

## UNIT GROUPS AND CLASS NUMBERS OF REAL CYCLIC OCTIC FIELDS

YUAN-YUAN SHEN

**ABSTRACT.** The generating polynomials of D. Shanks' simplest quadratic and cubic fields and M.-N. Gras' simplest quartic and sextic fields can be obtained by working in the group  $\mathrm{PGL}_2(\mathbf{Q})$ . Following this procedure and working in the group  $\mathrm{PGL}_2(\mathbf{Q}(\sqrt{2}))$ , we obtain a family of octic polynomials and hence a family of real cyclic octic fields. We find a system of independent units which is close to being a system of fundamental units in the sense that the index has a uniform upper bound. To do this, we use a group theoretic argument along with a method similar to one used by T. W. Cusick to find a lower bound for the regulator and hence an upper bound for the index. Via Brauer-Siegel's theorem, we can estimate how large the class numbers of our octic fields are. After working out the first three examples in §5, we make a conjecture that the index is 8. We succeed in getting a system of fundamental units for the quartic subfield. For the octic field we obtain a set of units which we conjecture to be fundamental. Finally, there is a very natural way to generalize the octic polynomials to get a family of real  $2^n$ -tic number fields. However, to select a subfamily so that the fields become Galois over  $\mathbf{Q}$  is not easy and still a lot of work on these remains to be done.

### 1. INTRODUCTION

To calculate the class number of an abelian algebraic number field via the analytic class number formula usually involves a calculation of the regulator of the field, which in turn requires finding a system of fundamental units. To do this, in general, is a very hard job. For real quadratic fields, there is an easy algorithm to find a fundamental unit. For higher degree real algebraic number fields, the situation is more difficult. However, for the so-called "simplest fields", we can find a system of fundamental units easily.

Daniel Shanks [8] selected a family of real cubic fields, which are generated by a root  $w_3$  of

$$X^3 - aX^2 - (a + 3)X - 1, \quad a \in \mathbf{Z},$$

and a conjugate of  $w_3$  is  $(-w_3 - 1)/w_3$ .

---

Received by the editors May 15, 1989.  
1980 *Mathematics Subject Classification* (1985 Revision). Primary 11R09, 11R16, 11R21, 11R27, 11R29.

*Key words and phrases.* Simplest octic fields, class number, unit group.

In the same paper, he studied the analogous real quadratic fields. We may call them “the simplest quadratic fields”, which are generated by a root  $w_2$  of

$$X^2 - aX - 1, \quad a \in \mathbf{Z},$$

and a conjugate of  $w_2$  is  $-1/w_2$ .

Marie-Nicole Gras [3] gave analogues for cyclic quartic and sextic fields. We may call them “the simplest quartic fields”, and “simplest sextic fields”. The quartic fields are generated by a root  $w_4$  of

$$X^4 - aX^3 - 6X^2 + aX + 1, \quad a \in \mathbf{Z} - \{0, \pm 3\},$$

and a conjugate of  $w_4$  is  $(w_4 - 1)/(w_4 + 1)$ . The sextic fields are generated by a root  $w_6$  of

$$X^6 - aX^5 - \left(\frac{5}{2}a + 15\right)X^4 - 20X^3 + \frac{5}{2}aX^2 + (a + 6)X + 1, \\ a \in 2\mathbf{Z} - \{0, -6, 10, -16\},$$

and a conjugate of  $w_6$  is  $(w_6 - 1)/(w_6 + 2)$ .

The main interest in these fields is that they have an explicit system of fundamental units which are relatively small and hence a relatively large class number. Gary Cornell and Larry Washington [1] pointed out a systematic way to construct these generating polynomials, which is as follows:

The quadratic ones come from the matrix

$$A_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

which is of order 2 in the group  $\mathbf{PGL}_2(\mathbf{Q})$ , and is similar to the diagonal matrix

$$\begin{pmatrix} \zeta_4 & 0 \\ 0 & \zeta_4^{-1} \end{pmatrix}.$$

The cubic ones come from the matrix

$$A_3 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix},$$

which is of order 3 in the group  $\mathbf{PGL}_2(\mathbf{Q})$ , and is similar to the diagonal matrix

$$\begin{pmatrix} \zeta_6 & 0 \\ 0 & \zeta_6^{-1} \end{pmatrix}.$$

The quartic ones come from the matrix

$$A_4 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix},$$

which is of order 4 in the group  $\mathbf{PGL}_2(\mathbf{Q})$ , and is similar to the diagonal matrix

$$\begin{pmatrix} 1 + \zeta_4 & 0 \\ 0 & 1 + \zeta_4^{-1} \end{pmatrix}.$$

The sextic ones come from the matrix

$$A_6 = \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix},$$

which is of order 6 in the group  $\mathbf{PGL}_2(\mathbf{Q})$ , and is similar to the diagonal matrix

$$\begin{pmatrix} 1 + \zeta_6 & 0 \\ 0 & 1 + \zeta_6^{-1} \end{pmatrix}.$$

The construction for each case goes like this:

Given  $\theta$ . Let  $\theta_i = A^{i-1}\theta$ ,  $i = 1, 2, \dots, n$ , where  $A$  acts on  $\theta$  by

$$A\theta = \frac{\alpha\theta + \beta}{\gamma\theta + \delta} \quad \text{if } A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

Then  $\theta$  satisfies the polynomial

$$X^n - a_1X^{n-1} + a_2X^{n-2} - a_3X^{n-3} + \dots,$$

where  $a_1 = \sum_{i=1}^n \theta_i$ ,  $a_2 = \sum_{i < j} \theta_i \theta_j$ , etc.

Using this method, we are trying to find “the simplest octic fields”. So we need a matrix  $A_8$ , which is of order 8 in the group  $\mathbf{PGL}_2(\mathbf{Q})$ . Since  $\zeta_8 = \sqrt{2}/2 + i(\sqrt{2}/2)$ , we cannot find a matrix of order 8 in the group  $\mathbf{PGL}_2(\mathbf{Q})$ . In fact, if  $A$  is of order  $n$  in  $\mathbf{PGL}_2(\mathbf{Q})$ , then  $A$  is conjugate in  $\mathbf{GL}_2(\mathbf{C})$  to the matrix

$$\lambda \begin{pmatrix} \zeta_n & 0 \\ 0 & 1 \end{pmatrix} \quad \text{for some } \lambda.$$

Therefore

$$\frac{(\text{tr } A)^2}{\det A} = \frac{(\zeta_n + 1)^2}{\zeta_n} = 2 + 2 \cos \frac{2\pi}{n}.$$

This is in  $\mathbf{Q}$  only for  $n = 1, 2, 3, 4, 6$ . Thus we have to work on the quadratic field  $\mathbf{Q}(\sqrt{2})$ .

So now, we are looking for a matrix  $A_8$ , which is order 8 in the group  $\mathbf{PGL}_2(\mathbf{Q}(\sqrt{2}))$ . Of course, we start with the matrices

$$\begin{pmatrix} 1 + \zeta_8 & 0 \\ 0 & 1 + \zeta_8^{-1} \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \zeta_{16} & 0 \\ 0 & \zeta_{16}^{-1} \end{pmatrix}.$$

However, it turns out that the diagonal matrix

$$D_8 = \begin{pmatrix} \sqrt{2}(1 + \zeta_8) & 0 \\ 0 & \sqrt{2}(1 + \zeta_8^{-1}) \end{pmatrix}$$

is a better one to start with. Note that  $D_8$  has trace  $2\varepsilon$  and norm  $2\varepsilon + 2$ , where  $\varepsilon = \sqrt{2} + 1$ . Any matrix which is similar to  $D_8$  must have the same trace and norm. One such  $A$  is  $\begin{pmatrix} \varepsilon & -1 \\ 1 & \varepsilon \end{pmatrix}$ , since  $\varepsilon^2 = 2\varepsilon + 1$ .

Using this matrix, we will construct a family of octic polynomials in §2 and select an interesting subfamily so that the generating fields are totally real cyclic octic fields. In §3, we will study these fields, finding a system of independent units, which is close to being a system of fundamental units. To show how

close it is, we get a lower bound on the regulator and hence an upper bound on the index in §4. In fact, we obtain an upper bound which works for all fields in the family. Also via Brauer-Siegel's theorem we can estimate how large the class number is. After that we will do some calculations in §5 on the first few examples and then make a conjecture that the index is 8. From this conjecture, we succeed in getting a system of fundamental units for the quartic subfield. For the octic field, we obtain a set of units which we conjugate to be fundamental. Finally, there is a very natural way to generalize the polynomials we constructed in §2 to get a family of real  $2^n$ -tic algebraic number fields. However, to select a subfamily so that the fields are Galois over  $\mathbf{Q}$  is not easy and still a lot of work on these remains to be done.

This paper comes from the author's Ph.D. dissertation at the University of Maryland in College Park under the direction of Lawrence C. Washington. The author would like to thank him for his continued interest and many conversations to improve the results in this work.

## 2. THE CONSTRUCTION OF THE OCTIC POLYNOMIALS

Let  $\varepsilon = \sqrt{2} + 1$  and let  $A = \begin{pmatrix} \varepsilon & -1 \\ 1 & \varepsilon \end{pmatrix}$ . Then  $A$  is of order 8 in the group  $\mathbf{PGL}_2(\mathbf{Q}(\sqrt{2}))$ , since

$$\begin{aligned} A^2 &\sim \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, & A^3 &\sim \begin{pmatrix} 1 & -\varepsilon \\ \varepsilon & 1 \end{pmatrix}, & A^4 &\sim \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, & A^5 &\sim \begin{pmatrix} -1 & -\varepsilon \\ \varepsilon & -1 \end{pmatrix}, \\ A^6 &\sim \begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix}, & A^7 &\sim \begin{pmatrix} -\varepsilon & -1 \\ 1 & -\varepsilon \end{pmatrix}, & A^8 &\sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Let  $\theta_1 = \theta$  and let  $\theta_i = A^{i-1}\theta$ ,  $i = 2, \dots, 8$ . Writing them out, we have

$$(2.1) \quad \begin{aligned} \theta_1 &= \theta, & \theta_2 &= \frac{\varepsilon\theta - 1}{\theta + \varepsilon}, & \theta_3 &= \frac{\theta - 1}{\theta + 1}, \\ \theta_4 &= \frac{\theta - \varepsilon}{\varepsilon\theta + 1}, & \theta_5 &= \frac{-1}{\theta}, & \theta_6 &= \frac{-\theta - \varepsilon}{\varepsilon\theta - 1}, \\ \theta_7 &= \frac{-\theta - 1}{\theta - 1}, & \theta_8 &= \frac{-\varepsilon\theta - 1}{\theta - \varepsilon}. \end{aligned}$$

Clearly,  $\prod_{i=1}^8 \theta_i = 1$ . Therefore  $\theta$  satisfies the octic polynomial

$$X^8 - a_1X^7 + a_2X^6 - a_3X^5 + a_4X^4 - a_5X^3 + a_6X^2 - a_7X + 1,$$

where  $a_1 = \sum_{i=1}^8 \theta_i$ ,  $a_2 = \sum_{i < j} \theta_i \theta_j$ , etc. A straightforward calculation yields that

$$\begin{aligned} a_1 &= \theta + \frac{-1}{\theta} + \frac{-2}{\theta - 1} + \frac{-2}{\theta + 1} + \frac{-2 - 2\varepsilon}{\theta - \varepsilon} + \frac{-2 - 2\varepsilon}{\theta + \varepsilon} + \frac{-6 + 2\varepsilon}{\theta - \varepsilon^{-1}} + \frac{-6 + 2\varepsilon}{\theta + \varepsilon^{-1}}, \\ a_2 &= -28, \quad a_3 = -7a_1, \quad a_4 = 70, \quad a_5 = 7a_1, \quad a_6 = -28, \quad a_7 = -a_1. \end{aligned}$$

So we have a family of octic polynomials

$$(2.2) \quad P(X) = X^8 - a_1X^7 - 28X^6 + 7a_1X^5 + 70X^4 - 7a_1X^3 - 28X^2 + a_1X + 1.$$

*Remark.* It takes a lot of time to get the above straightforward calculation done. Don Zagier pointed out that we have a much quicker method to avoid such a lengthy calculation. For our case, it goes like this: The matrix  $A$  is similar to the diagonal matrix

$$D = \begin{pmatrix} \varepsilon + i & 0 \\ 0 & \varepsilon - i \end{pmatrix}.$$

Therefore  $A = B^{-1}DB$  for some invertible  $B$ . A calculation shows that we may choose  $B$  to be the matrix  $\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$ . Thus  $\theta$  satisfies the following polynomial:

$$P(X) = \prod_{\nu=1}^8 (X - A^\nu \theta).$$

Hence we have

$$\begin{aligned} P(X) = 0 &\Leftrightarrow X = A^k \theta = B^{-1} D^k B \theta, \\ &\Leftrightarrow BX = \begin{pmatrix} \varepsilon + i \\ \varepsilon - i \end{pmatrix}^k B \theta, \\ &\Leftrightarrow (BX)^8 = (B\theta)^8, \quad \text{since } \frac{\varepsilon + i}{\varepsilon - i} = \zeta_8, \\ &\Leftrightarrow \left( \frac{X+i}{X-i} \right)^8 = \left( \frac{\theta+i}{\theta-i} \right)^8. \end{aligned}$$

Therefore

$$\begin{aligned} P(X) &= \frac{(\theta - i)^8 (X + i)^8 - (\theta + i)^8 (X - i)^8}{(\theta - i)^8 - (\theta + i)^8} \\ &= \sum_{\nu=0}^8 \binom{8}{\nu} X^{8-\nu} \alpha_\nu, \end{aligned}$$

where

$$\alpha_\nu = \frac{i^\nu (\theta - i)^8 - (-i)^\nu (\theta + i)^8}{(\theta - i)^8 - (\theta + i)^8}.$$

It is easy to see that

$$\alpha_\nu = \begin{cases} (-1)^{\nu/2} & \text{if } \nu \text{ is even,} \\ (-1)^{(\nu-1)/2} \alpha_1 & \text{if } \nu \text{ is odd.} \end{cases}$$

Let  $a_1 = 8\alpha_1$ ; then we get the polynomial  $P(X)$  in equation (2.2). Note that  $\alpha_1 \in \mathbf{R}$ , since  $\bar{\alpha}_1 = \alpha_1$ .

