Indian J. pure appl. Math., **38**(4): 231-240, August 2007

THE CONDUCTOR OF LECACHEUX'S PARAMETRIC FAMILY OF CYCLIC QUINTIC FIELDS

ALAN K. SILVESTER*[1], BLAIR K. SPEARMAN**[2] AND KENNETH S. WILLIAMS***[3]

**Department of Mathematics and Statistics,*
Okanagan University of British Columbia, Kelowna, B.C. Canada V1V 1V7
e-mail: mascdman@canada.com
***Department of Mathematics and Statistics,*
Okanagan University of British Columbia, Kelowna, B.C. Canada V1V 1V7
e-mail: blair.spearman@ubc.ca
****School of Mathematics and Statistics,*
Carleton University, Ottawa, Ontario, Canada K1S 5B6
e-mail: williams@math.carleton.ca

(*Received* 25 *January* 2006; *after final revision* 9 *October* 2006; *accepted* 12 *October* 2006)

A formula for the conductor of Lecacheux's parametric family of cylic quintic fields is given.

Key Words: Cyclic Quintic Fields; Conductor

1. INTRODUCTION

Spearman and Williams [7] have given a theorem which enables one to determine the discriminant of a cyclic field of odd prime degree directly from the coefficients of a defining polynomial. They applied their theorem to a family of cyclic quintic polynomials due to Lehmer [5]. In this paper we apply the theorem of Spearman and Williams to a family of cyclic quintic polynomials due to Lecacheux [3], [4].

[1]The first author was supported at The University of British Columbia Okanagan by an undergraduate student research award from the Natural Sciences and Engineering Research Council of Canada.

[2]The second author was supported by a research grant from the Natural Sciences and Engineering Research Council of Canada.

[3]The third author was supported by Natural Sciences and Engineering Research Council of Canada grant A-7233.

2. Spearman and Williams' Theorem

In this section we state the theorem of Spearman and Williams [7].

Theorem 1 — *Let p be an odd prime. Let $f(X) = X^p + a_{p-2}X^{p-2} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ be such that $Gal(f) \simeq \mathbb{Z}/p\mathbb{Z}$ and such that there does not exist a prime q with $q^{p-i} \mid a_i (i = 0, 1, \dots, p-2)$. Let $\theta \in \mathbb{C}$ be a root of $f(X)$ and set $K = \mathbb{Q}(\theta)$ so that K is a cyclic extension of $\mathbb{Q}$ with $[K : \mathbb{Q}] = p$. Then*

$$d(K) = f(K)^{p-1},$$

where the conductor $f(K)$ is given by

$$f(K) = p^\alpha \prod_{\substack{q \equiv 1 \pmod{p} \\ q \mid a_i \ (i=0,1,\dots,p-2)}} q,$$

where q runs through primes and

$$\alpha = \begin{cases} 0, & \text{if } p^{p(p-1)} \nmid \operatorname{disc}(f) \text{ and } p \mid a_i \ (i = 1, \dots, p-2) \text{ does not hold} \\ & \qquad \text{or} \\ & p^{p(p-1)} \mid \operatorname{disc}(f) \text{ and } p^{p-1} \parallel a_0,\ p^{p-1} \mid a_1,\ p^{p+1-i} \mid a_i \\ & (i = 2, \dots, p-2) \text{ does not hold} \\ 2, & \text{if } p^{p(p-1)} \nmid \operatorname{disc}(f) \text{ and } p \mid a_i \ (i = 1, \dots, p-2) \text{ holds} \\ & \qquad \text{or} \\ & p^{p(p-1)} \mid \operatorname{disc}(f) \text{ and } p^{p-1} \parallel a_0,\ p^{p-1} \mid a_1,\ p^{p+1-i} \mid a_i \\ & (i = 2, \dots, p-2) \text{ holds.} \end{cases}$$

