ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 33, Number 3, Fall 2003

# THE DISCRIMINANT OF A CYCLIC FIELD OF ODD PRIME DEGREE

BLAIR K. SPEARMAN AND KENNETH S. WILLIAMS

ABSTRACT. Let $p$ be an odd prime. Let $f(x) \in \mathbf{Z}[x]$ be a defining polynomial for a cyclic extension field $K$ of the rational number field $\mathbf{Q}$ with $[K:\mathbf{Q}] = p$. An explicit formula for the discriminant $d(K)$ of $K$ is given in terms of the coefficients of $f(x)$.

**1. Introduction.** Throughout this paper $p$ denotes an odd prime. Let $K$ be a cyclic extension field of the rational field $\mathbf{Q}$ with $[K:\mathbf{Q}] = p$. In this paper we give an explicit formula for the discriminant $d(K)$ of $K$ in terms of the coefficients of a defining polynomial for $K$. We prove

**Theorem 1.** *Let* $f(X) = X^p + a_{p-2}X^{p-2} + \cdots + a_1X + a_0 \in \mathbf{Z}[X]$ *be such that*

$$\mathrm{Gal}\,(f) \simeq \mathbf{Z}/p\mathbf{Z} \tag{1}$$

*and*

(2) *there does not exist a prime* $q$ *such that*

$$q^{p-i} | a_i, \quad i = 0, 1, \ldots, p-2.$$

*Let* $\theta \in \mathbf{C}$ *be a root of* $f(X)$ *and set* $K = \mathbf{Q}(\theta)$ *so that* $K$ *is a cyclic extension of* $\mathbf{Q}$ *with* $[K:\mathbf{Q}] = p$. *Then*

$$d(K) = f(K)^{p-1}, \tag{3}$$

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

$$f(K) = p^{\alpha} \prod_{\substack{q \equiv 1 \ (\mathrm{mod}\ p) \\ q | a_i, i=0,1,\ldots,p-2}} q, \tag{4}$$

Received by the editors on December 7, 2000.
2000 *AMS Mathematics Subject Classification.* 11R09, 11R16, 11R20, 11R29.
Research of the first author supported by a grant from the Natural Sciences and Engineering Research Council of Canada.
Research of the second author supported by a grant from the Natural Sciences and Engineering Research Council of Canada, grant A-7233.

*where $q$ runs through primes, and*

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

This theorem will follow from a number of lemmas proved in Section 2. In Section 3 Theorem 1 is applied to some quintic polynomials introduced by Lehmer [**5**] in 1988. In Section 4 some numerical examples illustrating Theorem 1 are given.

**2. Results on the ramification of a prime in a cyclic field of odd prime degree.** We begin with the following result.

**Lemma 1.** *Let $g(X) \in \mathbf{Z}[X]$ be a monic polynomial of degree $p$ having $\operatorname{Gal}(g) \simeq \mathbf{Z}/p\mathbf{Z}$. Let $\theta \in \mathbf{C}$ be a root of $g(X)$ and set $K = \mathbf{Q}(\theta)$. Let $q$ be a prime. If $q$ ramifies in $K$, then there exists an integer $r$ such that*

$$g(X) \equiv (X - r)^p \pmod{q}.$$

*Proof.* Suppose that the prime $q$ ramifies in $K$. As $K$ is a cyclic extension of $\mathbf{Q}$, it is a normal extension, and so

$$q = Q^p$$

for some prime ideal $Q$ of $K$. Thus,

$$|O_K/Q| = N(Q) = q,$$

and so, as $\theta \in O_K$, there exists $r \in \mathbf{Z}$ such that

$$\theta \equiv r \pmod{Q}. \tag{5}$$

Let $\theta = \theta_1, \dots, \theta_p \in \mathbf{C}$ be the roots of $g(X)$. Taking conjugates of (5), we obtain

$$\theta_i \equiv r \pmod{Q}, \quad i = 1, 2, \dots, p.$$

Hence,

$$g(X) = \prod_{i=1}^{p}(X - \theta_i) \equiv \prod_{i=1}^{p}(X - r) \equiv (X - r)^p \pmod{Q}.$$

