Blair K. Spearman; Kenneth S. Williams

The conductor of a cyclic quartic field using Gauss sums

Czechoslovak Mathematical Journal, Vol. 47 (1997), No. 3, 453–462

Persistent URL: `http://dml.cz/dmlcz/127369`

THE CONDUCTOR OF A CYCLIC QUARTIC FIELD USING GAUSS SUMS

Blair K. Spearman, Kelowna and Kenneth S. Williams[1], Ottawa

(Received December 12, 1994)

Abstract. Let Q denote the field of rational numbers. Let K be a cyclic quartic extension of Q. It is known that there are unique integers A, B, C, D such that

$$K = Q\Big(\sqrt{A(D+B\sqrt{D})}\Big),$$

where

$$\begin{aligned}&A \text{ is squarefree and odd,}\\ &D = B^2 + C^2 \text{ is squarefree, } B > 0,\ C > 0,\\ &GCD(A, D) = 1.\end{aligned}$$

The conductor $f(K)$ of K is $f(K) = 2^l|A|D$, where

$$l = \begin{cases} 3, & \text{if } D \equiv 2 \pmod 4 \text{ or } D \equiv 1 \pmod 4,\ B \equiv 1 \pmod 2,\\ 2, & \text{if } D \equiv 1 \pmod 4,\ B \equiv 0 \pmod 2,\ A + B \equiv 3 \pmod 4,\\ 0, & \text{if } D \equiv 1 \pmod 4,\ B \equiv 0 \pmod 2,\ A + B \equiv 1 \pmod 4.\end{cases}$$

A simple proof of this formula for $f(K)$ is given, which uses the basic properties of quartic Gauss sums.

Let $\mathbb{Q}$ denote the field of rational numbers. Let K be a cyclic extension of $\mathbb{Q}$ of degree 4. It is known [1, Theorem 1] that there exist unique integers A, B, C, D such that

$$K = \mathbb{Q}\Big(\sqrt{A(D+B\sqrt{D})}\Big), \tag{1}$$

[1] Research supported by Natural Sciences and Engineering Research of Canada Grant A-7233.

where

$$A \text{ is squarefree and odd,} \tag{2}$$
$$D = B^2 + C^2 \text{ is squarefree, } B > 0,\ C > 0, \tag{3}$$
$$GCD(A, D) = 1. \tag{4}$$

The minimal polynomial of $\sqrt{A(D + B\sqrt{D})}$ is $X^4 - 2ADX^2 + A^2C^2D$ whose roots are $\pm\sqrt{A(D + B\sqrt{D})}$ and $\pm\sqrt{A(D - B\sqrt{D})}$. It is convenient to consider three cases as follows:

$$(5)_1 \qquad \begin{cases} \text{Case 1}: & D \equiv 2 \pmod 4, \\ \text{Case 2}: & D \equiv 1 \pmod 4, \quad B \equiv 1 \pmod 2, \\ \text{Case 3}: & D \equiv 1 \pmod 4, \quad B \equiv 0 \pmod 2. \end{cases}$$

We also divide case 3 into two subcases according as

$$(5)_2 \qquad \begin{cases} \text{(a)} & A + B \equiv 3 \pmod 4, \\ \text{(b)} & A + B \equiv 1 \pmod 4. \end{cases}$$

We note that

$$\begin{cases} B \equiv C \equiv 1 \pmod 2,\ D \equiv 2 \pmod 8, & \text{in case 1}, \\ C \equiv 0 \pmod 2, & \text{in case 2}, \\ C \equiv 1 \pmod 2, & \text{in case 3}, \end{cases} \tag{6}$$

and

$$\begin{cases} D \equiv 1 + 2C \pmod 8, & \text{in case 2}, \\ D \equiv -1 - 2A \equiv 1 + 2B \pmod 8, & \text{in case 3(a)}, \\ D \equiv 3 - 2A \equiv 1 + 2B \pmod 8, & \text{in case 3(b)}. \end{cases} \tag{7}$$

We set

$$l = l(K) = \begin{cases} 3, & \text{in cases 1 and 2}, \\ 2, & \text{in case 3(a)}, \\ 0, & \text{in case 3(b)}. \end{cases} \tag{8}$$

In [1, Theorem 5] the conductor of the field K was determined using p-adic arithmetic.

