数理解析研究所講究録
第837巻 1993年 130-141

On Certain Number Fields with Small Regulators

東京都立大学 理学部　　中村 憲 (Ken Nakamula)

1. Introduction.

Motivation. In [3] and [4], we have given a general effective algorithm called *cyclo-elliptic method* (cf. [5]) to compute the class number of any subfield of an abelian extension of an imaginary quadratic field. To get the computational time complexity of the cyclo-elliptic method, two estimations are required. One is to majorize the size of cyclotomic or elliptic units. The other is to minorize the regulator of a number field. In both cases, it is desirable from our viewpoint to estimate without using the class number. While, the latter arises from any method of computing fundamental units and has been treated by several authors. In particular, explicit fundamental units have been obtained when one could construct a family of fields with regulator as small as possible. It is not still clear what is the smallest possible regulator if we omit the class number as parameter. So some detailed study to find fields with small regulators will give us new information on the behaviour of the regulator.

Notation. We prepare a few symbols used throughout.

F	a subfield of $\mathbf{C}$ of degree finite over $\mathbf{Q}$
$n = n(F)$	the degree of $F/\mathbf{Q}$
$r = r(F)$	the unit rank of F
$R = R_F$	the regulator of F
$D = D_F$	the discriminant of F
h	the class number of F

Fix $n > 1$ and r. Once R is known exactly, evaluation of h is reduced to that of ζ-functions. In the simplest case where $(n, r) = (2, 0)$, we have $R = 1$ and

$$h|D|^{-1/2}w^{-1} = \frac{1}{2\pi}L\left(1, \left(\frac{D}{\cdot}\right)\right).$$

Here w is the number of roots of 1 in F and $\left(\frac{D}{\cdot}\right)$ is the Kronecker symbol. Moreover, an asymptotic behaviour of h is derived only from that of R by the Brauer-Siegel theorem

$$\log(hR) \sim \frac{1}{2}\log|D| \quad (|D| \to \infty).$$

We are interested in small R, i.e. large h. How small does R become? We are going to consider the following problem.

Problem. Fixing $n > 1$ and r, minorize R by an explicit function B of D, and construct infinitely many F so that R is asymptotically equal to B as $|D| \to \infty$.

Application. Before going into this problem, we refer to some related useful facts on such number fields with small regulators. Namely, important invariants of those constructed F are known together.

1. An integral basis of F is given. Because, we usually search a unit with discriminant exactly D to find units with small logarithmic norm, and then we obtain a power integral basis.

2. Fundamental units of F are given. Because, we always get a set S of units of F with regulator $R' = R_F(S)$ close to B, in most cases $2B > R'$, and then $R' = R$ since $2R > R' \geq R$, hence S is a set of fundamental units.

3. Therefore it is not so difficult to compute the ideal class group of F. Especially h is known by evaluating ζ-functions. As is mentioned above, we obtain infinitely many examples of F with the largest possible h.

2. Known Examples.

Let us first give known results to see what is explained in the introduction much better.

Case $(n,r) = (2,1)$. For real quadratic fields, the answer is complete as follows, see for example Pohst [7]. A minorization is given by

$$\begin{aligned} R &\geq \log \frac{D^{1/2} + (D-4)^{1/2}}{2} \\ &= \frac{1}{2} \log D + o(1) \quad (D \to \infty). \end{aligned}$$

In this minorization, the equality holds if and only if $D = s^2 + 4$ with $s \in \mathbf{N}$, narrow R-D type. This type of F is studied by many authors. There are infinitely many such F. For

these F, we have

$$hD^{-1/2}\log\frac{D^{1/2}+(D-4)^{1/2}}{2}=\frac{1}{2}L\left(1,\left(\frac{D}{\cdot}\right)\right)$$

and

$$\log h\sim\frac{1}{2}\log D\quad(D\to\infty).$$

Case $(n,r)=(3,1)$. For cubic fields with $D<0$, the following minorization is given by Artin, see for example [2].

$$\begin{aligned}R &> \frac{1}{3}\log\frac{|D+24|}{4}\\ &= \frac{1}{3}\log\frac{|D|}{4}+o(1)\quad(|D|\to\infty).\end{aligned}$$

For this minorization, a family of F with R asymptotically equal to the lower bound is constructed and studied by Ishida [2]. Namely, let $F=\mathbf{Q}(\varepsilon)$, $\varepsilon>1$, $f(\varepsilon)=0$, where

$$f=X^3-sX^2-1$$

with $s\in\mathbf{N}$ such that $D=-4s^3-27$ and $R=\log\varepsilon$. Then

$$R=\frac{1}{3}\log\frac{|D|}{4}+o(1)\quad(|D|\to\infty).$$

There are infinitely many such F. To compute h, we can use the formula

$$h|D|^{-1/2}R=\frac{1}{2\pi}L_{\mathbf{Q}(\sqrt{D})}(1,\chi).$$

Here χ is a Hecke character corresponding to the cyclic extension $F\left(\sqrt{D}\right)$ of $\mathbf{Q}\left(\sqrt{D}\right)$.