Since $g(X) \in \mathbf{Z}[X]$, $(X - r)^p \in \mathbf{Z}[X]$ and $q = Q^p$, we deduce that

$$g(X) \equiv (X - r)^p \pmod{q},$$

as asserted. $\square$

From this point on, we assume that $f(X) = X^p + a_{p-2}X^{p-2} + \cdots + a_1X + a_0 \in \mathbf{Z}[X]$ is such that (1) and (2) hold. We let $\theta = \theta_1, \dots, \theta_p \in \mathbf{C}$ be the roots of $f(X)$ and we set $K = \mathbf{Q}(\theta)$ so that $K$ is a cyclic extension of degree $p$.

**Lemma 2.** *Let $q$ be a prime $\neq p$. Then $q$ ramifies in $K \Leftrightarrow q \mid a_i$, $i = 0, 1, \dots, p-2$.*

*Proof.* (a) Suppose that $q$ ramifies in $K$. Then, by Lemma 1, there exists an integer $r$ such that

$$f(X) \equiv (X - r)^p \pmod{q},$$

that is,

$$\begin{aligned} &X^p + a_{p-2}X^{p-2} + \cdots + a_1X + a_0 \\ &\equiv X^p - prX^{p-1} + \binom{p}{2} r^2 X^{p-2} \\ &\quad - \cdots - r^p \pmod{q}. \end{aligned}$$

Equating the coefficients of $X^{p-1}$ (mod $q$), we see that $0 \equiv -pr$ (mod $q$). As $p \neq q$ we must have $q \mid r$. From the coefficients of $X^i$, $i = 0, 1, \dots, p-2$, we deduce that

$$a_i \equiv (-1)^{i+1} \binom{p}{i} r^{p-i} \pmod{q},$$

so that

$$q \mid a_i, \quad i = 0, 1, \dots, p-2.$$

(b) Now suppose that

$$q \mid a_i, \quad i = 0, 1, \dots, p-2,$$

but that $q$ does not ramify in $K$. Then

$$q = Q_1 \cdots Q_t, \quad t = 1 \text{ or } p,$$

where the $Q_i$ are distinct prime ideals in $K$. We have

$$0 = f(\theta) = \theta^p + a_{p-2}\theta^{p-2} + \cdots + a_1\theta + a_0 \equiv \theta^p \pmod{q},$$

so that $Q_i \mid \theta^p$ for $i = 1, \dots, t$. As $Q_i$ is a prime ideal, we deduce that $Q_i \mid \theta$ for $i = 1, \dots, t$, and so $q \mid \theta$. This shows that $\theta/q \in O_K$. The minimal polynomial of $\theta/q$ over $\mathbf{Q}$ is

$$X^p + \frac{a_{p-2}}{q^2} X^{p-2} + \cdots + \frac{a_1}{q^{p-1}} X + \frac{a_0}{q^p},$$

which must belong in $\mathbf{Z}[X]$. Hence we have

$$q^{p-i} \mid a_i, \quad i = 0, 1, \dots, p-2,$$

contradicting (2). Hence $q$ ramifies in $K$. $\square$

**Lemma 3.** *If*

$$p \mid a_i, \quad i = 1, 2, \dots, p-2 \text{ does not hold}$$

*then $p$ does not ramify in $K$.*

*Proof.* Suppose on the contrary that $p$ ramifies in $K$. By Lemma 1 there exists an integer $r$ such that