Theorem. *The conductor $f(K)$ of the cyclic quartic field K, as given in* (1)–(4), *is*

$$f(K) = 2^l|A|D, \tag{9}$$

where l is defined in (8).

In this paper we give a simpler proof of this theorem than the one given in [1]. Instead of p-adic arithmetic, we use the basic properties of quartic Gauss sums, as given for example in [2].

Since $D = (\pm B)^2 + (\pm C)^2$ and $K = \mathbb{Q}\left(\sqrt{A(D \pm B\sqrt{D})}\right)$, we are at liberty to change the signs of B and C without changing the field K. We do this as follows:

$$\left\{\begin{array}{ll} \text{Case 1:} & \text{replace } B \text{ by } -B \text{ if necessary and } C \text{ by } -C \text{ if necessary so that} \\ & \quad B \equiv C \equiv 1 \pmod 4; \\ \text{Case 2:} & \text{replace } B \text{ by } -B \text{ if necessary so that} \\ & \quad B \equiv \begin{cases} 1 \pmod 4, & \text{if } D \equiv 1 \pmod 8, \\ 3 \pmod 4, & \text{if } D \equiv 5 \pmod 8; \end{cases} \\ \text{Case 3:} & \text{replace } C \text{ by } -C \text{ if necessary so that} \\ & \quad C \equiv \begin{cases} 1 \pmod 4, & \text{if } D \equiv 1 \pmod 8, \\ 3 \pmod 4, & \text{if } D \equiv 5 \pmod 8). \end{cases} \end{array}\right. \tag{10}$$

The choices of B and C in (10) will always be assumed from this point on.

Next we define a Gaussian integer κ (that is, an integer of the field $\mathbb{Q}(\mathrm{i})$) as follows:

$$\begin{cases} \text{Case 1:} & \kappa = \frac{1}{2}(B+C) + \mathrm{i}\frac{1}{2}(C-B), \\ \text{Case 2:} & \kappa = B + \mathrm{i}C, \\ \text{Case 3:} & \kappa = C + \mathrm{i}B. \end{cases} \tag{11}$$

It is easy to check using (7) and (10) that

$$\kappa \equiv 1\left(\mathrm{mod}(1+\mathrm{i})^3\right),$$

that is, κ is primary. From (3) and (11) we deduce

$$N(\kappa) = \kappa\bar{\kappa} = \begin{cases} \frac{1}{2}D, & \text{in case 1,} \\ D, & \text{in cases 2 and 3.} \end{cases} \tag{12}$$

As $N(\kappa)$ is squarefree and odd, and κ is primary, κ is the (possibly empty) product $\pi_1 \ldots \pi_k$ of primary Gaussian primes whose norms $p_1, \ldots, p_k$ are distinct rational primes $\equiv 1 \pmod 4$. Note that

$$N(\kappa) = p_1 \ldots p_k. \tag{13}$$

The empty product is understood to be 1. This occurs only when $D = 2$ in which case $B = C = 1$, $\kappa = 1$. The Gauss sum $G(\pi_j)$ $(j = 1, \ldots, k)$ is defined by

$$(14) \qquad G(\pi_j) = \sum_{x=1}^{p_j-1} \left[\frac{x}{\pi_j}\right]_4 e^{2\pi i x/p_j},$$

where $\left[\frac{x}{\pi_j}\right]_4$ is the fourth root of unity given by

$$\left[\frac{x}{\pi_j}\right]_4 \equiv x^{(p-1)/4} \pmod{\pi}_j.$$

We set

$$(15) \qquad G = G(\kappa) = \prod_{j=1}^{k} G(\pi_j),$$

it being understood that $G = 1$ when $k = 0 \Longleftrightarrow \kappa = 1 \Longleftrightarrow D = 2$. As each Gauss sum $G(\pi_j)$ $(j = 1, \ldots, k)$ has the following properties:

$$\begin{aligned}
&G(\pi_j)\overline{G(\pi_j)} = p_j, \quad [2, \text{Prop. } 8.2.2]\\
&\overline{G(\pi_j)} = (-1)^{(p_j-1)/4} G(\overline{\pi}_j), \quad [2, \text{p. } 92]\\
&G(\pi_j)^2 = -(-1)^{(p_j-1)/4}\sqrt{p_j}\,\pi_j, \quad [2, \text{Prop. } 9.10.1]\\
&G(\pi_j) \in \mathbb{Q}(e^{2\pi i/4}, e^{2\pi i/p_j}) = \mathbb{Q}(e^{2\pi i/4p_j}),
\end{aligned}$$

we see from (13) and (15) that

$$\begin{aligned}
&(16) \qquad G(\kappa)\overline{G(\kappa)} = N(\kappa),\\
&(17) \qquad \overline{G(\kappa)} = (-1)^{(N(\kappa)-1)/4} G(\overline{\kappa}),\\
&(18) \qquad G(\kappa)^2 = (-1)^{k+(N(\kappa)-1)/4} N(\kappa)^{1/2}\kappa,\\
&(19) \qquad G(\kappa) \in \mathbb{Q}\big(e^{2\pi i/4N(\kappa)}\big).
\end{aligned}$$

Our first lemma determines the effect of a certain automorphism or $G = G(\kappa)$ when $D \equiv 1 \pmod 4$, a result we shall use later.

Lemma 1. *If* $D \equiv 1 \pmod 4$ *and* $1 \neq \sigma \in \mathrm{Gal}\big(\mathbb{Q}(e^{2\pi i/4D})/\mathbb{Q}(e^{2\pi i/D})\big)$ *then*

$$\sigma(G) = (-1)^{(D-1)/4}\overline{G}.$$

Proof. The automorphisms σ_r of $\mathbb{Q}\big(e^{2\pi i/4D}\big)$ are given by

$$\sigma_r\big(e^{2\pi i/4D}\big) = e^{2r\pi i/4D}, \quad r = 1, \ldots, 4D, \quad GCD(r, 4D) = 1.$$

Those automorphisms σ_r fixing $\mathbb{Q}(e^{2\pi i/D})$ must satisfy

$$r \equiv 1 \pmod{D}, \quad 1 \leqslant r \leqslant 4D, \quad GCD(r, 4D) = 1,$$

so that $r = 1$ or $r = 2D + 1$. Thus the unique nontrivial automorphism of $\mathrm{Gal}\left(\mathbb{Q}(e^{2\pi i/4D})/\mathbb{Q}(e^{2\pi i/D})\right)$ is $\sigma = \sigma_{2D+1}$ given by $\sigma\left(e^{2\pi i/4D}\right) = -e^{2\pi i/4D}$. As $\sigma(i) = -i$ and $\sigma\left(e^{2\pi i/p_j}\right) = e^{2\pi i/p_j}$ $(j = 1, \ldots, k)$, we have

$$\begin{aligned}\sigma\big(G(\pi_j)\big) &= \sigma\left(\sum_{x=1}^{p_j-1}\left[\frac{x}{\pi_j}\right]_4 e^{2\pi i/p_j}\right) = \sum_{x=1}^{p_j-1}\overline{\left[\frac{x}{\pi_j}\right]}_4 e^{2\pi i/p_j} \\ &= \sum_{x=1}^{p_j-1}\left[\frac{x}{\overline{\pi}_j}\right]_4 e^{2\pi i/p_j} = G(\overline{\pi}_j) = (-1)^{(p_j-1)/4}\overline{G(\pi_j)},\end{aligned}$$

so that by (15), (12) and (13)

$$\sigma(G) = (-1)^{\sum_{j=1}^{k}(p_j-1)/4}\overline{G} = (-1)^{(D-1)/4}\overline{G}.$$

□

Our next lemma determines the roots of the minimal polynomial $X^4 - 2ADX^2 + A^2C^2D$ in terms of $G = G(\kappa)$.