We may write the polynomial  $P(X)$  in equation (2.2) as

$$(2.3) \quad X^8 - 28X^6 + 70X^4 - 28X^2 + 1 - a_1 X(X^2 - 1)(X^2 - \varepsilon^2)(X^2 - \varepsilon^{-2}).$$

An easy calculation via equation (2.3) yields

$$\begin{aligned} P(-\infty) &> 0, & P(-\varepsilon) &< 0, & P(-1) &= 16 > 0, \\ P(-\varepsilon^{-1}) &< 0, & P(0) &= 1 > 0, & P(\varepsilon^{-1}) &< 0, \\ P(1) &= 16 > 0, & P(\varepsilon) &< 0, & P(+\infty) &> 0. \end{aligned}$$

Hence  $P(X) = 0$  has eight distinct real roots. Let  $\theta$  be the largest one. Then we have the following results:

$$(2.4) \quad \begin{aligned} \theta_1 &\in (\varepsilon, \infty), & \theta_2 &\in (1, \varepsilon), & \theta_3 &\in (\varepsilon^{-1}, 1), \\ \theta_4 &\in (0, \varepsilon^{-1}), & \theta_5 &\in (-\varepsilon^{-1}, 0), & \theta_6 &\in (-1, -\varepsilon^{-1}), \\ \theta_7 &\in (-\varepsilon, -1), & \theta_8 &\in (-\infty, -\varepsilon). \end{aligned}$$

They are all units in the ring of algebraic integers of the field  $\mathbf{Q}(\theta, \sqrt{2})$  if  $a_1$  is an algebraic integer of the field  $\mathbf{Q}(\sqrt{2})$ . Now let us check the irreducibility of the polynomial  $P(X)$ . For this, we have the following proposition. The proof is very long, but straightforward (see Shen [9]).

**Proposition 1.** *The octic polynomial  $P(X)$  in equation (2.2) is irreducible over the field  $\mathbf{Q}$  of rational numbers for  $a_1 \in \mathbf{Z} - \{0, \pm 6, \pm 15\}$ .*

*Remark.* For  $a_1 = 0, \pm 6, \pm 15$ , the polynomial  $P(X)$  does factor, and factors in the following way:

$$\begin{aligned} &(X^4 + 4X^3 - 6X^2 - 4X + 1)(X^4 - 4X^3 - 6X^2 + 4X + 1), \\ &(X^4 \pm 2X^3 - 6X^2 \mp 2X + 1)(X^4 \mp 8X^3 - 6X^2 \pm 8X + 1), \\ &(X^4 \pm X^3 - 6X^2 \mp X + 1)(X^4 \mp 16X^3 - 6X^2 \pm 16X + 1). \end{aligned}$$

Now let  $\theta$  be a root of  $P(X) = 0$  for  $a_1 \in \mathbf{Z} - \{0, \pm 6, \pm 15\}$ , and let  $\theta_i = A^{i-1}\theta$ ,  $i = 1, 2, 3, \dots, 8$ . Then they are all roots of  $P(X) = 0$ . Let  $y = \frac{1}{2}(\theta_1 + \theta_5)$  and  $z = \frac{1}{4}(\theta_1 + \theta_3 + \theta_5 + \theta_7)$ . Then we have the following proposition. For a proof, see Shen [9].

**Proposition 2.** (a) *The minimal polynomial of  $y$  over  $\mathbf{Q}$  is*

$$X^4 - \frac{1}{2}a_1X^3 - 6X^2 + \frac{1}{2}a_1X + 1,$$

*and hence  $\mathbf{Q}(y)$  is a "simplest quartic field".*

(b) *The minimal polynomial of  $z$  over  $\mathbf{Q}$  is  $X^2 - \frac{1}{4}a_1X - 1$ , and hence  $\mathbf{Q}(z) = \mathbf{Q}(\sqrt{a_1^2 + 64})$ .*

(c) *We have  $\mathbf{Q}(z) = \mathbf{Q}(\sqrt{2})$  if  $a_1 \in \{a_1 \in \mathbf{Z} \mid a_1 + b_1\sqrt{2} = \pm 8\varepsilon^{2n+1}, n \in \mathbf{Z}\}$ .*

*Remark.* In (b), when  $a_1^2 + 64$  is a square in  $\mathbf{Z}$ , then  $a_1 = 0, \pm 6, \pm 15$ . These are the degenerate cases, which made the polynomial  $P(X)$  reducible in Proposition 1.

Because of the special form for  $a_1$  in the last statement of Proposition 2, put  $a_1 = 8a$ , and let us work with the octic polynomial of the following form from now on:

$$(2.5) \quad Q(X) = X^8 - 8aX^7 - 28X^6 + 56aX^5 + 70X^4 - 56aX^3 - 28X^2 + 8aX + 1$$

for  $a \in \mathbf{Z}$ . Let  $\rho$  be the largest root of  $Q(X) = 0$  and let  $\rho_i = \sigma^{i-1}\rho$  for  $i = 1, 2, 3, \dots, 8$ , where  $\sigma \in \text{Gal}(\mathbf{Q}(\rho)/\mathbf{Q})$  is determined by

$$\rho \mapsto \frac{\varepsilon\rho - 1}{\rho + \varepsilon}.$$

Note that  $\rho_i = \theta_i$  for  $i = 1, 2, 5, 6$ . However,

$$\rho_3 = \theta_7, \quad \rho_4 = \theta_8, \quad \rho_7 = \theta_3, \quad \rho_8 = \theta_4.$$

We have a different ordering since  $\sigma(\varepsilon) = -\varepsilon^{-1}$ .

Let  $K_a = \mathbf{Q}(\rho)$ . Since  $K_{-a} = K_a$  for  $a \in \mathbf{Z}$ , we may assume  $a > 0$ ,  $a \in \mathbf{Z}$  hereafter. As above, we let  $y = \frac{1}{2}(\rho_1 + \rho_5)$  and  $z = \frac{1}{4}(\rho_1 + \rho_3 + \rho_5 + \rho_7)$ . Then  $y = \frac{1}{2}(\rho - 1/\rho)$  and  $z = \frac{1}{2}(y - 1/y)$ , and hence we have the following proposition.

**Proposition 3.** (a) *The polynomial  $Q(X)$  in equation (2.5) is irreducible over  $\mathbf{Q}$ .*

(b) *The minimal polynomial of  $y$  over  $\mathbf{Q}$  is  $X^4 - 4aX^3 - 6X^2 + 4aX + 1$ .*

(c) *The minimal polynomial of  $z$  over  $\mathbf{Q}$  is  $X^2 - 2aX - 1$ .*

(d) *The minimal polynomial of  $\rho$  over  $\mathbf{Q}(y)$  is  $X^2 - 2yX - 1$ .*

(e) *The minimal polynomial of  $y$  over  $\mathbf{Q}(z)$  is  $X^2 - 2zX - 1$ .*

(f) *The minimal polynomial of  $\rho$  over  $\mathbf{Q}(z)$  is  $X^4 - 4zX^3 - 6X^2 + 4zX + 1$ .*

*Remarks.* (a) We have

$$Q(X) = \Re(X + i)^8 - a\Im(X + i)^8,$$

$$X^4 - 4aX^3 - 6X^2 + 4aX + 1 = \Re(X + i)^4 - a\Im(X + i)^4,$$

and

$$X^2 - 2aX - 1 = \Re(x + i)^2 - a\Im(x + i)^2.$$

(b) We may say that  $\mathbf{Q}(\rho)$  is a simplest quartic field over  $\mathbf{Q}(z)$ .

Let  $y_i = \sigma^{i-1}y$ ,  $i = 1, 2, 3, 4$ , and let  $z_i = \sigma^{i-1}z$ ,  $i = 1, 2$ . Proposition 3 tells us that

$$(2.6) \quad z_1 = a + \sqrt{a^2 + 1}, \quad z_2 = a - \sqrt{a^2 + 1},$$

$$(2.7) \quad y_i = z_i + \sqrt{z_i^2 + 1}, \quad y_{i+2} = z_i - \sqrt{z_i^2 + 1}, \quad i = 1, 2,$$

$$(2.8) \quad \theta_i = y_i + \sqrt{y_i^2 + 1}, \quad \theta_{i+4} = y_i - \sqrt{y_i^2 + 1}, \quad i = 1, 2, 3, 4.$$

Thus we have

$$z_1z_2 = -1; \quad y_iy_{i+2} = -1, \quad i = 1, 2; \quad \theta_i\theta_{i+4} = -1, \quad i = 1, 2, 3, 4.$$

Note that if  $\rho = \theta$  then

$$\begin{aligned} \rho_1 = \theta_1, \quad \rho_2 = \theta_2, \quad \rho_3 = \theta_7, \quad \rho_4 = \theta_8, \\ \rho_5 = \theta_5, \quad \rho_6 = \theta_6, \quad \rho_7 = \theta_3, \quad \rho_8 = \theta_4. \end{aligned}$$

Also, as  $a \rightarrow \infty$ , the above formulas imply that

$$(2.9) \quad z_1 \sim 2a, \quad z_2 \rightarrow 0,$$

$$(2.10) \quad y_1 \sim 4a, \quad y_2 \rightarrow 1, \quad y_3 \rightarrow 0, \quad y_4 \rightarrow -1,$$

$$(2.11) \quad \rho_1 \sim 8a, \quad \rho_2 \rightarrow \varepsilon, \quad \rho_3 \rightarrow -1, \quad \rho_4 \rightarrow -\varepsilon.$$

For later use we express each  $y_i$  in term of  $a$  as follows:

$$(2.12) \quad \begin{aligned} y_1 &= a + \sqrt{a^2 + 1} + \sqrt{2(a^2 + 1) + 2a\sqrt{a^2 + 1}}, \\ y_2 &= a - \sqrt{a^2 + 1} + \sqrt{2(a^2 + 1) - 2a\sqrt{a^2 + 1}}, \\ y_3 &= a + \sqrt{a^2 + 1} - \sqrt{2(a^2 + 1) + 2a\sqrt{a^2 + 1}}, \\ y_4 &= a - \sqrt{a^2 + 1} - \sqrt{2(a^2 + 1) - 2a\sqrt{a^2 + 1}}. \end{aligned}$$

### 3. THE TOTALLY REAL CYCLIC OCTIC FIELDS

Let  $S = \{a_n \in \mathbf{Z} \mid a_n + b_n\sqrt{2} = \varepsilon^{2n+1}, n \in \mathbf{N}\}$ , and let  $K_n = K_{a_n}$ , where  $a_n \in S$ . Then  $K_n/\mathbf{Q}$  is Galois (since  $\sqrt{2} \in K_n$ ) and  $\sigma$  is an automorphism of  $K_n/\mathbf{Q}$ . We have the following theorem from the previous proposition.

**Theorem 1.** (a) For  $a_n \in S$ , the field  $K_n$  is a totally real cyclic octic field, whose Galois group  $\text{Gal}(K_n/\mathbf{Q})$  is  $\langle \sigma \rangle \simeq \mathbf{Z}/8\mathbf{Z}$ .

(b) The unique quartic subfield of  $K_n$  is a "simplest quartic field"  $\mathbf{Q}(y_n)$ , where  $y_n$  is a root of the polynomial

$$X^4 - 4a_n X^3 - 6X^2 + 4a_n X + 1.$$

(c) The unique quadratic subfield of  $K_n$  is always  $\mathbf{Q}(\sqrt{2})$ .