$$f(X) \equiv (X-r)^p \pmod p$$

so that

$$X^p + a_{p-2}X^{p-2} + \cdots + a_1 X + a_0 \equiv X^p - r \pmod p$$

and thus

$$p \mid a_i, \quad i = 1, 2, \dots, p-2,$$

which is a contradiction. Hence $p$ does not ramify in $K$. □

**Lemma 4.** *If*

$$p^{p(p-1)} \nmid \operatorname{disc}(f)$$

*and*

$$p \mid a_i, \quad i = 1, 2, \dots, p-2,$$

*then $p$ ramifies in $K$.*

*Proof.* Suppose $p$ does not ramify in $K$. Then

$$p = Q_1 \cdots Q_t, \quad t = 1 \text{ or } p$$

for distinct prime ideals $Q_i$, $i = 1, \dots, t$, of $K$. Now

$$\begin{aligned} 0 = f(\theta) = \theta^p + a_{p-2}\theta^{p-2} + \cdots + a_0 \equiv \theta^p + a_0 \\ \equiv \theta^p + a_0^p \equiv (\theta + a_0)^p \pmod p \end{aligned}$$

so that $Q_i \mid (\theta + a_0)^p$ and thus $Q_i \mid \theta + a_0$ for $i = 1, \dots, t$. Hence $Q_1 Q_2 \cdots Q_t \mid \theta + a_0$ and so $p \mid \theta + a_0$. By conjugation, as $K$ is a normal extension of $\mathbf{Q}$, we deduce that

$$p \mid \theta_i + a_0, \quad i = 1, 2, \dots, p.$$

Hence

$$p \mid \theta_i - \theta_j, \quad 1 \le i < j \le p,$$

and so

$$p^{p(p-1)} \Big| \prod_{1 \le i < j \le p} (\theta_i - \theta_j)^2,$$

that is,

$$p^{p(p-1)} \mid \operatorname{disc}(f),$$

contradicting $p^{p(p-1)} \nmid \operatorname{disc}(f)$. This proves that $p$ ramifies in $K$. $\square$

**Lemma 5.** *If*

$$p^{p-1} \| a_0, p^{p-1} \mid a_1, p^{p+1-i} | a_i, \quad i = 2, \dots, p-2,$$

*then*

(a) *$p$ ramifies in $K$*

*and*

(b) $p^{p(p-1)} \mid \operatorname{disc}(f)$.

*Proof.* We define $b_0, \dots, b_{p-2} \in \mathbf{Z}$ by

$$b_0 = a_0/p^{p-1}, b_1 = a_1/p^{p-1}, b_i = a_i/p^{p+1-i}, \quad i = 2, \dots, p-2.$$

Clearly $p \nmid b_0$. We set

$$h(X) = X^p + pb_1X^{p-1} + \sum_{i=2}^{p-2} p^2 b_0^{i-1} b_i X^{p-i} + pb_0^{p-1} \in \mathbf{Z}[X].$$

Then

$$\begin{aligned} h(b_0pX) &= b_0^p p^p X^p + b_0^{p-1} b_1 p^p X^{p-1} + \sum_{i=2}^{p-2} b_0^{p-1} b_i p^{p+2-i} X^{p-i} + pb_0^{p-1} \\ &= b_0^{p-1} pX^p \left( b_0 p^{p-1} + b_1 \frac{p^{p-1}}{X} + \sum_{i=2}^{p-2} b_i \frac{p^{p+1-i}}{X^i} + \frac{1}{X^p} \right) \\ &= b_0^{p-1} pX^p \left( a_0 + \frac{a_1}{X} + \sum_{i=2}^{p-2} \frac{a_i}{X^i} + \frac{1}{X^p} \right) \\ &= b_0^{p-1} pX^p f\left( \frac{1}{X} \right). \end{aligned}$$

Hence $h(X)$ can be taken as the defining polynomial for the field $K$. Since $h(X)$ is $p$-Eisenstein we have $p = \wp^p$ for some prime ideal $\wp$ of $K$, see, for example, [**7**, Proposition 4.18, p. 181]. Thus $p$ ramifies in $K$.

Next we define the nonnegative integer $k$ by $\wp^k \| \theta$. Then by conjugation we have $\wp^k \| \theta_i$, $i = 1, 2, \ldots, p$. Hence,

$$\wp^{pk} \| \theta_1 \cdots \theta_p = -a_0.$$

But $p^{p-1} \| a_0$ so that $\wp^{p(p-1)} \| a_0$. Hence $pk = p(p-1)$, that is, $k = p-1$ and $\wp^{p-1} \| \theta$.