Lemma 2. *The roots of the minimal polynomial $X^4 - 2ADX^2 + A^2CD$ of $\sqrt{A(D + B\sqrt{D})}$ are given as follows:*

$$\begin{cases} \textit{Case 1:} & \pm\sqrt{A}(\omega G + \overline{\omega}\overline{G}), \pm i\sqrt{A}(\omega G - \overline{\omega}\overline{G}), \\ \textit{Case 2:} & \pm\sqrt{A}(G + \overline{G})/\sqrt{2}, \pm i\sqrt{A}(G - \overline{G})/\sqrt{2}, \\ \textit{Case 3:} & \pm\frac{1}{2}\sqrt{A}\big((1+i)G + (1-i)\overline{G}\big), \pm\frac{1}{2}i\sqrt{A}\big((1-i)G + (1+i)\overline{G}\big), \end{cases}$$

where $\omega = e^{2\pi i/16}$.

Proof. We set

$$\varepsilon = (-1)^{k+(N(\kappa)-1)/4}.$$

From (18) we have

$$G^2 = \varepsilon N(\kappa)^{1/2}\kappa, \ \overline{G}^2 = \varepsilon N(\kappa)^{1/2}\overline{\kappa},$$

so that by (11), (12), (13) and (16)

$$G^2 + \overline{G}^2 = \begin{cases} \varepsilon D^{1/2}(B + C)/2^{1/2}, & \text{in case 1,} \\ 2\varepsilon D^{1/2}B, & \text{in case 2,} \\ 2\varepsilon D^{1/2}C, & \text{in case 3,} \end{cases}$$

$$G^2 - \overline{G}^2 = \begin{cases} i\varepsilon D^{1/2}(C - B)/2^{1/2}, & \text{in case 1,} \\ 2i\varepsilon D^{1/2}C, & \text{in case 2,} \\ 2i\varepsilon D^{1/2}B, & \text{in case 3,} \end{cases}$$

and

$$2G\overline{G} = \begin{cases} D, & \text{in case 1,} \\ 2D, & \text{in cases 2 and 3.} \end{cases}$$

Hence in case 1 we have

$$\begin{aligned}(\omega G + \overline{\omega}\overline{G})^2 &= \frac{(1+\mathrm{i})}{\sqrt{2}} G^2 + \frac{(1-\mathrm{i})}{\sqrt{2}} \overline{G}^2 + 2G\overline{G} \\ &= \varepsilon D^{1/2}(B+C)/2 + \varepsilon D^{1/2}(B-C)/2 + D \\ &= D + \varepsilon B\sqrt{D}\end{aligned}$$

and

$$\begin{aligned}\big(\mathrm{i}(\omega G - \overline{\omega}\overline{G})\big)^2 &= -\frac{(1+\mathrm{i})}{\sqrt{2}} G^2 - \frac{(1-\mathrm{i})}{\sqrt{2}} \overline{G}^2 + 2G\overline{G} \\ &= D - \varepsilon B\sqrt{D},\end{aligned}$$

so that

$$\begin{aligned}\big(\pm\sqrt{A}(\omega G + \overline{\omega}\overline{G})\big)^2 &= A(D + \varepsilon B\sqrt{D}), \\ \big(\pm\mathrm{i}\sqrt{A}(\omega G - \overline{\omega}\overline{G})\big)^2 &= A(D - \varepsilon B\sqrt{D}),\end{aligned}$$

as asserted. Cases 2 and 3 follow in a similar manner. □

We set

$$\text{(20)} \quad \begin{cases} \theta = \sqrt{A}(\omega G + \overline{\omega}\overline{G}), & \varphi = \mathrm{i}\sqrt{A}(\omega G - \overline{\omega}\overline{G}), \text{ in case 1,} \\ \theta = \sqrt{A}(G + \overline{G})/\sqrt{2}, & \varphi = \mathrm{i}\sqrt{A}(G - \overline{G})/\sqrt{2}, \text{ in case 2,} \\ \theta = \frac{1}{2}\sqrt{A}\big((1+\mathrm{i})G + (1-\mathrm{i})\overline{G}\big), & \varphi = \frac{1}{2}\sqrt{A}\big((1-\mathrm{i})G + (1+\mathrm{i})\overline{G}\big), \text{ in case 3,} \end{cases}$$

so that by Lemma 2

$$\text{(21)} \qquad K = \mathbb{Q}\Big(\sqrt{A(D + B\sqrt{D})}\Big) = \mathbb{Q}(\theta) = \mathbb{Q}(\varphi).$$