3. Odile Lecacheux's Quintics

Let $t \in \mathbb{Q}$ and set

$$f_t(X) = X^5 + a_4(t)X^4 + a_3(t)X^3 + a_2(t)X^2 + a_1(t)X + a_0(t),$$

where

$$\begin{aligned} a_4(t) &= t^5 - 3, \\ a_3(t) &= -t^9 - 2t^8 - 3t^7 - 5t^6 - 6t^5 - 2t^4 + t^3 - t^2 + 3, \\ a_2(t) &= t^{10} + 2t^9 + 4t^8 + 6t^7 + 10t^6 + 9t^5 + 4t^4 - 2t^3 + 2t^2 - 1, \\ a_1(t) &= -t^2(t^7 + 2t^6 + 3t^5 + 5t^4 + 5t^3 + 2t^2 - t + 1), \\ a_0(t) &= t^5. \end{aligned}$$

These polynomials were introduced by Odile Lecacheux [3] in 1990. We set

$$t = u/v,\ \ u \in \mathbb{Z},\ \ v \in \mathbb{Z},\ \ (u, v) = 1,\ \ v > 0,$$

and define

$$
\begin{aligned}
E_1 &= E_1(u,v) = u^4 - 2u^3v + 4u^2v^2 - 3uv^3 + v^4,\\
E_2 &= E_2(u,v) = u^4 + 3u^3v + 4u^2v^2 + 2uv^3 + v^4,\\
F &= F(u,v) = 2u^2 + 3uv + 3v^2,\\
G &= G(u,v) = 4u^3 - u^2v - 2uv^2 + 2v^3,\\
H &= H(u,v) = u^3 + u^2v - 3uv^2 + 3v^3,\\
J &= J(u,v) = -3u^5 + 4v^5,\\
L &= L(u,v) = 4u^{13} + 9u^{12}v - 22u^{11}v^2 + 22u^{10}v^3 + 6u^8v^5 - 74u^7v^6\\
&\qquad +142u^6v^7 - 142u^5v^8 + 96u^3v^{10} - 84u^2v^{11} + 72uv^{12} - 72v^{13},\\
M &= M(u,v) = 7u^3 + 22u^2v + 29uv^2 + 11v^3,\\
N &= N(u,v) = 7u^3 - 13u^2v + 24uv^2 - 14v^3,\\
P &= P(u,v) = 20u^{12} + 77u^{11}v - 14u^{10}v^2 + 75u^8v^4 + 105u^7v^5 - 282u^6v^6\\
&\qquad +159u^5v^7 - 475u^3v^9 + 5u^2v^{10} + 3uv^{11} + 49v^{12},\\
Q &= Q(u,v) = 5u^3 - 2u^2v + 10uv^2 + 8v^3,\\
R &= R(u,v) = 12u^{12} + 47u^{11}v - 33u^{10}v^2 - 75u^9v^3 + 175u^8v^4 - 12u^7v^5\\
&\qquad -267u^6v^6 + 108u^5v^7 + 475u^4v^8 - 1075u^3v^9 + 528u^2v^{10}\\
&\qquad +478uv^{11} - 527v^{12},\\
S &= S(u,v) = 3u^3 + 14u^2v + 24uv^2 + 16v^3.
\end{aligned}
$$

Let θ be a root of $f_t(X)$ and set $K = \mathbb{Q}(\theta)$. We prove

Theorem 2 — *Let t be a rational number such that $f_t(X)$ is irreducible in $\mathbb{Q}[X]$. Then K is a cyclic quintic field.*

PROOF: As $f_t(X)$ is assumed to be irreducible in $\mathbb{Q}[X]$, we have

$$[K:\mathbb{Q}] = \deg(f_t(X)) = 5$$

so that K is a quintic field. We next determine the Galois group of K over $\mathbb{Q}$. We set

$$g_t(X) = 5^5 f_t\left(\frac{X - (t^5 - 3)}{5}\right)$$

so that

$$g_t(X) = X^5 + g_3X^3 + g_2X^2 + g_1X + g_0,$$

where

$$
\begin{aligned}
g_3 &= -5(2t^2 + 3t + 3)(t^4 + 3t^3 + 4t^2 + 2t + 1)(t^4 - 2t^3 + 4t^2 - 3t + 1),\\
g_2 &= 5\left(4t^3 - t^2 - 2t + 2\right)\left(t^4 - 2t^3 + 4t^2 - 3t + 1\right)(t^4 + 3t^3 + 4t^2 + 2t + 1)^2,
\end{aligned}
$$