Further,

$$f'(\theta) = p\theta^{p-1} + \sum_{i=2}^{p-2} i a_i \theta^{i-1} + a_1.$$

We have

$$\begin{aligned} \wp^{p+(p-1)^2} &\ \| \ p\theta^{p-1}, \\ \wp^{p(p+1-i)+(p-1)(i-1)} &\mid i a_i \theta^{i-1}, \quad i = 2, \ldots, p-2, \\ \wp^{p(p-1)} &\mid a_1. \end{aligned}$$

As

$$p + (p-1)^2 = p^2 - p + 1 > p(p-1)$$

and

$$\begin{aligned} p(p+1-i) + (p-1)(i-1) &= p^2 - i + 1 \geq p^2 - (p-2) + 1 \\ &= p^2 - p + 3 > p(p-1), \end{aligned}$$

we see that

$$\wp^{p(p-1)} \mid f'(\theta).$$

By conjugation we deduce that

$$\wp^{p(p-1)} \mid f'(\theta_i), \quad i = 1, \ldots, p,$$

so that

$$\wp^{p^2(p-1)} \Big| \prod_{i=1}^{p} f'(\theta_i),$$

that is,

$$p^{p(p-1)} \mid \operatorname{disc}(f).$$

This completes the proof of Lemma 5. $\square$

**Lemma 6.** *If*

$$p^{p(p-1)} \mid \operatorname{disc}(f)$$

*and*

$$p^{p-1} \| a_0, p^{p-1} | a_1, p^{p+1-i} | a_i, \quad i = 2, \dots, p-2, \quad \textit{does not hold},$$

*then $p$ does not ramify in $K$.*

*Proof.* Suppose $p$ ramifies in $K$. Then $p = \wp^p$ for some prime ideal $\wp$ in $K$. As $N(\wp) = p$ there exists $r \in \mathbf{Z}$ with $0 \leq r \leq p-1$ such that

$$\theta \equiv r \pmod{\wp}.$$

We consider two cases.

*Case* (i): $r = 0$. In this case $\wp \mid \theta$ so that $\wp^k \| \theta$ for some positive integer $k$. Suppose that $k \geq p$. Then $p \mid \theta$ and thus $\theta/p \in O_K$. The minimal polynomial of $\theta/p$ over $\mathbf{Q}$ is

$$X^p + \frac{a_{p-2}}{p^2} X^{p-2} + \cdots + \frac{a_1}{p^{p-1}} X + \frac{a_0}{p^p},$$

which must belong in $\mathbf{Z}[X]$. Hence we have

$$p^{p-i} \mid a_i, \quad i = 0, 1, \dots, p-2,$$

contradicting (2). Thus $1 \leq k \leq p-1$.

Next we define the nonnegative integer $l$ by $\wp^l \| f'(\theta)$. By conjugation we have $\wp^l \| f'(\theta_i)$, $i = 1, 2, \dots, p$. Hence

$$\wp^{pl} \Big\| \prod_{i=1}^{p} f'(\theta_i) = \pm \operatorname{disc}(f).$$

But $\wp^{p^2(p-1)} = p^{p(p-1)} \mid \operatorname{disc}(f)$, so we must have $pl \geq p^2(p-1)$, that is, $l \geq p(p-1)$. Hence

$$\wp^{p(p-1)} \mid f'(\theta). \tag{6}$$

Now

$$f'(\theta) = p\theta^{p-1} + \sum_{i=2}^{p-1}(p-i)a_{p-i}\theta^{p-i-1}, \tag{7}$$

where

$$v_\wp(p\theta^{p-1}) = p + (p-1)k$$

and

$$v_\wp((p-i)a_{p-i}\theta^{p-i-1}) = v_\wp(a_{p-i}) + (p-i-1)k, \quad i = 2, \dots, p-1.$$

Clearly,

$$v_\wp(p\theta^{p-1}) \equiv -k \pmod p$$

and

$$v_\wp((p-i)a_{p-i}\theta^{p-i-1}) \equiv -ik - k \pmod p, \quad i = 2, \dots, p-1.$$