Lemma 3. (i)

$$\sqrt{A} \in \begin{cases} \mathbb{Q}\big(e^{2\pi\mathrm{i}/|A|}\big), & \text{if } A \equiv 1 \pmod 4, \\ \mathbb{Q}\big(e^{2\pi\mathrm{i}/4|A|}\big), & \text{if } A \equiv 3 \pmod 4. \end{cases}$$

(ii) *If* $D \equiv 1 \pmod 4$

$$\sqrt{(-1)^{(D-1)/4}A} \in \begin{cases} \mathbb{Q}\big(e^{2\pi\mathrm{i}/|A|}\big), & \text{in case 2 when } A + C \equiv 1 \pmod 4 \\ & \text{and in case 3(b),} \\ \mathbb{Q}\big(e^{2\pi\mathrm{i}/4|A|}\big), & \text{in case 2 when } A + C \equiv 3 \pmod 4 \\ & \text{and in case 3(a).} \end{cases}$$

Proof. The assertions of the Lemma are easily checked when $A = 1$ so we may assume $A \neq 1$. Set $k = \mathbb{Q}(\sqrt{A})$, so that k is a quadratic field, and let $f(k)$ denote the conductor of k. Now

$$f(k) = |\operatorname{disc}(k)|$$
$$= \begin{cases} A, & \text{if } A > 0, A \equiv 1 \pmod 4, \\ 4A, & \text{if } A > 0, A \equiv 3 \pmod 4, \\ -A, & \text{if } A < 0, A \equiv 1 \pmod 4, \\ -4A, & \text{if } A < 0, A \equiv 3 \pmod 4, \end{cases}$$
$$= \begin{cases} |A|, & \text{if } A \equiv 1 \pmod 4, \\ 4|A|, & \text{if } A \equiv 3 \pmod 4, \end{cases}$$

so that

$$\sqrt{A} \in k \subseteq \mathbb{Q}(e^{2\pi i/f(k)}) = \begin{cases} \mathbb{Q}(e^{2\pi i/|A|}), & \text{if } A \equiv 1 \pmod 4, \\ \mathbb{Q}(e^{2\pi i/4|A|}), & \text{if } A \equiv 3 \pmod 4. \end{cases}$$

This proves (i).

Suppose now $D \equiv 1 \pmod 4$. In case 2 we have

$$(-1)^{(D-1)/4} A \equiv \begin{cases} 1 \pmod 4, & \text{if } A + C \equiv 1 \pmod 4, \\ 3 \pmod 4, & \text{if } A + C \equiv 3 \pmod 4, \end{cases}$$

in case 3(a) $(-1)^{(D-1)/4} A \equiv 3 \pmod 4$, and in case 3(b) $(-1)^{(D-1)/4} A \equiv 1 \pmod 4$. Part (ii) now follows from (i). □

Lemma 4. *$f(K) \leqslant 2^l |A| D$, where l is defined in* (8).

Proof. We consider cases 1, 2 and 3 separately. Set $\omega = e^{2\pi i/16}$.

Case 1. Clearly $\omega \in \mathbb{Q}(e^{2\pi i/16})$ and, by (12) and (19), we have $G \in \mathbb{Q}(e^{2\pi i/2D})$, so that $\omega G \in \mathbb{Q}(e^{2\pi i/8D})$. Similarly $\overline{\omega G} \in \mathbb{Q}(e^{2\pi i/8D})$ so that $\omega G + \overline{\omega G} \in \mathbb{Q}(e^{2\pi i/8D})$. By Lemma 3(i) $\sqrt{A} \in \mathbb{Q}(e^{2\pi i/4|A|})$ so that $\theta = \sqrt{A}(\omega G + \overline{\omega G}) \in \mathbb{Q}(e^{2\pi i/8|A|D})$, that is by (21), $K \subseteq \mathbb{Q}(e^{2\pi i/8|A|D})$, and so $f(K) \leqslant 8|A|D = 2^l |A| D$, as $l = 3$ in case 1.