*Remark.* For  $a_n \in S$ ,  $a_n^2 + 1 = 2b_n^2$  and  $b_n > 0$ . Thus  $\sqrt{a_n^2 + 1} = b_n\sqrt{2}$ . Formulas in (2.12) and the above relation give us that

$$y_n = a_n + b_n\sqrt{2} + \sqrt{2\sqrt{2}b_n(a_n + b_n\sqrt{2})}.$$

But  $a_n + b_n\sqrt{2} = \varepsilon^{2n+1}$ ,  $n \in \mathbf{N}$ . So we have

$$y_n = \varepsilon^{2n+1} + \varepsilon^n \sqrt{b_n(4 + 2\sqrt{2})}.$$

*Claim.* The quotient

$$\frac{b_m(4 + 2\sqrt{2})}{b_n(4 + 2\sqrt{2})} = \frac{b_m}{b_n}$$

is not a square in  $\mathbf{Q}(\sqrt{2})$  for infinitely many  $m$  and  $n$ . Therefore there are infinitely many distinct octic fields  $K_n$ .

*Proof.* We now prove this claim. For any  $b_m$ ,  $a_m^2 + 1 = 2b_m^2$ . Say  $b_m = s^2 b_n$  for some  $s \in \mathbf{Z}[\sqrt{2}]$ . Then  $b_m^2 = s^4 b_n^2$ , and hence  $a_m^2 + 1 = 2b_n^2 s^4$ . A result due to Siegel [10] implies that  $a^2 + 1 = cs^4$  has only finite many integral solutions. Thus it follows easily that for any  $b_m$ , there are only finitely many  $b_n$  which differ from  $b_m$  be a square in  $\mathbf{Z}[\sqrt{2}]$ . Hence the claim is true.

We shall eventually want  $b_n$  squarefree in  $\mathbf{Z}$ . It is probably very hard to prove this happens infinitely often, though it is surely true. Since  $a_n - b_n\sqrt{2} = -\varepsilon^{-(2n+1)}$ ,

$$b_n = \frac{\sqrt{2}}{4}(\varepsilon^{2n+1} + \varepsilon^{-(2n+1)}),$$

and hence

$$b_n = \frac{\sqrt{2}}{4}\varepsilon^{-(2n+1)}(\varepsilon^{4n+2} + 1).$$

The situation is similar to proving that there are infinitely many squarefree Mersenne numbers  $2^n - 1$ , which is not yet proved.

Our main interest in  $K_n$  is that we can give a system of independent units explicitly, hence an upper bound on the regulator which is relatively small. We know that  $\rho_1, \rho_2, \rho_3, \rho_4, y_1, y_2$  and  $\varepsilon$  are all units in the ring of algebraic integers of the real cyclic octic field  $K_n = \mathbf{Q}(\rho)$ . Even better, we have the following theorem.

**Theorem 2.** *The units  $\rho_1, \rho_2, \rho_3, \rho_4, y_1, y_2$ , and  $\varepsilon$  in the ring of algebraic integers of the real cyclic octic field  $K_n$  are independent.*

*Proof.* See Shen [9]. Note that it also follows from the fact (see below) that  $R_\rho \rightarrow \infty$  as  $a \rightarrow \infty$  that the result is true for sufficiently large  $a$ .

Next, we calculate the regulator

$$R_1 = \text{Reg}(\rho_1, \rho_2, \rho_3, \rho_4, y_1, y_2, \varepsilon)$$

of  $\rho_1, \rho_2, \rho_3, \rho_4, y_1, y_2$ , and  $\varepsilon$ . A calculation yields

$$(3.1) \quad R_1 = 16 \log \varepsilon (\log^2 |y_1| + \log^2 |y_2|) R_\rho,$$

where  $R_\rho$  is the regulator of  $\rho_1, \rho_2, \rho_3$ , and  $\rho_4$ . In fact, it is

$$(3.2) \quad R_\rho = \sum_{i=1}^4 A_i^4 + 2 \sum_{i=1}^2 A_i^2 A_{i+2}^2 + 4(A_1 A_2 + A_3 A_4)(A_1 A_4 - A_2 A_3),$$

where  $A_i = \log |\rho_i| = -\log |\rho_{i+4}|$ ,  $i = 1, 2, 3, 4$ .

*Remark.* From (2.10) and (2.11), as  $a \rightarrow \infty$  we have

$$R_\rho \sim (\log^2(8a) + 2 \log^2 \varepsilon)^2,$$

and hence we have the asymptotic approximation for  $R_1$  as  $a \rightarrow \infty$ , as follows:

$$(3.3) \quad R_1 \sim 16 \log \varepsilon \log^2(4a) (\log^2(8a) + 2 \log^2 \varepsilon)^2 \sim 16 \log \varepsilon \log^6 a.$$

The discriminant  $d(K_n)$  of  $K_n = \mathbf{Q}(\rho)$  may be computed as follows: For  $a \in S$ ,

$$a + b\sqrt{2} = (\sqrt{2} + 1)^{2n+1} \quad \text{and} \quad a^2 + 1 = 2b^2.$$

Both  $a$  and  $b$  are odd. We will make the following assumption henceforth:

Assume that  $b$  is squarefree in  $\mathbf{Z}$ .

Since the discriminant  $d(\mathbf{Q}(\sqrt{2})) = 8$ , the conductor of  $\mathbf{Q}(\sqrt{2})$  is 8. From the remark right after Theorem 1, we know that

$$y = (\sqrt{2} + 1)^{2n+1} + (\sqrt{2} + 1)^n \sqrt{2} \sqrt{(2 + \sqrt{2})b},$$

and hence we have

$$\mathbf{Q}(y) = \mathbf{Q}\left(\sqrt{(2 + \sqrt{2})b}\right).$$

**Proposition 4.** *The set  $\{1, \sqrt{(2 + \sqrt{2})b}\}$  forms an integral basis of  $\mathbf{Q}(y)$  over  $\mathbf{Q}(\sqrt{2})$ .*

*Proof.* See Shen [9].

**Proposition 5.** *The discriminant  $d(\mathbf{Q}(y))$  of the quartic subfield  $\mathbf{Q}(y)$  of  $K_n$  is  $2^{11}b^2$ .*

*Proof.* By Proposition 4, we have

$$d(\mathbf{Q}(y)) = d\left(\sqrt{(2 + \sqrt{2})b}\right).$$

Using the tower property of discriminants, we have

$$\begin{aligned} d\left(\sqrt{(2 + \sqrt{2})b}\right) &= (d(\mathbf{Q}(\sqrt{2})))^2 N_{\mathbf{Q}(\sqrt{2})/\mathbf{Q}}\left(d_{\mathbf{Q}(y)/\mathbf{Q}(\sqrt{2})}\left(\sqrt{(2 + \sqrt{2})b}\right)\right), \\ &= 8^2 N_{\mathbf{Q}(\sqrt{2})}(4b(2 + \sqrt{2})), \\ &= 2^6 4^2 b^2 (2 + \sqrt{2})(2 - \sqrt{2}), \end{aligned}$$

and hence  $d(\mathbf{Q}(y)) = 2^{11}b^2$ .

There are eight Dirichlet characters corresponding to the field  $K_n$ . Denote the trivial one by  $\chi_0$ , the quadratic one by  $\chi_2$ , the quartic ones by  $\chi_4, \chi_4^3 = \bar{\chi}_4$ , and the octic ones by  $\chi_8, \chi_8^3, \chi_8^5 = \bar{\chi}_8^3, \chi_8^7 = \bar{\chi}_8$ . Clearly  $f_{\chi_0} = 1$  and  $f_{\chi_2} = 8$ . What are  $f_{\chi_4}$  and  $f_{\chi_8}$ ? We have the following proposition.

**Proposition 6.** *The conductor of  $\chi_4$  is  $f_{\chi_4} = 16b$ .*

*Proof.* From the conductor-discriminant formula, we obtain

$$2^{11}b^2 = d(\mathbf{Q}(y)) = f_{\chi_0} f_{\chi_2} f_{\chi_4} f_{\bar{\chi}_4} = 8f_{\chi_4}^2.$$

The result follows immediately.

To calculate the conductor  $f_{\chi_8}$ , we have to work a little bit harder. But, it is easy to see the possible candidates as follows: A calculation yields

$$\mathbf{Q}(\rho) = \mathbf{Q}\left(\sqrt{(2 + \sqrt{2})\left(2b + (\sqrt{2} + 1)^n \sqrt{(2 + \sqrt{2})b}\right)}\right).$$

Therefore the discriminant of the octic field  $K_n = \mathbf{Q}(\rho)$  must divide

$$(2^{11}b^2)^2 N_{\mathbf{Q}(y)/\mathbf{Q}}\left(d_{\mathbf{Q}(\rho)/\mathbf{Q}(y)}\sqrt{(2 + \sqrt{2})\left(2b + (\sqrt{2} + 1)^n \sqrt{(2 + \sqrt{2})b}\right)}\right),$$

which is  $2^{33}b^6$ . Again invoking the conductor-discriminant formula, we have

$$2^3(2^4b)^2 f_{\chi_8}^4 |2^{33}b^6|.$$

Hence  $f_{\chi_8} \leq 32b$ . Since  $f_{\chi_4} = 16b$ , we conclude that  $f_{\chi_8}$  is either  $16b$  or  $32b$ .

**Theorem 3.** *The conductor of  $\chi_8$  is  $f_{\chi_8} = 32b$ , and hence  $d(K_n) = 2^{31}b^6$ .*

*Proof.* See Shen [9]. Since  $f_{\chi_8}$  is either  $16b$  or  $32b$ , a much shorter argument is as follows: We can write  $\chi_8 = \psi\theta$ , where the conductor  $f_\psi$  of  $\psi$  is a power of 2 and 2 does not divide the conductor of  $\theta$ . Since 2 ramifies in  $\mathbf{Q}(\sqrt{2})$ , which corresponds to the character  $\chi_8^4$ , we must have  $\psi^4 \neq 1$ . Therefore  $\psi$  has order 8. This can only happen if the conductor of  $\psi$  is at least 32, since otherwise  $(\mathbf{Z}/f_\psi\mathbf{Z})^\times$  does not have a cyclic quotient of order 8. Therefore 32 divides  $f_{\chi_8}$ , which yields the result.

#### 4. AN ESTIMATE FOR THE REGULATOR

We want to estimate (and hopefully calculate) the class number of the real cyclic octic field  $K_n = \mathbf{Q}(\rho)$ . So let us look at the analytic class number formula:

$$\frac{2^{r_1}(2\pi)^{r_2}hR}{w\sqrt{d}} = \prod_{\chi \neq 1} L(1, \chi).$$

For  $K_n$ ,  $r_1 = 8$ ,  $r_2 = 0$ ,  $w = 2$ ,  $d = 2^{31}b^6$ , and therefore

$$\frac{hR}{2^8\sqrt{2}b^3} = L(1, \chi_2)|L(1, \chi_4)|^2|L(1, \chi_8)|^2|L(1, \chi_8^3)|^2.$$

We know that  $L(1, \chi_2) = \log \varepsilon/\sqrt{2}$ , since  $h(\mathbf{Q}(\sqrt{2})) = 1$ . So we have

$$(4.1) \quad h = \frac{2^8b^3 \log \varepsilon}{R} |L(1, \chi_4)|^2|L(1, \chi_8)|^2|L(1, \chi_8^3)|^2.$$

To calculate  $|L(1, \chi)|$ , we may use the following (since  $\chi$  is even)

$$(4.2) \quad |L(1, \chi)| = \frac{2}{\sqrt{f}} \left| \sum_{k < f/2} \chi(k) \log \sin \frac{k\pi}{f} \right|,$$

which is part of Theorem 46 in Marcus' book [7].

So now it is clear that, in an algebraic number field, estimating the class number  $h$  is equivalent to estimating the regulator  $R$ . In general, it is hard to estimate  $R$ . However, Theorem 2 provides us hope.

Recall formula (3.1),

$$R_1 = 16 \log \varepsilon (\log^2 |y_1| + \log^2 |y_2|) R_\rho.$$

Let  $q = R_1/R$ ; then  $q$  is an integer. In fact,  $q$  is the index  $[U : U_1]$ , where  $U$  is the unit group of  $K_n$  and  $U_1 = \langle -1, \varepsilon, y_1, y_2, \rho_1, \rho_2, \rho_3, \rho_4 \rangle$ . We may

estimate  $R_1$  in terms of  $a$ . To determine  $q$ , we need a lower bound for  $R$ . One such lower bound due to J. H. Silverman [11] says that  $R > c_8 \log^4(\gamma_8 D_8)$ , where  $D_8 = |d(K_n)| = 2^{31} b^6$ , and  $c_8, \gamma_8$  are constants depending on  $K_n$ . Since

$$D_8 = 2^{28} (2b^2)^3 = 2^{28} (a^2 + 1)^3,$$

$R > d_8 \log^4 a$ , where  $d_8$  is a constant. This lower bound is not good enough for our purpose, since  $R_1 \sim 16 \log \varepsilon \log^6 a$ . So we need some other technique to get a lower bound of order  $\log^6 a$ .

In the following, we denote the norm from  $K_n$  to the quartic field  $\mathbf{Q}(y)$  by  $N_{8/4}$ , the norm from  $\mathbf{Q}(y)$  to  $\mathbf{Q}(\sqrt{2})$  by  $N_{4/2}$ , etc.