Since $\{-ik-k \mid i = 0, 1, \dots, p-1\}$ is a complete residue system modulo $p$, $v_\wp(p\theta^{p-1})$ and $v_\wp((p-i)a_{p-i}\theta^{p-i-1})$, $i = 2, \dots, p-1$, are all distinct. Hence, by (6) and (7), we have

$$v_\wp(p\theta^{p-1}) \geq p(p-1)$$

and

$$v_\wp((p-i)a_{p-i}\theta^{p-i-1}) \geq p(p-1), \quad i = 2, \dots, p-1.$$

Thus

$$p + (p-1)k \geq p(p-1) \tag{8}$$

and

$$v_\wp(a_{p-i}) + (p-i-1)k \geq p(p-1), \quad i = 2, \dots, p-1. \tag{9}$$

From (8) we deduce that $k \geq p-1$. As $1 \leq k \leq p-1$, we must have $k = p-1$ so $\wp^{p-1} \| \theta$. From (9), we obtain

$$v_\wp(a_{p-i}) \geq (i+1)(p-i),$$

so that

$$v_p(a_{p-i}) \geq \frac{(i+1)(p-1)}{p}, \quad i = 2, \ldots, p-1.$$

Hence

$$v_p(a_{p-i}) \geq i+1, \quad \text{if } i = 2, \ldots, p-2,$$

and

$$v_p(a_1) \geq p-1.$$

Thus

$$\begin{aligned} \wp^{p(p-1)} &\mid \theta^p \\ \wp^{p(i+1)+(p-i)(p-1)} &\mid a_{p-i}\theta^{p-i}, \quad i = 2, \ldots, p-2, \\ \wp^{p(p-1)+(p-1)} &\mid a_1\theta, \end{aligned}$$

so that

$$\wp^{p^2-p} \mid \theta^p + \sum_{i=2}^{p-1} a_{p-i}\theta^{p-i} = -a_0.$$

Hence,

$$p^{p-1} \mid a_0.$$

Since $p^{p-1} \mid a_1$, $p^{p-2} \mid a_2, \ldots, p^2 \mid a_{p-2}$, we must have by (2) that $p^p \nmid a_0$. This proves that $p^{p-1} \| a_0$, contradicting the second assumption of the lemma.

*Case* (ii): $r = 1, 2, \ldots, p-1$. We set

$$g(X) = f(X+r) = \sum_{j=0}^{p} b_j X^j \in \mathbf{Z}[X]$$

so that, with $a_{p-1} = 0$, $a_p = 1$,

$$b_j = \sum_{i=j}^{p} a_i \binom{i}{j} r^{i-j}, \quad j = 0, 1, \ldots, p.$$

In particular, we have $b_{p-1} = rp$, $b_p = 1$. Further, we set $\alpha = \theta - r$ so that $\alpha \equiv 0 \pmod{\wp}$. Moreover, $g(\alpha) = f(\alpha + r) = f(\theta) = 0$ so that $\alpha$ is a root of $g(X)$. Define the positive integer $k$ by $\wp^k \| \alpha$. If $k \geq p$ then $\alpha/p \in O_K$ and, as the minimal polynomial of $\alpha/p$ is

$$g^*(X) = \sum_{j=0}^{p} \frac{b_j}{p^{p-j}} X^j,$$

we must have

$$\frac{b_j}{p^{p-j}} \in \mathbf{Z}, \quad j = 0, 1, \dots, p.$$

By Lemma 1 there exists an integer $s$ such that

$$g^*(X) \equiv (X - s)^p \pmod{p}.$$

Thus

$$r = b_{p-1}/p = \text{ coefficient of } X^{p-1} \text{ in } g^*(X) \equiv -ps \equiv 0 \pmod{p},$$

contradicting $1 \leq r \leq p - 1$. Hence, $k = 1, 2, \dots, p - 1$.