Case 2. By (12) and (19) we have $G \in \mathbb{Q}(e^{2\pi i/4D})$, $\overline{G} \in \mathbb{Q}(e^{2\pi i/4D})$, so that $G + \overline{G} \in \mathbb{Q}(e^{2\pi i/4D})$. By Lemma 3(i) $\sqrt{A} \in \mathbb{Q}(e^{2\pi i/4|A|})$, and clearly $\sqrt{2} \in \mathbb{Q}(e^{2\pi i/8})$, so that $\theta = \sqrt{A}(G + \overline{G})/\sqrt{2} \in \mathbb{Q}(e^{2\pi i/8|A|D})$, that is by (21), $K \subseteq \mathbb{Q}(e^{2\pi i/8|A|D})$, and so $f(K) \leqslant 8|A|D = 2^l |A| D$, as $l = 3$ in case 2.

Case 3. By (12) and (19) we have $G \in \mathbb{Q}(e^{2\pi i/4D})$, $\overline{G} \in \mathbb{Q}(e^{2\pi i/4D})$. Clearly $i \in \mathbb{Q}(e^{2\pi i/4D})$ so that $\frac{(1+i)G+(1-i)\overline{G}}{i^{(D-1)/4}} \in \mathbb{Q}(e^{2\pi i/4D})$. Then, by Lemma 1, we have

$$\sigma\Big(\frac{(1+i)G+(1-i)\overline{G}}{i^{(D-1)/4}}\Big) = \frac{(1-i)(-1)^{(D-1)/4}\overline{G}+(1+i)(-1)^{(D-1)/4}G}{(-i)^{(D-1)/4}} = \frac{(1+i)G+(1-i)\overline{G}}{i^{(D-1)/4}},$$

so that

$$(22) \qquad \frac{(1+i)G+(1-i)\overline{G}}{i^{(D-1)/4}} \in \mathbb{Q}(e^{2\pi i/D}).$$

By Lemma 3(ii) we have

$$(23) \qquad \pm i^{(D-1)/4}\sqrt{A} = \sqrt{(-1)^{(D-1)/4}A} \in \begin{cases} \mathbb{Q}\big(e^{2\pi i/|A|}\big), & \text{in case 3(b)}, \\ \mathbb{Q}\big(e^{2\pi i/4|A|}\big), & \text{in case 3(a)}. \end{cases}$$

Then, from (22) and (23), we deduce

$$\theta = \sqrt{A}\Big(\frac{(1+i)G+(1-i)\overline{G}}{2}\Big) \in \begin{cases} \mathbb{Q}\big(e^{2\pi i/|A|D}\big), & \text{in case 3(b)}, \\ \mathbb{Q}\big(e^{2\pi i/4|A|D}\big), & \text{in case 3(a)}, \end{cases}$$

so that, by (8) and (21), $K \subseteq \mathbb{Q}\big(e^{2\pi i/2^l|A|D}\big)$ and so $f(K) \leqslant 2^l|A|D$. □

Lemma 5.

$$\begin{cases} \frac{D}{2} \mid f(K), & \textit{in case } 1, \\ D \mid f(K), & \textit{in cases } 2 \textit{ and } 3. \end{cases}$$

Proof. Let p be an odd prime divisor of D. As D is squarefree, we have

$$\langle p\rangle = \langle p, \sqrt{D}\rangle^2$$

in $\mathbb{Q}(\sqrt{D})$. Thus p ramifies in $\mathbb{Q}(\sqrt{D})$ and, as $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}\Big(\sqrt{A(D+B\sqrt{D})}\Big) \subseteq \mathbb{Q}(e^{2\pi i/f(K)})$, p ramifies in $\mathbb{Q}(e^{2\pi i/f(K)})$. Hence $p \mid f(K)$ for every odd prime divisor of D. This proves the assertion of the lemma. □

Lemma 6. $|A| \mid f(K)$.

Proof. Let p be prime divisor of $|A|$. As A is odd, $p \neq 2$. In K we have

$$\langle p\rangle = \begin{cases} \Big\langle p, \sqrt{A(D+B\sqrt{D})}\Big\rangle^2, & \text{if } p \nmid C, \\ \Big\langle p, \sqrt{A(D+B\sqrt{D})} + \sqrt{A(D-B\sqrt{D})}\Big\rangle^2, & \text{if } p \nmid B. \end{cases}$$

Thus p ramifies in K and so in $\mathbb{Q}\big(e^{2\pi i/f(k)}\big)$. Hence $p \mid f(K)$ and so $|A| \mid f(K)$. □

Lemma 7. $4 \mid f(K)$ *in cases* 1, 2 *and* 3(a).