Let  $U_0 = \{\eta \in U \mid N_{8/4}(\eta) = \pm 1\}$ . Then  $U/\{\pm 1\}$  and  $U_0/\{\pm 1\}$  are both  $\mathbf{Z}[G]$ -modules, where

$$G = \text{Gal}(K_n/\mathbf{Q}) = \langle \sigma \rangle \simeq \mathbf{Z}/8\mathbf{Z}.$$

Let  $N = 1 + \sigma^4$  be the norm  $N_{8/4}$ . Then we have  $\mathbf{Z}[G]/\langle N \rangle \simeq \mathbf{Z}[\zeta_8]$ , which is a principal ideal domain. We may regard  $U_0/\{\pm 1\}$  as a  $\mathbf{Z}[\zeta_8]$ -module. Since  $\rho_1, \rho_2, \rho_3, \rho_4 \in U_0$  are independent, the  $\mathbf{Z}$ -rank of  $U_0/\{\pm 1\}$  is at least 4. Let  $U_y$  be the unit group of  $\mathbf{Q}(y)$ , and let  $U_{y0} = \{\xi \in U_y \mid N_{4/2}(\xi) = \pm 1\}$ .

The same argument yields that  $U_{y0}/\{\pm 1\}$  is a  $\mathbf{Z}[\zeta_4]$ -module, and the  $\mathbf{Z}$ -rank of  $U_{y0}/\{\pm 1\}$  is at least 2, since  $y_1, y_2 \in U_{y0}$  are independent. Clearly, the  $\mathbf{Z}$ -rank of the subgroup generated by  $\varepsilon, U_{y0}$ , and  $U_0$  is at most 7. Therefore, the  $\mathbf{Z}$ -rank of  $U_0/\{\pm 1\}$  must be 4, and that of  $U_{y0}/\{\pm 1\}$  must be 2. Hence  $U_0/\{\pm 1\}$  is a free  $\mathbf{Z}[\zeta_8]$ -module of rank 1, and  $U_{y0}/\{\pm 1\}$  is a free  $\mathbf{Z}[\zeta_4]$ -module of rank 1. Therefore, there exist units  $\eta_i \in U_0$  and  $\xi_i \in U_{y0}$  such that  $\{\eta_i = \eta_1^{\sigma^{i-1}} \mid i = 1, 2, 3, 4\}$  generates  $U_0/\{\pm 1\}$ , and  $\{\xi_i = \xi_1^{\sigma^{i-1}} \mid i = 1, 2\}$  generates  $U_{y0}/\{\pm 1\}$ .

Let  $U'$  be the group generated by the elements  $-1, \varepsilon, \xi_1, \xi_2, \eta_1, \eta_2, \eta_3, \eta_4$ , and let  $R' = \text{Reg}(\varepsilon, \xi_1, \xi_2, \eta_1, \eta_2, \eta_3, \eta_4)$  be the regulator. Then we have

$$q = [U : U_1] = [U : U'] [U' : U_1] = q_1 q'_1,$$

where  $q_1 = [U : U']$  and  $q'_1 = [U' : U_1]$ .

Let  $i_y = [U_y : \langle -1, \varepsilon, \xi_1, \xi_2 \rangle]$ . We may calculate  $q_1$  as follows:

**Proposition 7.** For  $\xi \in U_y$ , we have

$$N_{4/1}(\xi) = 1 \Leftrightarrow \xi \in \langle -1, \varepsilon, \xi_1, \xi_2 \rangle.$$

*Proof.* For any  $\xi \in U_y$  with  $N_{4/1}(\xi) = 1$ , we have  $N_{4/2}(\xi) = \pm \varepsilon^a$  for some  $a \in \mathbf{Z}$ . Thus

$$1 = N_{4/1}(\xi) = N_{2/1}(N_{4/2}(\xi)) = N_{2/1}(\pm \varepsilon^a) = (-1)^a,$$

and hence  $a$  is even, say  $a = 2A$ , for some  $A \in \mathbf{Z}$ . Therefore  $N_{4/2}(\xi) = \pm \varepsilon^{2A}$ , and so  $N_{4/2}(\xi/\varepsilon^A) = \pm 1$ . Hence we have  $\xi/\varepsilon^A \in U_{y0} = \langle -1, \xi_1, \xi_2 \rangle$ , which means  $\xi \in \langle -1, \varepsilon, \xi_1, \xi_2 \rangle$ . The converse is obvious. This completes the proof.

**Corollary 1.** *If  $N_{4/1}(\xi) = 1$  for all  $\xi \in U_y$ , then  $i_y = 1$ .*

**Corollary 2.** *If  $N_{4/1}(\xi) = -1$  for some  $\xi \in U_y$ , then  $i_y = 2$ .*

*Proof.* Let  $E_k = \{\xi \in U_y | N_{4/1}(\xi) = k\}$ ,  $k = 1, -1$ . Then the above proposition just says  $E_1 = \langle -1, \varepsilon, \xi_1, \xi_2 \rangle$ . Choose  $\xi_0 \in E_{-1}$ . Then

$$E_{-1} = \xi_0 E_1, \quad U_y = E_1 \cup E_{-1}, \quad \text{and} \quad E_1 \cap E_{-1} = \emptyset.$$

The result follows.

**Proposition 8.** *For  $\eta \in U$ , we have*

$$N_{8/1}(\eta) = 1 \Leftrightarrow \eta^2 \in U'$$

*Proof.* For any  $\eta \in U$  with  $N_{8/1}(\eta) = 1$ , Proposition 7 implies

$$N_{8/4}(\eta) = \pm \varepsilon^a \xi_1^b \xi_2^c \quad \text{for some } a, b, c \in \mathbf{Z},$$

since  $N_{4/1}(N_{8/4}(\eta)) = N_{8/1}(\eta) = 1$ . Therefore  $N_{8/4}(\eta^2) = \varepsilon^{2a} \xi_1^{2b} \xi_2^{2c}$ , and hence  $N_{8/4}(\eta^2 / \varepsilon^a \xi_1^b \xi_2^c) = 1$ . This gives us

$$\frac{\eta^2}{\varepsilon^a \xi_1^b \xi_2^c} \in U_0 = \langle -1, \eta_1, \eta_2, \eta_3, \eta_4 \rangle,$$

and we have  $\eta^2 \in \langle -1, \varepsilon, \xi_1, \xi_2, \eta_1, \eta_2, \eta_3, \eta_4 \rangle = U'$ . Conversely, write  $\eta^2 = \pm \varepsilon^a \xi_1^b \xi_2^c \eta_1^d \cdots \eta_4^e$ . Then  $N_{8/4}(\eta)^2 = \varepsilon^{2a} \xi_1^{2b} \xi_2^{2c}$ , and hence  $N_{8/4}(\eta) = \pm \varepsilon^a \xi_1^b \xi_2^c$ . Therefore, we have

$$N_{4/2}(N_{8/4}(\eta)) = \varepsilon^{2a} (\pm 1), \quad N_{8/1}(\eta) = N_{2/1}(\pm \varepsilon^{2a}) = (-1)^{2a} = 1.$$

This completes the proof.

Let  $U'_0 = \{\eta \in U | N_{8/1}(\eta) = 1\}$ . The same argument as in Proposition 7 yields that  $[U : U'_0] = 1$  or 2. Proposition 8 says that  $U'_0 = \{\eta \in U | \eta^2 \in U'\}$ . How large is  $[U'_0 : U']$ ? This index must be 1, 2, 4, or 8. To see this, we write

$$\eta^2 = \pm \varepsilon^a \xi_1^b \xi_2^c \eta_1^d \cdots \eta_4^e \quad \text{for } \eta \in U'_0.$$

Assume  $a, b, c$  are even, say  $a = 2A, b = 2B, c = 2C$ . Then

$$N_{8/4}(\eta)^2 = \varepsilon^{2a} \xi_1^{2b} \xi_2^{2c} = \varepsilon^{4A} \xi_1^{4B} \xi_2^{4C},$$

and hence

$$N_{8/4} \left( \frac{\eta}{\varepsilon^A \xi_1^B \xi_2^C} \right)^2 = 1 \quad \text{and} \quad N_{8/4} \left( \frac{\eta}{\varepsilon^A \xi_1^B \xi_2^C} \right) = \pm 1.$$

Therefore

$$\frac{\eta}{\varepsilon^A \xi_1^B \xi_2^C} \in U_0 = \langle -1, \eta_1, \eta_2, \eta_3, \eta_4 \rangle,$$

and hence  $\eta \in \langle -1, \varepsilon, \xi_1, \xi_2, \eta_1, \eta_2, \eta_3, \eta_4 \rangle = U'$ .

Now let us look at the norm  $N_{8/4}(\eta)$  for  $\eta \in U'_0$ . Since  $N_{4/1}(N_{8/4}(\eta)) = N_{8/1}(\eta) = 1$ , Proposition 7 tells us that

$$N_{8/4}(\eta) = \pm \varepsilon^a \zeta_1^b \zeta_2^c \text{ for some } a, b, c \in \mathbf{Z}.$$

The above result says that  $\eta \in U'$ , whenever  $a, b, c$  are all even. Therefore

$$U' = \{ \eta \in U'_0 \mid N_{8/4}(\eta) = \pm \varepsilon^{\text{even}} \zeta_1^{\text{even}} \zeta_2^{\text{even}} \}.$$

All other possibilities,  $\{ \eta \in U'_0 \mid N_{8/4}(\eta) = \pm \varepsilon^{\text{odd}} \zeta_1^{\text{even}} \zeta_2^{\text{even}} \}, \dots$ , are cosets of  $U'$  in  $U'_0$ . Hence the index  $[U'_0 : U']$  divides 8, and the result follows.

Putting everything together, we have the following:

**Theorem 4.** *Let  $U$  be the unit group of  $K_n$ , and let  $U'$  be the subgroup generated by the units  $-1, \varepsilon, \zeta_1, \zeta_2, \eta_1, \eta_2, \eta_3, \eta_4$ . Then we have the following:*

- (a) *The index  $q_1 = [U : U']$  is  $2^r$ ,  $r \leq 4$ .*
- (b) *If  $N_{8/1}(\eta) = 1 \ \forall \eta \in U$ , then the index  $q_1 = [U : U'] = 2^r$ ,  $r \leq 3$ .*

*Remark.* The result here cannot be improved for general cyclic octic fields. Consider the field

$$\mathbf{Q}(\zeta_{17})^+ = \mathbf{Q} \left( \cos \frac{2\pi}{17} \right),$$

which is a real cyclic octic field and has class number 1. Let  $\sigma_3$  be the Galois action determined by  $\zeta_{17} \mapsto \zeta_{17}^3$ . Then the Galois group of  $\mathbf{Q}(\zeta_{17})^+$  over  $\mathbf{Q}$  is

$$\langle \sigma_3 \rangle \simeq \mathbf{Z}/8\mathbf{Z} \simeq \{ \sigma_3, \sigma_9, \sigma_{10}, \sigma_{13}, \sigma_5, \sigma_{15}, \sigma_{11}, 1 \}.$$

Note that  $\mathbf{Q}(\zeta_{17})^+$  has a unique quadratic subfield  $\mathbf{Q}(\sqrt{17})$ , whose fundamental unit is

$$\varepsilon = 4 + \sqrt{17} \sim 8.12310562562.$$

By Theorem 8.2 of Washington's book [13], the cyclotomic units

$$\left\{ \psi_a = \sin \frac{\pi a}{17} / \sin \frac{\pi}{17} \mid a = 2, 3, 4, 5, 6, 7, 8 \right\}$$

form a system of fundamental units. Thus  $U = \langle -1, \psi_a \mid a = 2, 3, \dots, 8 \rangle$ . Note that we have

$$\psi_a = \zeta_{17}^{(1-a)/2} \frac{1 - \zeta_{17}^a}{1 - \zeta_{17}}$$

and hence

$$\psi_a^{\sigma_i} = \frac{\psi_{ai}}{\psi_i} \text{ for } a, i = 2, 3, \dots, 16.$$

Also, we have

$$\begin{aligned} \psi_a &= \psi_{17-a} \text{ for } a = 2, 3, \dots, 16. \\ N_{8/4}(\psi_a) &= \psi_a^{1+\sigma_{-4}}, \quad N_{8/2}(\psi_a) = \psi_a^{1+\sigma_{-8}+\sigma_{-4}+\sigma_{-2}}. \end{aligned}$$

Note that we have

$$\varepsilon = 4 + \sqrt{17} = \psi_2^{-1} \psi_3 \psi_4^{-1} \psi_5 \psi_6 \psi_7 \psi_8^{-1}.$$

Let

$$\begin{aligned} \xi_1 &= \psi_2 \psi_8 \psi_4^{-1}, & \xi_2 &= \psi_3 \psi_5 \psi_6^{-1} \psi_7^{-1}, \\ \eta_1 &= \psi_2 \psi_8^{-1}, & \eta_2 &= \psi_3^{-1} \psi_5, & \eta_3 &= \psi_4, & \eta_4 &= \psi_6 \psi_7^{-1}. \end{aligned}$$

Then  $\eta_1, \eta_2, \eta_3, \eta_4$  form a basis of  $U_0$ , and  $\xi_1$  and  $\xi_2$  form a basis for  $U_{y_0}$  (see Shen [9]). Therefore

$$\begin{pmatrix} \log|\varepsilon| \\ \log|\xi_1| \\ \log|\xi_2| \\ \log|\eta_1| \\ \log|\eta_2| \\ \log|\eta_3| \\ \log|\eta_4| \end{pmatrix} = \begin{pmatrix} -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & -1 & -1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & -1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 \end{pmatrix} \begin{pmatrix} \log|\psi_2| \\ \log|\psi_3| \\ \log|\psi_4| \\ \log|\psi_5| \\ \log|\psi_6| \\ \log|\psi_7| \\ \log|\psi_8| \end{pmatrix}.$$

A calculation yields that the determinant equals 16, and hence  $[U : U'] = 16$ . This is the case  $r = 4$  in Theorem 4.