Now let $\alpha = \alpha_1, \dots, \alpha_p \in \mathbf{C}$ be the roots of $g(X)$, so that

$$\wp^{p^2(p-1)} = p^{p(p-1)} \mid \operatorname{disc}(f) = \operatorname{disc}(g) = \pm \prod_{i=1}^{p} g'(\alpha_i).$$

Suppose that $\wp^t \| g'(\alpha)$. By conjugation we have $\wp^t \| g'(\alpha_i)$, $i = 1, 2, \dots, p$. Hence,

$$\wp^{pt} \Big\| \prod_{i=1}^{p} g'(\alpha_i). \tag{10}$$

Further

$$g'(\alpha) = p\alpha^{p-1} + rp(p-1)\alpha^{p-2} + \sum_{i=1}^{p-2} i b_i \alpha^{i-1} \tag{11}$$

and

$$\begin{aligned} v_\wp(p\alpha^{p-1}) &= p + (p-1)k, \\ v_\wp(rp(p-1)\alpha^{p-2}) &= p + (p-2)k, \\ v_\wp(i b_i \alpha^{i-1}) &= v_\wp(b_i) + (i-1)k, \quad i = 1, \dots, p-2. \end{aligned}$$

Since

$$v_\wp(p\alpha^{p-1}),\ v_\wp(rp(p-1)\alpha^{p-2}),\ v_\wp(ib_i\alpha^{i-1}),\quad i=1,\dots,p-2,$$

are all distinct modulo $p$, they must all be different. From (10) and (11), we deduce

$$\begin{cases} \wp^{p(p-1)} \mid p\alpha^{p-1}, & \wp^{p(p-1)} \mid rp(p-1)\alpha^{p-2}, \\ \wp^{p(p-1)} \mid ib_i\alpha^{i-1}, & i=1,\dots,p-2. \end{cases} \tag{12}$$

From the first of these, we have

$$p(p-1) \le p + (p-1)k$$

so that

$$k \ge \frac{p^2-2p}{p-1}.$$

As $k \in \mathbf{Z}$ we must have $k \ge p-1$. Since $k \in \{1,2,\dots,p-1\}$, we deduce that $k=p-1$. Then, from the second divisibility condition in (12), we deduce that

$$p(p-1) \le p+(p-2)k = p+(p-2)(p-1) = p^2-2p+2,$$

which is impossible.

In both cases we have been led to a contradiction. Thus $p$ does not ramify in $K$. □

**3. Proof of Theorem 1.** It is well known, see, for example, [**6**, p. 831], that

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

and

$$f(K) = p^\alpha \prod_{\substack{q\equiv 1 \pmod p \\ q \text{ ramifies in } K}} q,$$

where $q$ runs through primes and

$$\alpha = \begin{cases} 0 & \text{if } p \text{ does not ramify in } K, \\ 2 & \text{if } p \text{ ramifies in } K. \end{cases}$$

Clearly, by Lemma 2, we have

$$\prod_{\substack{q\equiv 1 \pmod p \\ q \text{ ramifies in } K}} = \prod_{\substack{q\equiv 1 \pmod p \\ q \mid a_i, i=0,1,\dots,p-2}} q.$$

Finally we treat the prime $p$. We consider four cases.

(I) $p^{p(p-1)} \nmid \operatorname{disc}(f)$, $p \mid a_i$, $i = 1, \dots, p-2$, does not hold,

(II) $p^{p(p-1)} \nmid \operatorname{disc}(f)$, $p \mid a_i$, $i = 1, \dots, p-2$, holds,

(III) $p^{p(p-1)} \mid \operatorname{disc}(f)$, $p^{p-1} \| a_0$, $p^{p-1} \mid a_1$, $p^{p+1-i} \mid a_i$, $i = 2, \dots, p-2$, holds,

(IV) $p^{p(p-1)} \mid \operatorname{disc}(f)$, $p^{p-1} \| a_0$, $p^{p-1} \mid a_1$, $p^{p+1-i} \mid a_i$, $i = 2, \dots, p-2$, does not hold.