Proof. We have

$$\langle 2\rangle = \begin{cases} \left\langle 2, \sqrt{D}\right\rangle^2 & \text{in } \mathbb{Q}(\sqrt{D}) \text{ in case 1,} \\ \left\langle 2, \sqrt{A(D+B\sqrt{D})} + \sqrt{A(D-B\sqrt{D})}\right\rangle^2 & \text{in } K \text{ in case 2,} \\ \left\langle 2, 1+\sqrt{A(D+B\sqrt{D})}\right\rangle^2 & \text{in } K \text{ in case 3(a),} \end{cases}$$

so that 2 ramifies in $\mathbb{Q}(e^{2\pi i/f(K)})$, and thus $4 \mid f(K)$. □

Lemma 8.

$$16 \mid f(K), \quad \textit{in case } 1,$$
$$8 \mid f(K), \quad \textit{in case } 2.$$

Proof. From (21) we have

$$\theta, \varphi \in K \subseteq \mathbb{Q}(e^{2\pi i/f(K)}),$$

and by Lemma 7 for cases 1 and 2 we have

$$i \in \mathbb{Q}(e^{2\pi i/f(K)}).$$

Case 1. By Lemmas 3(i), 6 and 7 we have

$$\sqrt{A} \in \mathbb{Q}(e^{2\pi i/4|A|}) \subseteq \mathbb{Q}(e^{2\pi i/f(K)}).$$

By (12), (19), Lemma 5 and Lemma 7, we have

$$G \in \mathbb{Q}(e^{2\pi i/2D}) \subseteq \mathbb{Q}(e^{2\pi i/f(K)}).$$

Hence, appealing to (20), we see that

$$e^{2\pi i/16} = \omega = \frac{\theta - i\varphi}{2G\sqrt{A}} \in \mathbb{Q}(e^{2\pi i/f(K)}),$$

and so $16 \mid f(K)$.

Case 2. By (12) and (19) we have $G \in \mathbb{Q}(e^{2\pi i/4D})$, $\overline{G} \in \mathbb{Q}(e^{2\pi i/4D})$, so that $G+\overline{G} \in \mathbb{Q}(e^{2\pi i/4D})$. By Lemmas 5 and 7, we have $4D \mid f(K)$, so that

$$G+\overline{G} \in \mathbb{Q}(e^{2\pi i/f(K)}).$$

By Lemma 3(i) we have

$$\sqrt{A} \in \mathbb{Q}(e^{2\pi i/4|A|}),$$

and, by Lemmas 6 and 7, $4|A| \mid f(K)$ so that

$$\sqrt{A} \in \mathbb{Q}(e^{2\pi i/f(K)}).$$

Hence we have shown that

$$\sqrt{A}(G+\overline{G}) \in \mathbb{Q}(e^{2\pi i/f(K)}).$$

But, by (20) and (21), $\theta = \sqrt{A}(G+\overline{G})/\sqrt{2} \in K \subseteq \mathbb{Q}(e^{2\pi i/f(K)})$ so $\sqrt{2} \in \mathbb{Q}(e^{2\pi i/f(K)})$ and thus $8 \mid f(K)$. $\square$

Proof of Theorem. From (8) and Lemmas 5, 6, 7 and 8, we see that $2^l|A|D$ divides $f(K)$. Hence by Lemma 4 we have $f(K) = 2^l|A|D$. $\square$

References

[1] *K. Hardy, R.H. Hudson, D. Richman, K.S. Williams and N.M. Holtz*: Calculation of the class numbers of imaginary cyclic quartic fields. Carleton-Ottawa Mathematical Lecture Note Series (Carleton University, Ottawa, Ontario, Canada), Number 7, July 1986, pp. 201.

[2] *K. Ireland and M. Rosen*: A Classical Introduction to Modern Number Theory. Springer-Verlag, New York, Second Edition (1990).

Authors' addresses: B.K. Spearman, Department of Mathematics and Statistics, Okanagan University College, Kelowna, B.C., Canada, V1V 1V7; K.S. Williams, Department of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada, K1S 5B6.