Next, we calculate the index  $q'_1$  as follows: Clearly, we have  $q'_1 = R_1/R'$ . Equation (3.1) implies that

$$R_1 = 16R(\varepsilon)R(y_1, y_2)R(\rho_1, \rho_2, \rho_3, \rho_4).$$

Exactly the same calculation yields

$$R' = 16R(\varepsilon)R(\xi_1, \xi_2)R(\eta_1, \eta_2, \eta_3, \eta_4).$$

Let  $q_2 = [(\xi_1, \xi_2) : (y_1, y_2)]$ , and let  $q_3 = [(\eta_1, \eta_2, \eta_3, \eta_4) : (\rho_1, \rho_2, \rho_3, \rho_4)]$ . Then

$$q_2 = \frac{R(y_1, y_2)}{R(\xi_1, \xi_2)} \quad \text{and} \quad q_3 = \frac{R(\rho_1, \rho_2, \rho_3, \rho_4)}{R(\eta_1, \eta_2, \eta_3, \eta_4)}.$$

Therefore  $q'_1 = q_2 q_3$  and  $q = q_1 q_2 q_3$ .

To estimate  $q_2$  and  $q_3$ , we need lower bounds for  $R(\xi_1, \xi_2)$  and  $R(\eta_1, \eta_2, \eta_3, \eta_4)$ . Our approach below is similar to Cusick's [2]. Let  $\varepsilon_1 \in U_{y_0}$ , and let  $\varepsilon_2 = \varepsilon_1^\sigma$ . Then by the definition of  $U_{y_0}$ , we have

$$\varepsilon_1^{\sigma^2} = \pm \frac{1}{\varepsilon_1} \quad \text{and} \quad \varepsilon_2^{\sigma^2} = \pm \frac{1}{\varepsilon_2}.$$

Consider the norm  $N_{2/1}(d_{4/2}(\varepsilon_1))$ , where  $d_{4/2}$  is the discriminant from  $\mathbf{Q}(y)$  to  $\mathbf{Q}(\sqrt{2})$ . A calculation yields

$$\left(\varepsilon_1 \pm \frac{1}{\varepsilon_1}\right)^2 \left(\varepsilon_2 \pm \frac{1}{\varepsilon_2}\right)^2,$$

or

$$\left(1 \pm \frac{1}{\varepsilon_1^2}\right)^2 \left(1 \pm \frac{1}{\varepsilon_2^2}\right)^2 \varepsilon_1^2 \varepsilon_2^2.$$

Replacing  $\varepsilon_i$  by  $1/\varepsilon_i$  or possibly using  $\varepsilon_2$  in place of  $\varepsilon_1$  and  $\varepsilon^{-1} = \pm\varepsilon_2^\sigma$  in place of  $\varepsilon_2$  if necessary, we may assume  $|\varepsilon_i| \geq 1$  for  $i = 1, 2$ . Then the above expression is less than or equal to  $2^4\varepsilon_1^2\varepsilon_2^2$ . Since  $N_{2/1}(d_{4/2}(\mathbf{Q}(y))) = 2^5b^2$ , we have  $2^5b^2 \leq 2^4\varepsilon_1^2\varepsilon_2^2$ . Therefore we have the following inequality by Cauchy-Schwarz:

$$\begin{aligned} \log(a^2) &< \log(a^2 + 1) = \log(2b^2) \leq 2 \sum_{i=1}^2 \log |\varepsilon_i| \\ &\leq 2\sqrt{2} \sqrt{\log^2 |\varepsilon_1| + \log^2 |\varepsilon_2|}. \end{aligned}$$

Hence we have

$$(4.3) \quad \log^2 |\varepsilon_1| + \log^2 |\varepsilon_2| > \frac{1}{2} \log^2 a.$$

Since  $\{\xi_1, \xi_2\}$  generates  $U_{y_0}/\{\pm 1\}$ ,

$$\varepsilon_1 = \pm \xi_1^{x_1} \xi_2^{x_2} \quad \text{for some } x_1, x_2 \in \mathbf{Z}.$$

Therefore

$$\log |\varepsilon_1| = x_1 \log |\xi_1| + x_2 \log |\xi_2|,$$

and hence

$$\log |\varepsilon_2| = x_1 \log |\xi_2| - x_2 \log |\xi_1|.$$

Define a quadratic form  $Q(x_1, x_2)$  in  $x_1, x_2$  by

$$Q(x_1, x_2) = \log^2 |\varepsilon_1| + \log^2 |\varepsilon_2| = \sum_{i,j=1}^2 a_{ij} x_i x_j.$$

A simple calculation gives that

$$Q(x_1, x_2) = R(\xi_1, \xi_2)(x_1^2 + x_2^2).$$

Thus  $Q(1, 0) = R(\xi_1, \xi_2)$ , and the inequality (29) gives a lower bound for  $R(\xi_1, \xi_2)$ , as follows:

$$(4.4) \quad R(\xi_1, \xi_2) > \frac{1}{2} \log^2 a.$$

Similarly, we can do the same thing as above to get a lower bound for  $R(\eta_1, \eta_2, \eta_3, \eta_4)$ . However, the situation is a little bit complicated. Let  $\varepsilon_1 \in U_0$ , and let  $\varepsilon_i = \varepsilon_1^{\sigma^{i-1}}$ ,  $i = 1, 2, 3, 4$ . Then by the definition of  $U_0$ , we have  $\varepsilon_i^{\sigma^4} = \pm 1/\varepsilon_i$ ,  $i = 1, 2, 3, 4$ . Consider the norm  $N_{4/1}(d_{8/4}\varepsilon_1)$ . A calculation yields

$$\left(\varepsilon_1 \pm \frac{1}{\varepsilon_1}\right)^2 \left(\varepsilon_2 \pm \frac{1}{\varepsilon_2}\right)^2 \left(\varepsilon_3 \pm \frac{1}{\varepsilon_3}\right)^2 \left(\varepsilon_4 \pm \frac{1}{\varepsilon_4}\right)^2,$$

or

$$\left(1 \pm \frac{1}{\varepsilon_1^2}\right)^2 \cdots \left(1 \pm \frac{1}{\varepsilon_4^2}\right)^2 \varepsilon_1^2 \varepsilon_2^2 \varepsilon_3^2 \varepsilon_4^2.$$

Again, we may assume that  $|\varepsilon_i| \geq 1$  for  $i = 1, 2$ . Then the above expression is less than or equal to  $2^8 \varepsilon_1^2 \varepsilon_2^2 \varepsilon_3^2 \varepsilon_4^2$ . Since  $N_{4/1}(d_{8/4} K_n) = 2^9 b^2$ ,

$$2^9 b^2 \leq 2^8 \varepsilon_1^2 \varepsilon_2^2 \varepsilon_3^2 \varepsilon_4^2.$$

Therefore, we have

$$2 \log a = \log(a^2) < \log(a^2 + 1) = \log(2b^2) \leq 2 \sum_{i=1}^4 \log |\varepsilon_i|.$$

By Cauchy-Schwarz, the above is less than or equal to

$$2\sqrt{4} \left( \sum_{i=1}^4 \log^2 |\varepsilon_i| \right)^{1/2}.$$

Thus we have

$$(4.5) \quad \log^2 |\varepsilon_1| + \log^2 |\varepsilon_2| + \log^2 |\varepsilon_3| + \log^2 |\varepsilon_4| > \frac{1}{4} \log^2 a.$$

Since  $\{\eta_1, \eta_2, \eta_3, \eta_4\}$  generates  $U_0/\{\pm 1\}$ ,

$$\varepsilon_1 = \pm \eta_1^{x_1} \eta_2^{x_2} \eta_3^{x_3} \eta_4^{x_4} \quad \text{for some } x_i \in \mathbf{Z}.$$

Therefore we have

$$\log |\varepsilon_1| = x_1 \log |\eta_1| + x_2 \log |\eta_2| + x_3 \log |\eta_3| + x_4 \log |\eta_4|,$$

and hence

$$\begin{aligned} \log |\varepsilon_2| &= x_1 \log |\eta_2| + x_2 \log |\eta_3| + x_3 \log |\eta_4| - x_4 \log |\eta_1|, \\ \log |\varepsilon_3| &= x_1 \log |\eta_3| + x_2 \log |\eta_4| - x_3 \log |\eta_1| - x_4 \log |\eta_2|, \\ \log |\varepsilon_4| &= x_1 \log |\eta_4| - x_2 \log |\eta_1| - x_3 \log |\eta_2| - x_4 \log |\eta_3|. \end{aligned}$$

Define a quadratic form  $Q(x_1, x_2, x_3, x_4)$  in  $x_1, x_2, x_3, x_4$  by

$$(4.6) \quad Q(x_1, x_2, x_3, x_4) = \sum_{i=1}^4 \log^2 |\varepsilon_i| = \sum_{i,j=1}^4 a_{ij} x_i x_j.$$

A calculation shows that the determinant of the quadratic form  $Q$  is

$$(4.7) \quad \det(Q) = \det(a_{ij}) = R(\eta_1, \eta_2, \eta_3, \eta_4)^2.$$

In fact,

$$(a_{ij}) = \begin{pmatrix} A & B & 0 & -B \\ B & A & B & 0 \\ 0 & B & A & B \\ -B & 0 & B & A \end{pmatrix},$$

where  $A = \sum_{i=1}^4 \log^2 |\eta_i|$  and  $B = \log |\eta_1| \log |\eta_2| + \log |\eta_2| \log |\eta_3| + \log |\eta_3| \log |\eta_4| - \log |\eta_4| \log |\eta_1|$ . An old result due to A. Korkine and G. Zolotareff [5] gives us that there exist integers  $x_1, x_2, x_3, x_4$  not all zero, such that

$$Q(x_1, x_2, x_3, x_4) \leq (4 \det(Q))^{1/4}.$$

Putting (4.5)–(4.7) together, we get a lower bound of  $R(\eta_1, \eta_2, \eta_3, \eta_4)$ :

$$(4.8) \quad R(\eta_1, \eta_2, \eta_3, \eta_4) > 2^{-5} \log^4 a.$$

Since  $R'/R = q_1 = 1, 2, 4, 8$  or  $16$ ,

$$R \geq 2^{-4} R'.$$

Recall the formula

$$R' = 16 \log \varepsilon R(\xi_1, \xi_2) R(\eta_1, \eta_2, \eta_3, \eta_4).$$

Then (4.4) and (4.8) give us a lower bound for  $R$  as follows:

**Theorem 5.** *Let  $R$  be the regulator of the field  $K_n$ . Then a lower bound for  $R$  is*

$$(2^{-6} \log \varepsilon) \log^6 a \quad (\approx 0.0137714623 \log^6 a).$$

This bound is much better than Silverman’s bound, since we have used more information about the field  $K_n$ . So we have an upper bound for the index  $q = [U : U_1]$ , where  $U_1 = \langle -1, \varepsilon, y_1, y_2, \rho_1, \rho_2, \rho_3, \rho_4 \rangle$ .

**Corollary.** *An upper bound for the index  $q = [U : U_1]$  is  $2^{10} R_y R_\rho \log^{-6} a$ , where  $R_y = R(y_1, y_2)$  and  $R_\rho = R(\rho_1, \rho_2, \rho_3, \rho_4)$ .*

*Remark.* As  $a \rightarrow \infty$ , from (3.3) we have

$$2^{10} R_y R_\rho \log^{-6} a \rightarrow 2^{10}.$$

So the index  $q = [U : U_1]$  is uniformly bounded.

To emphasize this result, we state it as follows:

**Theorem 6.** *Let  $U$  be the unit group of  $K_n$ , and let  $U_1$  be the subgroup generated by the units  $\rho_1, \rho_2, \rho_3, \rho_4, y_1, y_2$ , and  $\varepsilon$ . Then the index  $q = [U : U_1]$  is bounded, independent of  $a$ .*

To conclude this section, let us go back to estimate the class numbers of our real cyclic octic fields  $K_n$ , which was one of our original goals mentioned in the very beginning of this section. Since we have a sequence of cyclic octic number fields  $K_n$  with the property (by Theorem 3)

$$\frac{[K_n : \mathbf{Q}]}{\log |d(K_n)|} = \frac{8}{\log(2^{31} b_n^6)} \rightarrow 0 \quad \text{as } n \rightarrow \infty,$$

we may apply Brauer-Siegel’s theorem (see Lang [6, p. 321]), which yields

$$\frac{\log(hR)}{\log \sqrt{d(K_n)}} \rightarrow 1.$$

But  $R_1/R = q$  is uniformly bounded by Theorem 6, thus

$$C' \log^6 a < R < C \log^6 a \quad \text{for some } C, C'.$$

Therefore we have

$$\frac{\log h}{\frac{1}{2} \log(d(K_n))} \rightarrow 1,$$

and hence

$$\log h \sim \frac{1}{2} \log(d(K_n)) \sim 3 \log(a_n).$$

This means that the class number  $h$  of the field  $K_n$  is very large, as  $n \rightarrow \infty$ . So we have the following corollary of Theorem 6.

