

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>

Terms of use:

© Institute of Mathematics AS CR, 1997

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://dml.cz>

THE CONDUCTOR OF A CYCLIC QUARTIC
FIELD USING GAUSS SUMS

BLAIR K. SPEARMAN, Kelowna and KENNETH S. WILLIAMS¹, Ottawa

(Received December 12, 1994)

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

$$K = \mathbb{Q}\left(\sqrt{A(D + B\sqrt{D})}\right),$$

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

$$(1) \quad K = \mathbb{Q}\left(\sqrt{A(D + B\sqrt{D})}\right),$$

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

where

- (2) A is squarefree and odd,
- (3) $D = B^2 + C^2$ is squarefree, $B > 0$, $C > 0$,
- (4) $GCD(A, D) = 1$.

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:

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

We also divide case 3 into two subcases according as

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

We note that

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

and

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

We set

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

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

$$(9) \quad f(K) = 2^l |A|D,$$

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:

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

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 $\mathbb{Q}(i)$) as follows:

$$(11) \quad \left\{ \begin{array}{l} \text{Case 1: } \kappa = \frac{1}{2}(B + C) + i\frac{1}{2}(C - B), \\ \text{Case 2: } \kappa = B + iC, \\ \text{Case 3: } \kappa = C + iB. \end{array} \right.$$

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

$$\kappa \equiv 1 \pmod{(1+i)^3},$$

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

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

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

$$(13) \quad N(\kappa) = p_1 \dots p_k.$$

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 $G(\pi_j)$ ($j = 1, \dots, k$) is defined by

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

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

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

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

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

we see from (13) and (15) that

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

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 $1 \neq \sigma \in \text{Gal}(\mathbb{Q}(e^{2\pi i/4D})/\mathbb{Q}(e^{2\pi i/D}))$ then*

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

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

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

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

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

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

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

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:*

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

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

Proof. We set

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

From (18) we have

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

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

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

and

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

Hence in case 1 we have

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

and

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

so that

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

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

We set

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

so that by Lemma 2

$$(21) \quad K = \mathbb{Q}\left(\sqrt{A(D + B\sqrt{D})}\right) = \mathbb{Q}(\theta) = \mathbb{Q}(\varphi).$$

Lemma 3. (i)

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

(ii) If $D \equiv 1 \pmod{4}$

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

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

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

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). \square

Lemma 4. $f(K) \leq 2^l |A|D$, 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 $f(K) \leq 8|A|D = 2^l |A|D$, 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 $f(K) \leq 8|A|D = 2^l |A|D$, 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

$$\begin{aligned} \sigma\left(\frac{(1+i)G+(1-i)\overline{G}}{i^{(D-1)/4}}\right) &= \frac{(1-i)(-1)^{(D-1)/4}\overline{G}+(1+i)(-1)^{(D-1)/4}G}{(-i)^{(D-1)/4}} \\ &= \frac{(1+i)G+(1-i)\overline{G}}{i^{(D-1)/4}}, \end{aligned}$$

so that

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

By Lemma 3(ii) we have

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

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

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

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

Lemma 5.

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

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 $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}\left(\sqrt{A(D+B\sqrt{D})}\right) \subseteq \mathbb{Q}(e^{2\pi i/f(K)})$, 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

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

Thus p ramifies in K and so in $\mathbb{Q}(e^{2\pi i/f(K)})$. 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

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

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

Lemma 8.

$$16 \mid f(K), \text{ in case 1,}$$

$$8 \mid f(K), \text{ in case 2.}$$

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.