Theorem 1 in [24]). So this polynomial is not suitable for our purpose.

References

- [1] A. BAKER, *Linear forms in the logarithms of algebraic numbers I*. *Mathematika* **13** (1966), 204–216.
- [2] P. J. CHO AND H. H. KIM, *Application of the strong Artin conjecture to class number problem*. To appear in *Can. J. Math.*
- [3] D. COX, *Galois Theory*. Wiley, 2004.
- [4] W. DUKE, *Number fields with large class groups*. Number theory, 117–126, CRM Proc. Lecture Notes, **36**, Amer. Math. Soc., Providence, RI, 2004.
- [5] R. C. DAILED A, *Non-abelian number fields with very large class numbers*. *Acta Arith.* **125** (2006) no.3 , 215–255.
- [6] R. C. DAILED A, R. KRISHNAMOORTHY, AND A. MALYSHEV, *Maximal class numbers of CM number fields*. *J. Number Theory* **130** (2010), 936–943.
- [7] M. DRMOTA AND M. SKALBA, *On multiplicative and linear independence of polynomial roots*. *Contributions to general algebra* **7**, Vienna, 1991, 127–135.
- [8] V. ENNOLA, S. MAKI, AND T. TURUNEN, *On real cyclic sextic fields* *Math. Comp.* Vol **45** (1985), 591–611.
- [9] M.-N. GRAS, *Special Units in Real Cyclic sextic Fields*. *Math. Comp.* **48** (1987) no.177, 179–182.
- [10] C. HOOLEY, *Applications of sieve methods to the theory of numbers*. Cambridge; New York: Cambridge University Press, 1976.
- [11] M. ISHIDA, *Fundamental Units of Certain Number Fields*. *Abh. Math. Sem. Univ. Hamburg.* **39** (1973), 245–250.
- [12] S. JEANNIN, *Nombre de classes et unités des corps de nombres cycliques quintiques d'E. Lehmer*. *J. Theor. Nombres Bordeaux* **8** (1996), no. 1, 75–92.
- [13] C. JENSEN, A. LEDET AND N. YUI, *Generic Polynomials; Constructive Aspects of the Inverse Galois Problem*. *Mathematical Sciences Research Institute Publications* **45**, Cambridge University Press 2002.
- [14] E. KOWALSKI AND P. MICHEL, *Zeros of families of automorphic L-functions close to 1*. *Pacific J. Math.* **207** (2002), no.2, 411–431.
- [15] M. J. LAVALLEE, B. K. SPEARMAN, K. S. WILLIAMS AND Q. YANG, *Dihedral Quintic Fields With A Power Basis*. *Math J. Okayama Univ.* **47** (2005), 75–79.
- [16] A. J. LAZARUS, *The Class Numbers and Cyclotomy of Simplest Quartic Fields*. PhD thesis, University of California, Berkeley, 1989.
- [17] E. LEHMER, *Connection between Gaussian periods and cyclic units*. *Math. Comp.* **50** (1988) no. 182, 341–355.

- [18] M. NAIR, *Power Free Values of Polynomials*. *Mathematika* **23** (1976), 159–183.
- [19] K. NAKAMULA, *Certain Quartic Fields with Small Regulators*. *J. Number Theory* **57** (1996), no.1, 1–21.
- [20] J. SANDOR, D. S. MITRINOVIC AND B. CRSTICI, *Handbook of Number Theory I*. 1st edn, Springer-Netherlands (1995).
- [21] R. SCHOOF AND L. WASHINGTON, *Polynomials and Real Cyclotomic Fields with Large Class Number*. *Math. Comp.* **50** (1988) no. 182, 543–556.
- [22] A.M. SCHÖPP, *Fundamental units in a parametric family of not totally real quintic number fields*. *J. de Theorie des Nom. de Bordeaux*, **18** (2006), no. 3, 693–706.
- [23] J.P. SERRE, *Topics in Galois Theory*. Research Notes in Mathematics, A K Peters, Ltd. 2008.
- [24] Y.-Y. SHEN, *Unit groups and class numbers of real cyclic octic fields*. *Trans. Amer. Math. Soc.* **326** (1991), no. 1, 179–209.
- [25] J.H. SILVERMAN, *An inequality relating the regulator and the discriminant of a number field*. *J. Number Theory* **19** (1984), no. 3, 437–442.
- [26] L.C. WASHINGTON, *Introduction to Cyclotomic Fields*. Graduate Texts in Math., vol 83, Springer-Verlag, New York, 1982.
- [27] L.C. WASHINGTON, *Class numbers of the simplest cubic fields*. *Math. Comp.* **48** (1987), no. 177, 371–384.

Peter J. CHO
Department of Mathematics
University of Toronto
Toronto ON M5S 2E4 Canada
E-mail: jcho@math.toronto.edu

Henry H. KIM
Department of Mathematics
University of Toronto
Toronto ON M5S 2E4 CANADA
and Korea Institute for Advanced Study
E-mail: henrykim@math.toronto.edu