**Corollary.** *Let  $h$  be the class number of the field  $K_n$ . Then  $\log h \sim 3 \log(a_n)$  as  $n \rightarrow \infty$ .*

### 5. EXAMPLES AND CONJECTURES

We are trying to make a conjecture on the index  $q = [U : U_1]$  mentioned in Theorem 6 for the octic field  $K_n$ .

Since  $a_n + b_n\sqrt{2} = (\sqrt{2} + 1)^{2n+1}$ , we have the following recursion formulas and a table for  $a_n$  and  $b_n$ :

$$a_{n+1} = 3a_n + 4b_n, \quad b_{n+1} = 2a_n + 3b_n.$$

TABLE FOR  $a_n$  AND  $b_n$

$n$	$a_n$	$b_n$
0	1	1
1	7	5
2	41	29
3	239	169
4	1393	985
5	8119	5741
6	47321	33461
7	275807	195025
8	1607521	1136689
9	9369319	6625109
10	54608393	38613965
11	318281039	225058681
12	1855077841	1311738121
13	10812186007	7645370045
14	63018038201	44560482149
15	367296043199	259717522849

Note that since  $b_3 = 13^2$  and  $b_7 = 5^2 \times 7801$  are not squarefree, both are excluded from our discussion.

Now recall formula (27),

$$h = \frac{2^8 b^3 \log \varepsilon}{R} |L(1, \chi_4)|^2 |L(1, \chi_8)|^2 |L(1, \chi_8^3)|^2.$$

To simplify the calculation of  $|L(1, \chi)|$  we need the following:

**Proposition 9.** *Let  $\chi$  be a primitive character with conductor  $f$ , which is divisible by 4. Then  $\chi(a + \frac{f}{2}) = -\chi(a)$ , and hence  $\chi(\frac{f}{2} - a) = -\chi(a)$  if  $\chi$  is even.*

*Proof.* Since  $4|f$ ,

$$\left(1 + \frac{f}{2}\right)^2 = 1 + f + \frac{f}{4}f \equiv 1 \pmod{f}.$$

Therefore,  $\chi(1 + \frac{f}{2}) = \pm 1$ . For  $a$  odd, since  $\frac{f}{2}(a - 1) \equiv 0 \pmod{f}$ ,

$$a \left(1 + \frac{f}{2}\right) = a + a\frac{f}{2} \equiv a + \frac{f}{2} \pmod{f},$$

and hence

$$\chi\left(a + \frac{f}{2}\right) = \chi(a)\chi\left(1 + \frac{f}{2}\right).$$

Note that  $\chi(1 + \frac{f}{2})$  must be  $-1$ , otherwise  $\chi(a + \frac{f}{2}) = \chi(a) \forall \text{ odd } a$ ; which means that  $\chi$  is not primitive, a contradiction. Therefore  $\chi(a + \frac{f}{2}) = -\chi(a)$  for all odd  $a$ . For even  $a$ , both are zero. This completes the proof.

**Corollary.** *Let  $\chi$  be a primitive even character with conductor  $f$  which is divisible by 4. Then*

$$(5.1) \quad |L(1, \chi)| = \frac{2}{\sqrt{f}} \left| \sum_{a < f/4} \chi(a) \log \tan\left(\frac{a\pi}{f}\right) \right|.$$

*Proof.* It follows from (4.2) and the above proposition

Now we are ready to set up the calculations of the quotient  $q/h$ , for the first few examples,  $n = 0, 1, 2$ . Let us denote the quartic characters of  $K_n$  by  $\chi_{16b}, \bar{\chi}_{16b} = \chi_{16b}^3$ , and denote the octic ones by  $\chi_{32b}, \chi'_{32b} = \chi_{32b}^3, \bar{\chi}'_{32b} = \chi_{32b}^5, \bar{\chi}_{32b} = \chi_{32b}^7$ . With  $q = R_1/R$  in mind, put (3.1), (4.1), and (5.1) together; we have the following formula for  $q/h$ :

**Theorem 7.** *Let  $h$  be the class number of  $K_n$ , and let  $q = [U : U_1]$  be the index mentioned in Theorem 6. Then we have*

$$\frac{q}{h} = \frac{16R_y R_\rho}{L_{16b} L_{32b} L'_{32b}},$$

where

$$R_y = \log^2 |y_1| + \log^2 |y_2|, \quad y_i = \frac{1}{2} \left( \rho_i - \frac{1}{\rho_i} \right), \quad i = 1, 2;$$

$$R_\rho = \pm \det \begin{vmatrix} A_1 & A_2 & A_3 & A_4 \\ A_2 & A_3 & A_4 & -A_1 \\ A_3 & A_4 & -A_1 & -A_2 \\ A_4 & -A_1 & -A_2 & -A_3 \end{vmatrix}, \quad A_i = \log |\rho_i|, \quad i = 1, 2, 3, 4;$$

$$L_{16b} = \left| \sum_{k < 4b} \chi_{16b}(k) \log \tan \left( \frac{k\pi}{16b} \right) \right|^2,$$

$$L_{32b} = \left| \sum_{k < 8b} \chi_{32b}(k) \log \tan \left( \frac{k\pi}{32b} \right) \right|^2,$$

$$L'_{32b} = \left| \sum_{k < 8b} \chi_{32b}^3(k) \log \tan \left( \frac{k\pi}{32b} \right) \right|^2.$$

In the examples below, to determine which is the correct choice of  $\chi$ , we have used Proposition 25 in Chapter 1 of Lang’s book [6], along with the following fact:

*Fact.* Let  $p$  be an unramified rational prime in a number field  $K$ . Then we have

$$\chi(p) = \begin{cases} 1, & g = 8 \text{ (} p \text{ splits),} \\ -1, & g = 4, \\ \pm i, & g = 2, \\ \pm \zeta_8^{1,3,5,7}, & g = 1 \text{ (} p \text{ inert),} \end{cases}$$

where  $g$  is the number of primes in  $K$  lying above  $p$ , and  $\chi$  is a generator of the character group.

*Remarks.* (a) Note also our  $\chi$ ’s are always even characters, since our number fields are all totally real.

(b) We know that  $(\mathbf{Z}/16\mathbf{Z})^\times$  is generated by 3 and  $-1$ , thus  $\chi_{16}$  is determined by  $\chi_{16}(3)$  and  $\chi_{16}(-1)$ . Clearly,  $\chi_{16}(3) = \pm i$  and  $\chi_{16}(-1) = \pm 1$ .

(c) Similarly, we have  $\chi_{32}(3) = \pm \zeta_8^{1,3,5,7}$  and  $\chi_{32}(-1) = \pm 1$ .

Here are the calculations: Let  $\zeta = \zeta_8 = \exp(2\pi i/8)$ .

(A) For  $n = 0, a = 1, b = 1: f = 16$

$$\begin{aligned} \rho_1 &\sim 10.1531703876, & A_1 &\sim 2.31778601017, \\ \rho_2 &\sim 1.87086841179, & A_2 &\sim 0.626402714402, \\ \rho_3 &\sim -1.21850352559, & A_3 &\sim 0.197623487464, \\ \rho_4 &\sim -3.29655820893, & A_4 &\sim 1.19287895721, \\ y_1 &\sim 5.0273394921, & y_2 &\sim 0.66817863792. \end{aligned}$$

Therefore,

$$R_\rho \sim 50.4046133952, \quad R_y \sim 2.77044268466.$$

Note that the quartic character  $\chi_{16}$  is determined by  $\chi_{16}(3) = i$  and  $\chi_{16}(-1) = 1$ , and the octic character  $\chi_{32}$  is determined by  $\chi_{32}(3) = \zeta$  and  $\chi_{32}(-1) = 1$ .

Therefore, we have

$$L_{16} = \left| \sum_{a<4} \chi_{16}(a) \log \tan \left( \frac{a\pi}{16} \right) \right|^2 \sim 2.77044268468,$$

$$L_{32} = \left| \sum_{a<8} \chi_{32}(a) \log \tan \left( \frac{a\pi}{32} \right) \right|^2 \sim 8.57489233007,$$

$$L'_{32} = \left| \sum_{a<8} \chi_{32}^3(a) \log \tan \left( \frac{a\pi}{32} \right) \right|^2 \sim 5.87816247538.$$

A calculation yields  $q/h \sim 16.0000009745$ . Therefore we must have  $q/h = 16$  in the field  $K_0$ . Note that  $K_0$  is contained in the cyclotomic field  $\mathbf{Q}(\zeta_{32})$ , whose class number is 1. Since  $\mathbf{Q}(\zeta_{32})/K_0$  is totally ramified, we must have  $h = 1$ , by class field theory (Theorem 10.1 in Washington's book [13]), and hence  $q = 16$ .

*Remarks.* (a) Observe that we have  $L_{16} = R_y$  and  $L_{32}L'_{32} = R_\rho$ .

(b) Let

$$B_1 = \log \tan (\pi/32), \quad B_2 = \log \tan (5\pi/32),$$

$$B_3 = \log \tan (7\pi/32), \quad B_4 = \log \tan (3\pi/32).$$

Then

$$L_{32}L'_{32} = \sum_{i=1}^4 B_i^4 + 2(B_1^2B_3^2 + B_2^2B_4^2) + 4(B_1B_2 + B_3B_4)(B_1B_4 - B_2B_3),$$

which is the determinant as in  $R_\rho$ , i.e.,

$$L_{32}L'_{32} = \pm \begin{vmatrix} B_1 & B_2 & B_3 & B_4 \\ B_2 & B_3 & B_4 & -B_1 \\ B_3 & B_4 & -B_1 & -B_2 \\ B_4 & -B_1 & -B_2 & -B_3 \end{vmatrix}.$$

(c) Even better, we have

$$\rho_1 = \cot(\pi/32), \quad \rho_2 = \cot(5\pi/32),$$

$$\rho_3 = -\cot(7\pi/32), \quad \rho_4 = \cot(3\pi/32).$$

**(B)** For  $n = 1$ ,  $a = 7$ ,  $b = 5$ :  $f = 160$

$$\rho_1 \sim 56.3729885432, \quad A_1 \sim 4.03199011724,$$

$$\rho_2 \sim 2.29805856808, \quad A_2 \sim 0.832064665647,$$

$$\rho_3 \sim -1.03611869347, \quad A_3 \sim 0.0354817062613,$$

$$\rho_4 \sim -2.54076252734, \quad A_4 \sim 0.932464243591,$$

$$y_1 \sim 28.1776247756, \quad y_2 \sim 0.931454324485.$$

Therefore,

$$R_\rho \sim 317.319066816, \quad R_y \sim 11.1508127982.$$

Note that the quartic character is  $\chi_{80} = \chi_5 \chi_{16}$ , where  $\chi_5$  is quadratic and is uniquely determined by  $\chi_5(2) = -1$ . It is easy to see that  $\chi_5$  is even, so we must choose an even  $\chi_{16}$ ; one choice for  $\chi_{16}$  is determined by  $\chi_{16}(3) = i$  and  $\chi_{16}(-1) = 1$ . Therefore, we have

$$L_{80} = \left| \sum_{a < 20} \chi_{80}(a) \log \tan \left( \frac{a\pi}{80} \right) \right|^2 \sim 22.3016255964.$$

For the octic character  $\chi_{160} = \chi_5 \chi_{32}$ , where  $\chi_5$  is quartic and  $\chi_5(2)$  has two choices, both are odd, and we choose the one determined by  $\chi_5(2) = i$ . Thus we need odd octic  $\chi_{32}$ . There are four choices for  $\chi_{32}(3)$ . To make a right decision, we use Proposition 25 in Lang's book [6]. Reduced to modulo 23,  $Q(X)$  is factored into the product of four squares of irreducibles; this says  $g = 4$  and  $\chi_{160}(23)$  must be  $-1$ , which forces us to choose  $\chi_{32}(3) = \zeta$  and  $\chi_{32}(-1) = -1$ . Therefore, we have

$$L_{160} = \left| \sum_{a < 40} \chi_{160}(a) \log \tan \left( \frac{a\pi}{160} \right) \right|^2 \sim 59.189069019$$

and

$$L'_{160} = \left| \sum_{a < 40} \chi_{160}^3(a) \log \tan \left( \frac{a\pi}{160} \right) \right|^2 \sim 10.7222176717.$$

A calculation yields  $q/h \sim 4.00000032779$ , and hence we must have  $q/h = 4$ . Note also,  $L_{80} = 2R_y$  and  $L_{160}L'_{160} = 2R_\rho$ . To calculate the class number  $h$ , we use Theorem 3 of Van der Linden's paper [12], and Theorem 3.5 in Washington's book [13] as follows:

Since  $K_1$  and its Hilbert class field  $H(K_1) = H$  are both in the maximal real subfield  $\mathbf{Q}(\zeta_{160})^+$  of the cyclotomic field  $\mathbf{Q}(\zeta_{160})$ , by Van der Linden's results and

$$[\mathbf{Q}(\zeta_{160}) : \mathbf{Q}] = \phi(160) = 64, \quad [K_1 : \mathbf{Q}] = 8,$$

we have  $h = [H : K_1]$  divides 4. Therefore  $h = 1, 2$  or  $4$ . Thus we have

$$h = [H : K_1][\langle \chi_5, \chi_{32} \rangle_{\text{even}} : \langle \chi_{160} \rangle].$$

Since the order of  $\chi_{160}$  is 8, and clearly

$$\langle \chi_5, \chi_{32} \rangle = \{ \chi_5^a \chi_{32}^b \mid a + b = \text{even} \}$$

has order 16, we have  $h = 2$ , and hence  $q = 8$  in this case.