$$\begin{aligned} g_1 &= -5(t^3+t^2-3t+3)(t^4-2t^3+4t^2-3t+1)(3t^5-4) \\ &\quad \times(t^4+3t^3+4t^2+2t+1)^2, \\ g_0 &= (4t^{13}+9t^{12}-22t^{11}+22t^{10}+6t^8-74t^7+142t^6-142t^5+96t^3-84t^2 \\ &\quad +72t-72)(t^4-2t^3+4t^2-3t+1)(t^4+3t^3+4t^2+2t+1)^2. \end{aligned}$$

Using MAPLE we find that

$$\operatorname{disc}(g_t(X)) = 5^{20}t^{18}(t^4-2t^3+4t^2-3t+1)^4(t^4+3t^3+4t^2+2t+1)^8.$$

As $f_0(X)$ is reducible we have $t \neq 0$ so that the discriminant of $g_t(X)$ is a nonzero perfect square. Thus Gal(K) is a subgroup of the alternating group A_5, and so Gal$(K) \simeq \mathbb{Z}_5$, D_5 or A_5. Using the expression for the resolvent sextic of a quintic polynomial given by Dummit [2], we find using MAPLE that the resolvent sextic of $g_t(X)$ has the rational root

$$\begin{aligned} &5\left(t^4-2t^3+4t^2-3t+1\right)\left(4t^8+4t^7-12t^6+12t^5+78t^3-47t^2+16t-16\right) \\ &\times\left(t^4+3t^3+4t^2+2t+1\right)^2. \end{aligned}$$

Thus Gal(K) is a solvable group and so Gal$(K) \simeq \mathbb{Z}_5$ or D_5. Suppose that Gal$(K) \simeq D_5$. Let $\theta_1, \ldots, \theta_5 \in \mathbb{C}$ be the roots of $g_t(X)$. Set

$$g(X) = \prod_{\substack{i,j=1 \\ i\neq j}}^{5} (x - (\theta_i - \theta_j)) \in \mathbb{Q}[X].$$

Soicher [6] (see also [1]) has shown that $g(X)$ can be determined by using resultants as

$$g(X) = \frac{\text{resultant } (g_t(x+X), g_t(x))}{X^5}.$$

MAPLE gives

$$g(X) = q_1(X)q_2(X)q_3(X)q_4(X),$$

where each $q_i(X)$ is a quintic polynomial in $\mathbb{Q}[X]$. Using MAPLE we find that

$$\text{resultant}(q_i(X), q_j(X)) \neq 0 \text{ for } t \neq 0, \quad 1 \leq i < j \leq 4,$$

and

$$\text{resultant } (q_i(X), q_i'(X)) \neq 0 \text{ for } t \neq 0, \quad i = 1, 2, 3, 4,$$

so that $g(X)$ is a squarefree polynomial in $\mathbb{Q}[X]$. Then, by [1, Theorem 3.1(i)], $g(X)$ factors as a product of two irreducible polynomials of degree 10 in $\mathbb{Q}[X]$. Thus Gal$(K) \not\simeq D_5$. Therefore Gal$(K) \simeq \mathbb{Z}_5$. □

4. THE CONDUCTOR OF K.

We apply Spearman and Williams' theorem to prove the following result.

***Theorem* 3** — *Let t be a rational number such that $f_t(X)$ is irreducible in $\mathbb{Q}[X]$. Let θ be a root of $f_t(X)$. Set $K = \mathbb{Q}(\theta)$ so, by Theorem 2, K is a cyclic quintic field. Then the conductor $f(K)$ is given by*

$$f(K) = 5^{\alpha} \prod_{\substack{q \equiv 1 \pmod 5 \\ q \mid E_1 E_2 \\ v_q(E_1 E_2) \not\equiv 0 \pmod 5}} q,$$

where q runs through primes,

$$\alpha = \begin{cases} 0, \text{if } 2u - v \not\equiv 0 (\bmod 5), \\ 2, \text{if } 2u - v \equiv 0 (\bmod 5), \end{cases}$$