We also have

$$\log h\sim\frac{1}{2}\log|D|\quad(|D|\to\infty).$$

Case $(n,r) = (3,2)$. For cubic field with $D > 0$, the following minorization is given by Pohst [7].

$$\begin{aligned} R &\geq \frac{1}{16}\log^2\frac{D}{4} + \frac{3}{4}\log^2 x_D \\ &= \frac{1}{16}\log^2\frac{D}{4} + o(1) \quad (D \to \infty). \end{aligned}$$

For this minorization, a family of F, the simplest cubic fields, with R asymptotically equal to the lower bound is constructed and studied by Shanks [8] and others. Namely, let $F = \mathbf{Q}(\varepsilon)$, $\varepsilon > 1$, $f(\varepsilon) = 0$, where

$$f = X^3 - sX^2 - (s+3)X - 1$$

with $s \in \mathbf{N}$ such that $D = (s^2 + 3s + 9)^2$ and $\varepsilon, 1+\varepsilon$ are fundamental units of F. Then

$$R = \frac{1}{16}\log^2 D + o(1) \quad (D \to \infty).$$

There are infinitely many such F. To compute h, we can use the formula

$$h|D|^{-1/2}R = \left|\frac{1}{2}L(1,\chi)\right|^2.$$

Here χ is a Dirichlet character corresponding to the cyclic extension $F/\mathbf{Q}$. We also have

$$\log h \sim \frac{1}{2}\log D \quad (D \to \infty).$$

3. Minorization of R.

Let us now consider general minorization of R. Let r_0 be the maximum of $r(K)$ of all proper subfileds K of F. Then there exist explicit constants c and d depending only on

n such that

$$R > c \log^{r-r_0}(d|D|).$$

This estimate is given by J. H. Silverman [9]. It is conjectured that $r - r_0$ cannot be replaced by a larger exponent when n, r and r_0 are fixed. On the other hand, there is a refined formulation proved by K. Uchida [10]. Let $k > 1$. Further let K be a maximal subfield of F such that

$$n(K)^{-k} \log |D_K| < n^{-k} \log |D|.$$

Then there exist explicit constants c and d depending only on n and k such that

$$R > c \log^{r-r(K)}(d|D|).$$

It is not known whether these estimations cannot be replaced by a better one. Is $r - r_0$ (or $r - r(K)$) best possible? The previous examples show the answer is yes for $n \leq 3$. But, for $n \geq 4$, it seems to be difficult to construct F with R asymptotically attaining these lower bounds. So far, the only known example supporting Silverman's conjecture is given for $(n, r, r_0) = (4, 3, 1)$ by Cusick [1] as follows. Let $F = \mathbf{Q}\left(\sqrt{2}, \sqrt{s^2+1}\right)$, $s \in \mathbf{Z}$, $s > 1$, such that

$$x^2 - 2s^2 = 1 \quad \text{for some} \quad x \in \mathbf{Z}.$$

Then $R = O\left(\log^2 D\right)$. Recall that $R \geq c \log^2 D$ with a constant $c > 0$. The author could not reproduce any proof of the existence of infinitely many such F, and asked it as a question at the talk. After the talk, Ryotaro Okazaki has obtained a proof by means of Thue's theorem.

One of the reasons why it is not so simple to construct infinitely many F for $n \geq 4$ supporting Silverman's conjecture is that the parametric polynomial

$$f = X^n - sX^{n-1} + \cdots \pm 1$$

always has the discriminant of the form

$$D_f = (\pm 1)^{n-2} n^n s^n + \cdots .$$

Note that the degree of D_f in s is equal to n. We usually encounter the next question in the course of constructing such F with small R. Is D_f squarefree for infinitely many $s \in \mathbf{Z}$? As is well known, we do not have a general answer for this when $n \geq 4$. So we shall try to get a sharper estimate of R in a slightly different form for a special case.