(C) For  $n = 2$ ,  $a = 41$ ,  $b = 29$ :  $f = 928$

$$\begin{aligned}\rho_1 &\sim 328.064014277, & A_1 &\sim 5.79320875482, \\ \rho_2 &\sim 2.39355130221, & A_2 &\sim 0.872778163592, \\ \rho_3 &\sim -1.00611501086, & A_3 &\sim 0.0060939005349, \\ \rho_4 &\sim -2.43518218298, & A_4 &\sim 0.890021572208, \\ y_1 &\sim 164.030483046, & y_2 &\sim 0.98788102681.\end{aligned}$$

Therefore,

$$R_p \sim 1233.06032039, \quad R_y \sim 26.0106819565.$$

The quartic character is  $\chi_{464} = \chi_{29}\chi_{16}$ , where  $\chi_{29}$  is quadratic and even, which is determined by  $\chi_{29}(2) = -1$ . Thus we must choose  $\chi_{16}$  even, which is determined by  $\chi_{16}(3) = i$  and  $\chi_{16}(-1) = 1$ . Therefore, we have

$$L_{464} = \left| \sum_{a < 116} \chi_{464}(a) \log \tan \left( \frac{a\pi}{464} \right) \right|^2 = |A + iB|^2 \sim 52.021363913,$$

where

$$A = \log \left( \frac{\tan(\pi/464) \cdots \tan(111\pi/464)}{\tan(7\pi/464) \cdots \tan(113\pi/464)} \right) \sim \sqrt{26.1350518997}$$

and

$$B = \log \left( \frac{\tan(11\pi/464) \cdots \tan(115\pi/464)}{\tan(3\pi/464) \cdots \tan(107\pi/464)} \right) \sim \sqrt{25.8863120133}.$$

Finally the octic character is  $\chi_{928} = \chi_{29}\chi_{32}$ , where  $\chi_{29}$ , which is determined by  $\chi_{29}(2) = -i$ , is odd, and hence  $\chi_{32}$  must be odd. As before, a correct one is determined by  $\chi_{32}(3) = \zeta$  and  $\chi_{32}(-1) = -1$ . Therefore, we have

$$L_{928} = \left| \sum_{a < 232} \chi_{928}(a) \log \tan \left( \frac{a\pi}{928} \right) \right|^2 = |B_1 + \zeta B_2 + iB_3 + \zeta^3 B_4|^2,$$

where

$$B_1 = \log \left( \frac{\tan(\pi/928) \cdots \tan(215\pi/928)}{\tan(33\pi/928) \cdots \tan(225\pi/928)} \right) \sim 0.849438364885,$$

$$B_2 = \log \left( \frac{\tan(21\pi/928) \cdots \tan(229\pi/928)}{\tan(11\pi/928) \cdots \tan(213\pi/928)} \right) \sim 10.707542956,$$

$$B_3 = \log \left( \frac{\tan(7\pi/928) \cdots \tan(199\pi/928)}{\tan(9\pi/928) \cdots \tan(231\pi/928)} \right) \sim -8.44603006283,$$

$$B_4 = \log \left( \frac{\tan(5\pi/928) \cdots \tan(219\pi/928)}{\tan(3\pi/928) \cdots \tan(221\pi/928)} \right) \sim -4.91537996272.$$

Therefore,

$$L_{928} L'_{928} = \pm \det \begin{vmatrix} B_1 & B_2 & B_3 & B_4 \\ B_2 & B_3 & B_4 & -B_1 \\ B_3 & B_4 & -B_1 & -B_2 \\ B_4 & -B_1 & -B_2 & -B_3 \end{vmatrix} \sim 41924.0508935.$$

Observe that

$$L_{928}L'_{928} = 34R_\rho, \quad L_{464} = 2R_y.$$

So we have

$$\frac{q}{h} = \frac{16R_yR_\rho}{(2R_y)(34R_\rho)} = \frac{4}{17}.$$

To calculate the class number, we let  $L$  be the quartic field between  $\mathbf{Q}(\zeta_{29})$  and  $\mathbf{Q}$ . Clearly, our field  $K_2$  is contained in  $L(\zeta_{29})$ . Theorem 10.4(b) in Washington's book [13], implies  $2 \nmid h(L)$ . Since 2 is a primitive root modulo 29, we have 2 is inert in  $\mathbf{Q}(\zeta_{29})/\mathbf{Q}$ , and hence  $(2) = \text{prime}$  in  $L$ . Thus, only one prime ramifies in  $L(\zeta_{29})/L$ . Theorem 10.4(a) in Washington's book implies  $2 \nmid h(L(\zeta_{32}))$ . Let  $H_2 = 2$ -part of the Hilbert class field of  $K_2$ . Then

$$H_2 \subseteq L(\zeta_{32}), \quad \text{since } 2 \nmid h(L(\zeta_{32})).$$

Again we have

$$[H_2 : K_2] = [\langle \chi_{29}, \chi_{32} \rangle_{\text{even}} : \langle \chi_{928} \rangle] = 2.$$

Therefore 2-part of  $h(K_2)$  is 2, and probably  $h = 2 \times 17 = 34$ . Hence, probably, we have  $q = 8$ , and we know that  $q$  is 8 times an odd number.

(D) For  $n = 4$ ,  $a = 1393$ ,  $b = 985$ :  $f = 31520$

$$R_y = 74.3994141935, \quad R_\rho = 7812.96909763, \\ L_{16b}/R_y = 68, \quad L_{32b}L'_{32b}/R_\rho = 4964 = 4 \cdot 1241.$$

Hence  $h/q = 1241 \cdot 17$ . As above, genus theory implies that  $8|h$ , but we do not know the exact power of 2 for  $h$ . This happens probably because 985 is a composite number. Therefore the only thing we can say is

$$8|q,$$

and hence probably we have  $q = 8$ .

(E) For  $n = 5$ ,  $a = 8119$ ,  $b = 5741$ :  $f = 183712$

$$R_y = 107.915875995, \quad R_\rho = 15463.2083598, \\ L_{16b}/R_y = 130 = 2 \cdot 65, \quad L_{32b}L'_{32b}/R_\rho = 135458 = 2 \cdot 67729.$$

Hence  $h/q = (67729 \cdot 65)/4$ . As above, genus theory implies that  $2|h$ . Since 2 is a primitive root mod 5741, 2 is inert in the field  $\mathbf{Q}(\zeta_{5741})$ . This implies that 2 does not divide the class number of the genus field. Therefore  $2 \parallel h$ , and hence  $2^3 \parallel q$ . Again we have

$$q = 8 \cdot (\text{odd}),$$

and hence probably we have  $q = 8$ .

So now from our examples above, we suspect that for  $n > 0$ , the index  $q = 8$ . For  $n = 0$ , the index  $q = 16$ , which is probably because the conductor of  $K_0$  is a prime power. Therefore we may make the following conjecture.

**Conjecture 1.** For  $n > 0$  with  $b_n$  squarefree, the index  $q = [U : U_1]$  is 8.

From this conjecture, we should be able to find some unit whose square root is also a unit in  $U$ . To do so, it is better to observe what happens to the quartic subfield  $\mathbf{Q}(y)$ . By exactly the same argument as in Theorem 7, we have the following:

**Proposition 10.** Let  $h_y$  be the class number of  $\mathbf{Q}(y)$ , and let  $q_y = [U_y : U_{1y}]$ , where  $U_y$  is the full unit group of  $\mathbf{Q}(y)$ , and  $U_{1y} = \langle \pm 1, \varepsilon, y_1, y_2 \rangle$ . Then we have

$$\frac{q_y}{h_y} = \frac{2R_y}{L_{16b}},$$

where  $R_y = \log^2 |y_1| + \log^2 |y_2|$  and

$$L_{16b} = \left| \sum_{k < 4b} \chi_{16b}(k) \log \tan \left( \frac{k\pi}{16b} \right) \right|^2.$$

A calculation yields  $q_y = 2$  for  $n = 0, 1, 2$ . This says that there exists a unit in  $U_{1y}$ , whose square root is a unit in  $U_y$ . It is clear that such a unit must be totally positive and it is easy to see that  $y_1 y_2 \varepsilon$  is one such unit in  $U_{1y}$ . We know  $y_1 = y$ ,  $y_2 = (y - 1)/(y + 1)$ , and

$$\begin{aligned} z &= \frac{1}{4}(\rho_1 + \rho_3 + \rho_5 + \rho_7) = \frac{1}{2}(y - \frac{1}{y}) \\ &= a + \sqrt{a^2 + 1} = a + \sqrt{2}b = \varepsilon^{2n+1}, \end{aligned}$$

by equation (9). So we have the following:

$$y_1 y_2 \varepsilon = y_1 y_2 z \varepsilon^{-2n} = y \left( \frac{y - 1}{y + 1} \right) \left( \frac{y^2 - 1}{2y} \right) \varepsilon^{-2n} = \frac{(y - 1)^2}{2\varepsilon^{2n}}.$$

Therefore

$$\sqrt{y_1 y_2 \varepsilon} = \frac{y - 1}{\sqrt{2}\varepsilon^n}, \quad \text{since } y > 1.$$

Let  $\xi = (y - 1)/(\sqrt{2}\varepsilon^n)$ ; then  $\xi \in \mathbf{Q}(y)$  and  $\xi$  is a unit. Therefore  $\xi \in U_y$ . Now the units  $\varepsilon, y, \xi$  are independent, and the index  $[U_y : \langle \pm 1, y, \xi \rangle]$  must be 1 for  $n = 0, 1, 2$ . Therefore they form a system of fundamental units of the quartic subfield  $\mathbf{Q}(y)$  for  $n = 0, 1, 2$ . In general, M.-N. Gras [4] showed that  $q_y = 1$  or 2, in any simplest quartic field. Thus the index  $q_y$  in our quartic subfield  $\mathbf{Q}(y)$  must be 2 for all  $n$  with  $b_n$  squarefree, and hence we have the following:

**Theorem 8.** In the quartic subfield  $\mathbf{Q}(y)$  of the octic field  $K_n$ , let  $h_y$  be its class number, and let  $q_y = [U_y : U_{1y}]$ , where  $U_y$  is the full unit group of  $\mathbf{Q}(y)$ , and  $U_{1y} = \langle \pm 1, \varepsilon, y_1, y_2 \rangle$ . Then for all  $n \in \mathbf{N}$  with  $b_n$  squarefree, we have

- (a)  $q_y = 2$ ,
- (b) the units  $\varepsilon, y, \xi = (y - 1)/(\sqrt{2}\varepsilon^n)$  form a system of fundamental units for  $\mathbf{Q}(y)$ ,

(c)

$$h_y = \left| \sum_{k < 4b} \chi_{16b}(k) \log \tan \left( \frac{k\pi}{16b} \right) \right|^2 / \left[ \log^2 y + \log^2 \left( \frac{y-1}{y+1} \right) \right],$$

(d)  $\log h_y \sim \log a$ , as  $n \rightarrow \infty$ .