and

$$q^{v_q(E_1 E_2)} \parallel E_1 E_2.$$

PROOF : As in the proof of Theorem 2, we set

$$g_t(X) = 5^5 f_t\left(\frac{X - (t^5 - 3)}{5}\right) = X^5 + g_3 X^3 + g_2 X^2 + g_1 X + g_0,$$

where g_3, g_2, g_1, g_0 are given in the proof of Theorem 2. Next we set

$$h_{u,v}(X) = v^{25} g_{u/v}(X/v^5) = X^5 + h_3 X^3 + h_2 X^2 + h_1 X + h_0,$$

where

$$\begin{aligned} h_3 &= -5(u^4 - 2u^3v + 4u^2v^2 - 3uv^3 + v^4) \\ &\quad \times (u^4 + 3u^3v + 4u^2v^2 + 2uv^3 + v^4)(2u^2 + 3uv + 3v^2), \\ h_2 &= 5(u^4 - 2u^3v + 4u^2v^2 - 3uv^3 + v^4)(u^4 + 3u^3v + 4u^2v^2 + 2uv^3 + v^4)^2 \\ &\quad \times (4u^3 - u^2v - 2uv^2 + 2v^3), \\ h_1 &= 5(u^4 - 2u^3v + 4u^2v^2 - 3uv^3 + v^4)(u^4 + 3u^3v + 4u^2v^2 + 2uv^3 + v^4)^2 \\ &\quad \times (u^3 + u^2v - 3uv^2 + 3v^3)(-3u^5 + 4v^5), \\ h_0 &= (u^4 - 2u^3v + 4u^2v^2 - 3uv^3 + v^4)(u^4 + 3u^3v + 4u^2v^2 + 2uv^3 + v^4)^2 \\ &\quad \times (4u^{13} + 9u^{12}v - 22u^{11}v^2 + 22u^{10}v^3 + 6u^8v^5 - 74u^7v^6 + 142u^6v^7 \\ &\quad -142u^5v^8 + 96u^3v^{10} - 84u^2v^{11} + 72uv^{12} - 72v^{13}), \end{aligned}$$

so that, from the definitions given in Section 3, we have

$$h_3 = -5E_1E_2F, \quad h_2 = 5E_1E_2^2G, \quad h_1 = 5E_1E_2^2HJ, \quad h_0 = E_1E_2^2L. \tag{4.1}$$

Let m denote the largest positive integer such that

$$m^2 \mid h_3,\ \ m^3 \mid h_2,\ \ m^4 \mid h_1,\ \ m^5 \mid h_0, \tag{4.2}$$

and set

$$k_{u,v}(X) = h_{u,v}(mX)/m^5 = X^5 + k_3X^3 + k_2X^2 + k_1X + k_0, \tag{4.3}$$

where

$$k_3 = h_3/m^2,\ \ k_2 = h_2/m^3,\ \ k_1 = h_1/m^4,\ \ k_0 = h_0/m^5. \tag{4.4}$$

Appealing to MAPLE, we find

$$\begin{aligned} \operatorname{disc}(k_{u,v}(X)) &= \frac{5^{20}E_1^4E_2^8u^{18}v^{34}}{m^{20}}, && (4.5)\\ E_1M - E_2N &= 5^2v^7, && (4.6)\\ E_1P - LQ &= 5^4v^{16}, && (4.7) \end{aligned}$$

and

$$E_2R - LS = 5^4v^{16}. \tag{4.8}$$

Clearly $k_{u,v}(X)$ is a defining polynomial for the cyclic quintic field K. Hence, by Theorem 1, we have

$$f(K) = 5^\alpha \prod_{\substack{q\equiv 1 \pmod 5\\ q\mid k_0,\ q\mid k_1,\ q\mid k_2,\ q\mid k_3}} q, \tag{4.9}$$