Assume $\boxed{n = 4 \text{ and } F \text{ is imprimitive with a quadratic subfield } K}$ from now on. Then we can utilize K. For CM fields, i.e. $r = r_0 = 1$,

$$R \geq \log\left(\frac{3+\sqrt{5}}{2}\right),$$

where the equality holds if and only if $K = \mathbf{Q}\left(\sqrt{5}\right)$, this is of course best possible.

We have $\boxed{(r, r_0) = (1,0),\ (2,1) \text{ or } (3,1)}$ for other cases. Then a minorization of R is given by using D and D_K. Indeed, we can prove that there exist explicit constants c, d and e such that

$$R > c \log^{r-r(K)}(d|D|) \log^{r(K)}(e\,|D_K|).$$

Precise results are stated in [6], see also the theorems below.

We now ask the next question. Is this estimation best possible? The answer is yes as in the following.

4. Quartic Relative Units

Let us define a parametric polynomial giving a quartic relative unit. All examples of F with asymptotically minimal R are obtained from this polynomial. For $s, t, u \in \mathbf{Z}$, $s > 0$, $u^2 = 1$, $(s,t,u) \neq (1,-1,1)$, let

$$f = X^4 - sX^3 + (t+2u)X^2 - usX + 1.$$

Then $D_f = D_1^2 D_2$, where

$$D_1 = s^2 - 4t, \quad D_2 = (t+4u)^2 - 4us^2.$$

Let $F = \mathbf{Q}(\varepsilon)$, $\varepsilon \in \mathbf{C}$, $|\varepsilon| \geq 1$, $f(\varepsilon) = 0$, and

$$K = \mathbf{Q}\left(\sqrt{D_1}\right), \quad L = \mathbf{Q}\left(\sqrt{D_2}\right).$$

Then we have

Proposition 1. *Let $K \neq \mathbf{Q}$, $L \neq \mathbf{Q}$, $D_K = D_1$, $D_L = D_2$. Then F is a non-CM quadratic extension of the quadratic field K, and is non-galois (resp. cyclic) over $\mathbf{Q}$ if $K \neq L$ (resp. $K = L$). Moreover*

$$(r, r_0) = \begin{cases} (1,0) & \text{if } D_1 < 0, \\ (2,1) & \text{if } D_2 < 0, \\ (3,1) & \text{otherwise.} \end{cases}$$

Especially, if $K \neq L$, then $D = D_f$ and, in each case above, there exist infinitely many such F.

Till the end of this section, let the assumption be the same as in the proposition above. If $K \neq L$, the ring of integers of F is given by $\mathbf{Z}[\varepsilon]$. Let $E = E_F$ be the group of units of F, and W the group of roots of 1 in F. Then we obtain explicit fundamental units as follows.

Proposition 2. *Let $D_K < 0$, so $(r, r_0) = (1, 0)$, $t > 0$. Then $E = W \times \langle \varepsilon \rangle$ unless*

$$(s, t, u) = (3, 3, 1), (4, 5, 1), (5, 7, 1), (1, 1, -1).$$

Fixing $(s, u) \in \mathbf{N} \times \{\pm 1\}$, one has

$$R = \frac{1}{4} \log \frac{D}{16} + o(1) \quad \text{as } D \to \infty.$$

Recall $E' := \left\{ \varepsilon \in E \mid \varepsilon > 0,\ N_{F/K}(\varepsilon) = 1 \right\} \cong \mathbf{Z}$, $E' \cap E_K = 1$, and $Q := (E : E' \times E_K) \mid 2$ when $(r, r_0) = (2, 1)$. Then we have

Proposition 3. *Let $D_L < 0$, $(s, t) \neq (1, -5)$, so $(r, r_0) = (2, 1)$, $u = 1$. Then $E' = \langle \varepsilon \rangle$. Fixing $t \in \mathbf{Z} \setminus ((2 + 4\mathbf{Z}) \cup \{0, -4\})$, one has*

$$\frac{QR}{R_K} = \frac{1}{3} \log \frac{|D|}{4} + o(1) \quad \text{as } |D| \to \infty.$$

If $t = \pm 1, (s, t) \neq (3, 1)$, then $E_K = \langle -1, \varepsilon + \varepsilon^{-1} \rangle$, $Q = 1$, $E = \langle -1, \varepsilon, \varepsilon + \varepsilon^{-1} \rangle$, and

$$R_K = \frac{1}{2} \log D_K + o(1) \quad \text{as } D_K \to \infty.$$

We have a similar result when $D_K > 0$ and $D_L > 0$, i.e. $(r, r_0) = (3, 1)$, but is omitted, see [6].