Now let us go back to the octic field  $K_n$ . We are looking for some totally positive units in  $U_1$ . It is easy to see  $-\rho_1 \rho_3 y_1$  is totally positive and

$$-\rho_1 \rho_3 y_1 = -\rho \left( \frac{-\rho-1}{\rho-1} \right) \left( \frac{\rho^2-1}{2\rho} \right) = \frac{(\rho+1)^2}{2}.$$

Therefore  $\sqrt{-\rho_1 \rho_3 y_1} = (\rho+1)/\sqrt{2}$ . Let  $\eta = (\rho+1)/\sqrt{2}$ , and let  $\eta_k = \eta^{\sigma_{k-1}}$ ,  $k = 1, 2, 3, \dots, 8$ . Then

$$\eta_k = \frac{\rho_k + 1}{(-1)^{k-1} \sqrt{2}}, \quad k = 1, 2, 3, \dots, 8.$$

Therefore we have

$$\prod_{k=1}^8 \eta_k = \frac{1}{16} \prod_{k=1}^8 (\rho_k + 1) = \frac{1}{16} P(1) = 1,$$

by equation (3). For the sum, we have

$$\sum_{k=1}^8 \eta_k = \frac{1}{\sqrt{2}} (4z_1 - 4z_2) = 2\sqrt{2}(z_1 - z_2).$$

But  $z_1 + z_2 = 2a$  and  $z_1 z_2 = -1$  imply

$$z_1 - z_2 = \sqrt{4a^2 + 4} = 2\sqrt{2}b.$$

Therefore

$$\sum_{k=1}^8 \eta_k = 8b.$$

It is very easy to see that  $\eta$  is a unit in  $U$ , since  $\eta^2$  is a unit and  $\eta \in K_n$ . However, to work out its minimal polynomial takes a lot of time. A calculation yields that the minimal polynomial of  $\eta$  is

$$X^8 - 8bX^7 - 4aX^6 + 40bX^5 - 6X^4 - 40bX^3 + 4aX^2 + 8bX + 1.$$

Clearly, the units  $\varepsilon, y, \xi, \rho_1, \rho_2, \eta_1, \eta_2$  are independent in  $U$ , and for  $n = 1, 2$ , the index

$$[U : \langle \pm 1, y, \xi, \rho_1, \rho_2, \eta_1, \eta_2 \rangle] = 1.$$

Therefore these seven units form a system of fundamental units for  $n = 1, 2$ . Hence we make the following conjecture for all  $n > 0$ .

**Conjecture 2.** The units  $\varepsilon, \gamma, \xi, \rho_1, \rho_2, \eta_1, \eta_2$  in the ring of algebraic integers of the field  $K_n$  form a system of fundamental units for all  $n > 0$ , such that  $b_n$  is squarefree.

### 6. A POSSIBLE GENERALIZATION TO $2^n$ -TIC FIELDS

Now, let us analyse what we have so far. In the simplest quadratic field, we have the polynomial

$$P_2(X) = X^2 - aX - 1 = (X^2 - 1) - aX.$$

Let  $Q_1(X) = X$ , and let  $Q_2(X) = X^2 - 1$ . Then

$$P_2(X) = Q_2(X) - aQ_1(X).$$

In the simplest quartic field, we have the polynomial

$$P_4(X) = X^4 - aX^3 - 6X^2 + aX + 1 = (X^4 - 6X^2 + 1) - aX(X^2 - 1).$$

Let  $Q_4(X) = X^4 - 6X^2 + 1$ . Then

$$P_4(X) = Q_4(X) - aQ_1(X)Q_2(X).$$

In the simplest octic field, we have the polynomial

$$\begin{aligned} P_8(X) &= X^8 - aX^7 - 28X^6 + 7aX^5 + 70X^4 - 7aX^3 - 28X^2 + aX + 1 \\ &= (X^8 - 28X^6 + 70X^4 - 28X^2 + 1) - aX(X^2 - 1)(X^4 - 6X^2 + 1). \end{aligned}$$

Let  $Q_8(X) = X^8 - 28X^6 + 70X^4 - 28X^2 + 1$ . Then

$$P_8(X) = Q_8(X) - aQ_1(X)Q_2(X)Q_4(X).$$

Note that

$$\begin{aligned} Q_1(X) &= Q_{2^0}(X) = X = \Re(X + i), \\ Q_2(X) &= X^2 - 1 = \Re(X + i)^2, \\ Q_4(X) &= X^4 - 6X^2 + 1 = X^4 - \binom{4}{2}X^2 + 1 = \Re(X + i)^4, \end{aligned}$$

and

$$Q_8(X) = X^8 - \binom{8}{2}X^6 + \binom{8}{4}X^4 - \binom{8}{6}X^2 + 1 = \Re(X + i)^8.$$

Hence the next one,  $Q_{16}(X)$ , should be the real part of  $(X + i)^{16}$ , and

$$P_{16}(X) = Q_{16}(X) - aQ_1(X)Q_2(X)Q_4(X)Q_8(X).$$

In general, for  $n = 0, 1, 2, \dots$ , let  $Q_{2^n}(X)$  be the real part of  $(X + i)^{2^n}$ , which is

$$X^{2^n} - \binom{2^n}{2}X^{2^n-2} + \binom{2^n}{4}X^{2^n-4} - \dots + \binom{2^n}{2^n-4}X^4 - \binom{2^n}{2^n-2}X^2 + 1.$$

Let

$$P_{2^n}(X) = Q_{2^n}(X) - a \prod_{k=0}^{n-1} Q_{2^k}(X) \quad \text{for } a \in \mathbf{Z}, \quad n = 1, 2, 3, \dots$$

Write  $P_{2^n}(X; a) = P_{2^n}(X)$ . Then  $Q_{2^n}(X) = P_{2^n}(X; 0) = \Re(X + i)^{2^n}$ . Note also that in fact, we have

$$(6.1) \quad P_{2^n}(X) = \Re(X + i)^{2^n} - \frac{a}{2^n} \Im(X + i)^{2^n}.$$

To prove equation (6.1), it suffices to prove

$$\prod_{k=0}^{n-1} \Re(X + i)^{2^k} = \frac{1}{2^n} \Im(X + i)^{2^n}.$$

But this is true by induction on  $n$ .

As expected, we have the following:

**Proposition 11.** *Let  $N = 2^n$ . Then  $P_N(X) = 0$  has  $2^n$  distinct real roots.*

*Proof.* The proof is by induction on  $n$ . See Shen [9].

*Remark. Claim.* If  $\rho$  is a real root of  $P_N(X) = 0$ , then so is  $(\varepsilon\rho - 1)/(\rho + \varepsilon)$ .

To see this, we let

$$\alpha = \rho + i, \quad \beta = \frac{\varepsilon\rho - 1}{\rho + \varepsilon} + i.$$

Then

$$(6.2) \quad P_N(\rho) = \Re(\alpha^N) - \frac{a}{N} \Im(\alpha^N) = 0.$$

A calculation shows

$$\beta = \frac{\alpha}{\rho + \varepsilon}(\varepsilon + i).$$

Note that  $\rho + \varepsilon \in \mathbf{R}$  and

$$(\varepsilon + i)^N = -(\Im(\varepsilon + i)^{N/2})^2 \in \mathbf{R},$$

since  $\Re(\varepsilon + i)^{N/2} = Q_{N/2}(\varepsilon) = 0$ , and hence  $(\varepsilon + i)^{N/2} = i\Im(\varepsilon + i)^{N/2}$  is purely imaginary. Therefore  $\beta^N = c\alpha^N$  for some  $c \in \mathbf{R}$ . Hence we have

$$\begin{aligned} P_N\left(\frac{\varepsilon\rho - 1}{\rho + \varepsilon}\right) &= \Re(\beta^N) - \frac{a}{N} \Im(\beta^N), \\ &= c\Re(\alpha^N) - \frac{a}{N} c\Im(\alpha^N), \\ &= c(\Re(\alpha^N) - \frac{a}{N} \Im(\alpha^N)), \\ &= 0 \quad (\text{by equation (6.2)}). \end{aligned}$$

This proves the claim.

**Proposition 12.** Let  $\rho$  be a root of  $P_{2^n}(X) = 0$ , and let  $\varepsilon$  be the largest root of  $Q_{2^{n-1}}(X) = 0$ . Then the transformation  $\sigma(\rho) = (\varepsilon\rho - 1)/(\rho + \varepsilon)$  has order  $2^n$ . In other words, the  $2 \times 2$  matrix

$$A = \begin{pmatrix} \varepsilon & -1 \\ 1 & \varepsilon \end{pmatrix},$$

is of order  $2^n$ , in the group  $\mathbf{PGL}_2(\mathbf{R})$ .

(The proof is given below.)

**Examples.** (a) For  $n = 1$ . The root of  $Q_1(X) = 0$  is 0, thus  $\varepsilon = 0$ , and hence  $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  is of order 2.

(b) For  $n = 2$ . The roots of  $Q_2(X) = 0$  are  $\pm 1$ , thus  $\varepsilon = 1$ , and hence  $A = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$  is of order 4.

(c) For  $n = 3$ . The roots of  $Q_4(X) = 0$  are  $\pm(\sqrt{2} + 1)$ ,  $\pm(\sqrt{2} - 1)$ , thus  $\varepsilon = \sqrt{2} + 1$ , and hence  $A = \begin{pmatrix} \varepsilon & -1 \\ 1 & \varepsilon \end{pmatrix}$  is of order 8.

(d) For  $n = 4$ . The roots of  $Q_8(X) = 0$  are

$$\pm \left( \sqrt{2} + 1 \pm \sqrt{4 + 2\sqrt{2}} \right), \quad \pm \left( \sqrt{2} - 1 \pm \sqrt{4 - 2\sqrt{2}} \right).$$

Therefore

$$\varepsilon = \sqrt{2} + 1 + \sqrt{4 + 2\sqrt{2}} \sim 5.02733949213,$$

and hence  $A = \begin{pmatrix} \varepsilon & -1 \\ 1 & \varepsilon \end{pmatrix}$  is of order 16.

*Proof of Proposition 12.* We prove that  $A$  is of order  $2^n$ . Since  $A$  has two distinct eigenvalues  $\varepsilon + i$ , and  $\varepsilon - i$ ,  $A$  must be similar to the diagonal matrix

$$D = \begin{pmatrix} \varepsilon + i & 0 \\ 0 & \varepsilon - i \end{pmatrix}.$$

Clearly,  $A$  and  $D$  have the same order. Hence it suffices to show that  $D$  is of order  $2^n$ . Now

$$D\rho = \frac{\varepsilon + i}{\varepsilon - i}\rho = \zeta\rho,$$

where  $\zeta = (\varepsilon + i)/(\varepsilon - i)$ . Note that  $\varepsilon$  is real and

$$Q_{2^{n-1}}(\varepsilon) = 0 = \Re(\varepsilon + i)^{2^{n-1}}.$$

Therefore

$$(\varepsilon + i)^{2^{n-1}} = \Re(\varepsilon + i)^{2^{n-1}} + i\Im(\varepsilon + i)^{2^{n-1}} = i\Im(\varepsilon + i)^{2^{n-1}},$$

and hence

$$(\varepsilon - i)^{2^{n-1}} = \overline{(\varepsilon + i)^{2^{n-1}}} = -i\Im(\varepsilon + i)^{2^{n-1}}.$$

All these imply

$$\zeta^{2^{n-1}} = \left( \frac{\varepsilon + i}{\varepsilon - i} \right)^{2^{n-1}} = -1,$$

and thus  $\zeta$  is of order  $2^n$ . But  $D\rho = \zeta\rho$ , so the result follows immediately.

Everything described above is very nice. However, when  $n$  is getting large, a lot of difficulties arise. In the octic case, we were able to select a family of  $a$ , so that the generating fields are cyclic, and  $\mathbf{Q}(\sqrt{2}) = \mathbf{Q}(\varepsilon)$  is always the unique quadratic subfield in every field of the family. For  $n \geq 4$ , we have the same problem and the selection of  $a$  to make the generating fields cyclic or even Galois becomes much harder. Anyway, this is a possible generalization to  $2^n$ -tic algebraic number fields, and still a lot of work remains to be done. So this is not the end of the story, instead it is the beginning of another story.

#### REFERENCES

1. G. Cornell and L. C. Washington, *Class numbers of cyclotomic fields*, J. Number Theory **21** (1985), 260–274.
2. T. W. Cusick, *Lower bounds for regulators*, in Number Theory (Noordwijkerhout 1983, Proc. Journées Arithmétiques), Lecture Notes in Math., vol. 1068, Springer-Verlag, New York, 1984.
3. M. N. Gras, *Special units in real cyclic sextic fields*, Math. Comp. **48** (1977), 179–182.
4. —, *Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de  $\mathbf{Q}$* , Publ. Math. Fac. Sci. Besançon **2** (1977/78), 1–26, 1–53.
5. A. Korkine and G. Zolotareff, *Sur les formes quadratiques positives quaternaires*, Math. Ann. **5** (1872), 581–583.
6. S. Lang, *Algebraic number theory*, Graduate Texts in Math., no. 110, Springer-Verlag, New York, 1986.
7. D. A. Marcus, *Number fields*, Universitext, Springer-Verlag, New York, 1977.
8. D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137–1152.
9. Y. Y. Shen, *Units of real cyclic octic fields*, Ph. D. Dissertation, University of Maryland at College Park, 1988.
10. C. L. Siegel, *The integer solutions of the equation  $y^2 = ax^n + bx^{n-1} + \dots + k$* , J. London Math. Soc. **1** (1926), 66–88 (=Gesammelte Abhandlungen, Band I, pp. 207–208).
11. J. H. Silverman, *An inequality relating the regulator and the discriminant of a number field*, J. Number Theory **19** (1984), 437–442.
12. F. Van der Linden, *Class number computations of real abelian number fields*, Math. Comp. **39** (1982), 693–707.
13. L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math., no. 83, Springer-Verlag, New York, 1982.

DEPARTMENT OF MATHEMATICS, THE CATHOLIC UNIVERSITY OF AMERICA, WASHINGTON D.C.  
20064