where q runs through primes and

$$\alpha = \begin{cases} 0, & \text{if } 5^{20} \nmid \operatorname{disc}(k_{u,v}) \text{ and } 5 \mid k_1,\ 5 \mid k_2,\ 5 \mid k_3 \text{ does not hold}\\ & \text{or}\\ & 5^{20} \mid \operatorname{disc}(k_{u,v}) \text{ and } 5^4 \parallel k_0,\ 5^4 \mid k_1,\ 5^4 \mid k_2,\ 5^3 \mid k_3\\ & \text{does not hold}\\ 2, & \text{if } 5^{20} \nmid \operatorname{disc}(k_{u,v}) \text{ and } 5 \mid k_1,\ 5 \mid k_2,\ 5 \mid k_3\\ & \text{or}\\ & 5^{20} \mid \operatorname{disc}(k_{u,v}) \text{ and } 5^4 \parallel k_0,\ 5^4 \mid k_1,\ 5^4 \mid k_2,\ 5^3 \mid k_3. \end{cases} \tag{4.10}$$

Let q be a prime with

$$q \equiv 1 (\bmod 5),\ \ q \mid k_3,\ \ q \mid k_2,\ \ q \mid k_1,\ \ q \mid k_0.$$

We show that

$$q \mid E_1E_2,\ \ v_q(E_1E_2) \not\equiv 0 (\bmod 5).$$

As $q \equiv 1 (\bmod 5)$ we have $q \neq 2, 3, 5$. Suppose $q \mid u$. As $q \mid h_0$, we see by (4.1) that $q \mid E_1$ or $q \mid E_2$ or $q \mid L$. If $q \mid E_1$ or $q \mid E_2$ then from the definitions of E_1 and E_2 we see that $q \mid v$, contradicting $(u, v) = 1$. If $q \mid L$ then as $q \neq 2, 3$ we see from the definition of L that $q \mid v$, contradicting $(u, v) = 1$. Hence $q \nmid u$. Suppose $q \mid v$. As $q \mid h_0$, we see by (4.1) that $q \mid E_1$

or $q \mid E_2$ or $q \mid L$. If $q \mid E_1$ or $q \mid E_2$ then from the definitions of E_1 and E_2 we have $q \mid u$, contradicting $(u,v) = 1$. If $q \mid L$ then as $q \neq 2$ we have from the definition of L that $q \mid u$, contradicting $(u,v) = 1$. Thus $q \nmid uv$. As $q \mid f(K)$ we have $q \mid \text{disc}\,(k_{u,v})$. It follows by (4.5) that $q \mid E_1$ or $q \mid E_2$ as $q \nmid u, v, 5$. By (4.6) we see that $q \mid E_1$ or $q \mid E_2$ but not both. Assume that $q \mid E_1$. If $v_q(E_1E_2) \equiv 0 \pmod 5$ then $v_q(E_1) = 5w$ for some $w \in \mathbb{N}$. By (4.7) we have $q \nmid L$. Thus by (4.1) we have

$$q^{5w} \mid h_3, \quad q^{5w} \mid h_2, \quad q^{5w} \mid h_1, \quad q^{5w} \parallel h_0,$$

and by (4.2) we deduce that

$$q^w \parallel m.$$

Thus

$$q \nmid \frac{h_0}{m^5} = k_0,$$

contradicting $q \mid k_0$. Hence $v_q(E_1) \not\equiv 0 \pmod 5$. Now assume $q \mid E_2$. If $v_q(E_2) \equiv 0 \pmod 5$ then $v_q(E_2) = 5w$ for some $w \in \mathbb{N}$. By (4.8) we see that $q \nmid L$. As $q^{5w} \parallel E_2$ we have $q^{10w} \parallel E_2^2$. Thus by (4.1) we see that

$$q^{5w} \mid h_3, \quad q^{10w} \mid h_2, \quad q^{10w} \mid h_1, \quad q^{10w} \parallel h_0,$$

and by (4.2) we have

$$q^{2w} \parallel m.$$

Thus

$$q \nmid \frac{h_0}{m^5} = k_0,$$

contradicting $q \mid k_0$. Hence $v_q(E_2) \not\equiv 0 \pmod 5$. Thus $v_q(E_1E_2) \not\equiv 0 \pmod 5$.