5. Theorems.

Lastly, we state the answer of the problem for imprimitive non-CM quartic fields as theorems.

Theorem 1. *Let* $(r, r_0) = (1, 0)$. *Then there is an explicit minorization* $R \geq B$ *such that*

$$B = \frac{1}{4}\log^2 \frac{D}{16} + o(1) \quad (D \to \infty),$$

and there are infinitely many non-galois F *such that* $\lim_{D\to\infty}(R - B) = 0$, *or equivalently*

$$R = \frac{1}{4}\log^2 \frac{D}{16} + o(1) \quad (D \to \infty).$$

Theorem 2. *Let* $(r, r_0) = (2, 1)$ *and* K *be the quadratic subfield of* F. *Then there are explicit minorizations* $R_K \geq B_1$ *and* $R/R_K \geq B_2$, *so* $R \geq B_1 B_2$, *such that*

$$B_1 = \frac{1}{2}\log D_K + o(1) \quad (D_K \to \infty),$$

$$B_2 = \frac{1}{6}\log \frac{|D|}{4} + o(1) \quad (|D| \to \infty),$$

and there are infinitely many F *such that* $R \sim 2B_1B_2$ *as* D_K, $|D| \to \infty$, *or exactly*

$$R_K = \frac{1}{2}\log D_K + o(1) \quad (D_K \to \infty)$$

$$\frac{R}{R_K} = \frac{1}{3}\log \frac{|D|}{4} + o(1) \quad (|D| \to \infty).$$

Theorem 3. *Let* $(r, r_0) = (3, 1)$. (i) *Let* F *contain a unique quadratic subfield* K. *Then there are explicit minorizations* $R_K \geq B_1$ *and* $R/R_K \geq B_2$, *so* $R \geq B_1 B_2$, *such that*

$$B_1 = \frac{1}{2}\log D_K + o(1) \quad (D_K \to \infty)$$

$$B_2 = \frac{\sqrt{3}}{80}\log^2\frac{D}{16},$$

and there are infinitely many non-galois F *such that* $R \sim \left(20\sqrt{3}/27\right) B_1 B_2$ *as* D_K, $D \to \infty$, *or exactly*

$$R_K = \frac{1}{2}\log D_K + o(1) \quad (D_K \to \infty)$$

$$\frac{R}{R_K} = \frac{1}{36}\log\frac{D}{16}\log\frac{D}{2^{10}} + o(1) \quad (D \to \infty).$$

(ii) The case where F has distinct quadratic subfields K_1, K_2, K_3 is omitted.

Remarks We add a few remarks about the proofs of the theorems.

1. To minorize R, we employ Artin's elementary idea to majorize $|D|$ by a "good" polynomial of a unit.

2. To decide E, we remove finite exceptions with very small regulators (or relative regulators) between R and $2R$ (or R/R_K and $2R/R_K$) by virtue of the obtained lower bounds.

3. To get precise results, symbolic manipulation (computer algebra) is used everywhere.

参考文献

[1] T. W. Cusick. Lower bounds for regulators. In *Number Theory, Noordwijkerhout 1983*, number 1068 in Lect. Notes in Math., pages 63–73. Springer-Verlag, 1984.

[2] M. Ishida. Fundamental units of certain algebraic number fields. *Abh. Math. Semi. Univ. Hamburg*, 39:245–250, 1973.

[3] K. Nakamula. Calculation of the class numbers and fundamental units of abelian extensions over imaginary quadratic fields from approximate values of elliptic units. *J. Math. Soc. Japan*, 37:245–273, 1985.

[4] K. Nakamula. Elliptic units and the class numbers of non-galois fields. *J. Number Theory*, 31:142–166, 1989.

[5] K. Nakamula. Class number computation by cyclotomic or elliptic units. In *Computational Number Theory*, pages 139–162. Walter de Gruyter Verlag, 1991.

[6] K. Nakamula. Imprimitive quartic fields with minimal regulators. Preprint Series 1992: No. 10, Department of Mathematics, Tokyo Metropolitan University, 11 May 1992. (preprint, 15 pp.).

[7] M. Pohst. Regulatorabschätzungen für total reelle algebraische Zahlkörper. *J. Number Th.*, 9:459–492, 1977.

[8] D. Shanks. The simplest cubic fields. *Math. Comp.*, 28:1137–1152, 1974.

[9] J. H. Silverman. An inequality relating the regulator and the discriminant of a number field. *J. Number Th.*, 19:437–442, 1984.

[10] K. Uchida. On Silverman's estimate of regulators. (preprint), 1992.