Now conversely let q be a prime with

$$q \equiv 1 (\text{mod } 5), \quad q \mid E_1E_2, \quad v_q(E_1E_2) \not\equiv 0 (\text{mod } 5)$$

We show that

$$q \equiv 1 (\text{mod } 5), \quad q \mid k_3, \quad q \mid k_2, \quad q \mid k_1, \quad q \mid k_0.$$

By (4.6) we see that either $q \mid E_1$ or $q \mid E_2$ but not both. As $v_q(E_1E_2) \not\equiv 0 \pmod 5$ we have $q^{5z+r} \parallel E_1E_2$ for some nonnegative integer z and $r \in \{1,2,3,4\}$. Assume $q \mid E_1$. Then by (4.7) we see that $q \nmid L$. We have by (4.1)

$$q^{5z+r} \mid h_3, \quad q^{5z+r} \mid h_2, \quad q^{5z+r} \mid h_1, \quad q^{5z+r} \parallel h_0,$$

and by (4.2) we have

$$q^z \parallel m$$

so

$$q^{3z+r} \mid k_3, \quad q^{2z+r} \mid k_2, \quad q^{z+r} \mid k_1, \quad q^r \mid k_0.$$

Thus

$$q \mid k_3, \quad q \mid k_2, \quad q \mid k_1, \quad q \mid k_0.$$

Now assume $q \mid E_2$. Then by (4.8) we have $q \nmid L$. As $v_q(E_2) = 5z+r$ we see that $q^{10z+2r} \parallel E_2^2$. Thus by (4.1) we have

$$q^{5z+r} \mid h_3, \quad q^{10z+2r} \mid h_2, \quad q^{10z+2r} \mid h_1, \quad q^{10z+2r} \parallel h_0.$$

From the definition of m it follows that $q^{2z} \parallel m$ if $r = 1, 2$ and $q^{2z+1} \parallel m$ if $r = 3, 4$. In the second case we note that $(5z + r) - (4z + 2) = z + (r - 2) > 0$ so $q \mid k_3$. Thus

$$q \mid k_3, \quad q \mid k_2, \quad q \mid k_1, \quad q \mid k_0.$$

We have proved

$$\prod_{\substack{q \equiv 1 \pmod 5 \\ q \mid k_0,\, q \mid k_1,\, q \mid k_2,\, q \mid k_3}} q = \prod_{\substack{q \equiv 1 \pmod 5 \\ q \mid E_1 E_2 \\ v_q(E_1 E_2) \not\equiv 0 \pmod 5}} q. \tag{4.11}$$

It remains to show that

$$\alpha = \begin{cases} 0, \text{if } 2u - v \not\equiv 0 \pmod 5, \\ 2, \text{if } 2u - v \equiv 0 \pmod 5. \end{cases}$$

The following simple divisibilty result will be useful.

Lemma —

(a) $5 \nmid E_1, E_2, F, G, H, J, L$, if $2u - v \not\equiv 0 \pmod 5$.

(b) $5 \parallel E_1, E_2, F, G, H$ and $5^2 \mid J, L$, if $2u - v \equiv 0 \pmod 5$.

PROOF : (a) Suppose $2u - v \not\equiv 0 \pmod 5$. Then $u + 2v \not\equiv 0 \pmod 5$ and

$$\begin{aligned} E_1 &\equiv (u + 2v)^4 \not\equiv 0 \pmod 5, \\ E_2 &\equiv (u + 2v)^4 \not\equiv 0 \pmod 5, \\ F &\equiv 2(u + 2v)^2 \not\equiv 0 \pmod 5, \\ G &\equiv 4(u + 2v)^3 \not\equiv 0 \pmod 5, \\ H &\equiv (u + 2v)^3 \not\equiv 0 \pmod 5, \\ J &\equiv 2(u + 2v)^5 \not\equiv 0 \pmod 5, \\ L &\equiv 4(u + 2v)^{13} \not\equiv 0 \pmod 5. \end{aligned}$$

(b) Suppose $2u - v \equiv 0 \pmod 5$. Then $v = 2u + 5w$ for some $w \in \mathbb{Z}$. Thus

$$\begin{aligned} E_1 &\equiv 5u^4 \pmod{25}, \\ E_2 &\equiv 5u^4 \pmod{25}, \\ F &\equiv 20u^2 \pmod{25}, \\ G &\equiv 10u^3 \pmod{25}, \\ H &\equiv 15u^3 \pmod{25}, \\ J &\equiv 0 \pmod{25}, \\ L &\equiv 0 \pmod{25}. \end{aligned}$$

As $(u, v) = 1$ we have $5 \nmid u$. Thus $5 \parallel E_1, 5 \parallel E_2, 5 \parallel F, 5 \parallel G, 5 \parallel H, 5^2 \mid J$ and $5^2 \mid L$. □

We now show that $2u - v \not\equiv 0 \pmod 5$ implies $\alpha = 0$. By the Lemma we have

$$5 \nmid E_1,\ E_2,\ F,\ G,\ H,\ J,\ L, \tag{4.12}$$

and by (4.1)

$$5 \parallel h_3,\quad 5 \parallel h_2,\quad 5 \parallel h_1,\quad 5 \nmid h_0.$$

Thus by (4.2) we have

$$5 \nmid m \tag{4.13}$$

and by (4.4) we have

$$5 \parallel k_3,\quad 5 \parallel k_2,\quad 5 \parallel k_1,\quad 5 \nmid k_0. \tag{4.14}$$

Now by (4.5), (4.13) and (4.14) we have $5^{20} \mid \text{disc}\,(k_{u,v})$. By (4.13) the conditions $5^4 \parallel k_0$, $5^4 \mid k_1, 5^4 \mid k_2, 5^3 \mid k_3$ do not hold. Thus by (4.10) we have $\alpha = 0$.

Finally we show that $2u - v \equiv 0 \pmod 5$ implies $\alpha = 2$. In this case $5 \nmid u, 5 \nmid v$. By the Lemma we have

$$5 \parallel E_1,\ E_2,\ F,\ G,\ H \text{ and } 5^2 \mid J,\ L, \tag{4.15}$$

and by (4.1)

$$5^4 \parallel h_3,\ 5^5 \parallel h_2,\ 5^7 \mid h_1,\ 5^5 \mid h_0.$$

As $5^5 \mid h_0$ and $5^5 \parallel h_2$, we see from (4.2) that

$$5 \parallel m \tag{4.16}$$

and thus from (4.4) we have

$$5^2 \parallel k_3,\quad 5^2 \parallel k_2,\quad 5^3 \mid k_1. \tag{4.17}$$

Now, by (4.5), (4.15) and (4.16), we have $5^{12} \parallel \text{disc}\,(k_{u,v})$ so that $5^{20} \nmid \text{disc}\,(k_{u,v})$. By (4.17) the conditions $5 \mid k_1, 5 \mid k_2, 5 \mid k_3$ hold. So by (4.10) we have $\alpha = 2$. Thus

$$\alpha = \begin{cases} 0, \text{if } 2u - v \not\equiv 0 (\text{mod } 5), \\ 2, \text{if } 2u - v \equiv 0 (\text{mod } 5). \end{cases} \tag{4.18}$$

Theorem 3 now follows from (4.9), (4.10), (4.11) and (4.18). □

REFERENCES

1. L. Cangelmi, Polynomials with Frobenius Galois groups, *Comm. Algebra*, **28** (2000), 845–859.
2. D. S. Dummit, Solving solvable quintics, *Math. Comp.*, **57** (1991), 387–401.
3. O. Lecacheux, Unités d'une famille de corps lié's à la courbe $X_1(25)$, *Ann. Inst. Fourier (Grenoble)*, **40** (1990), 237–253.

4. O. Lecacheux, Constructions de polynômes génériques à groupe de Galois résoluble, *Acta Arith.*, **86** (1998), 207–216.

5. E. Lehmer, Connection between Gaussian periods and cyclic units, *Math. Comp.*, **50** (1988), 535–541.

6. L. Soicher, The computation of Galois groups, *M. Comp. Sci. thesis*, Concordia University, Montréal, (1981).

7. B. K. Spearman and K. S. Williams, The discriminant of a cyclic field of odd prime degree, *Rocky Mountain J. Math.*, **32** (2003), 1101–1122.