In Case (I), by Lemma 3, $p$ does not ramify in $K$, and so $\alpha = 0$. In Case (II), by Lemma 4, $p$ ramifies in $K$, and so $\alpha = 2$. In Case (III), by Lemma 5, $p$ ramifies in $K$, and so $\alpha = 2$. In Case (IV), by Lemma 6, $p$ does not ramify in $K$, and so $\alpha = 0$.

This completes the proof of Theorem 1. □

We conclude this section by looking at the case $p = 3$ in some detail. Let $f(X) = X^3 + aX + b \in \mathbf{Z}[X]$ be such that $\operatorname{Gal}(f) \simeq \mathbf{Z}/3\mathbf{Z}$ and suppose that there does not exist a prime $q$ such that $q^2 \mid a$ and $q^3 \mid b$. Here $\operatorname{disc}(f) = -4a^3 - 27b^2$. As $\operatorname{Gal}(f) \simeq \mathbf{Z}/3\mathbf{Z}$, we have

$$-4a^3 - 27b^2 = c^2$$

for some positive integer $c$. Since $3^2 \mid a$, $3^3 \mid b$ cannot occur, we deduce as in [**4**, p. 4] that exactly one of the following four possibilities occurs:

(i) $3 \nmid a$, $3 \nmid c$,

(ii) $3 \| a$, $3 \nmid b$, $3^2 \| c$,

(iii) $3 \| a$, $3 \nmid b$, $3^3 \mid c$,

(iv) $3^2 \| a$, $3^2 \| b$, $3^3 \| c$.

Clearly (i) is equivalent to

(i)′ $3^6 \nmid \operatorname{disc}(f)$, $3 \nmid a$;

(ii) is equivalent to

(ii)′ $3^6 \nmid \operatorname{disc}(f)$, $3 \mid a$;

(iii) is equivalent to

(iii)′ $3^6 \mid \operatorname{disc}(f)$, $3 \| a$;

(iv) is equivalent to

(iv)′ $3^6 \mid \operatorname{disc}(f)$, $3^2 \mid a$, $3^2 \| b$.

By Theorem 1, we have

$$f(K) = 3^{\alpha} \prod_{\substack{q \equiv 1 \pmod 3 \\ q \mid a,\ q \mid b}} q,$$

where $q$ runs through primes, and

$$\alpha = \begin{cases} 0 & \text{in cases (i)}', \text{(iii)}', \\ 2 & \text{in cases (ii)}', \text{(iv)}', \end{cases}$$

that is,

$$\alpha = \begin{cases} 0 & \text{in cases (i), (iii)}, \\ 2 & \text{in cases (ii), (iv)}, \end{cases}$$

in agreement with [**4**].

**3. Emma Lehmer's quintics.** Let $t \in \mathbf{Q}$ and set

$$f_t(X) = X^5 + a_4(t)X^4 + a_3(t)X^3 + a_2(t)X^2 + a_1(t)X + a_0(t), \tag{13}$$

where

$$\begin{aligned} a_4(t) &= t^2, \\ a_3(t) &= -(2t^3 + 6t^2 + 10t + 10), \\ a_2(t) &= t^4 + 5t^3 + 11t^2 + 15t + 5, \\ a_1(t) &= t^3 + 4t^2 + 10t + 10, \\ a_0(t) &= 1. \end{aligned} \tag{14}$$

These polynomials were introduced by Lehmer [**5**] in 1988 and have been discussed by Schoof and Washington [**8**], Darmon [**2**] and Gaál and Pohst [**3**]. We set

$$t = u/v,\ u \in \mathbf{Z},\ v \in \mathbf{Z}, \quad (u,v) = 1,\ v > 0. \tag{15}$$

It is convenient to define

$$
\begin{aligned}
E = E(u,v) &= u^4 + 5u^3v + 15u^2v^2 + 25uv^3 + 25v^4, \\
F = F(u,v) &= 4u^2 + 10uv + 5v^2, \\
G = G(u,v) &= 3u^4 + 15u^3v + 20u^2v^2 - 50v^4, \\
H = H(u,v) &= 4u^6 + 30u^5v + 65u^4v^2 - 200u^2v^4 \\
&\qquad - 125uv^5 + 125v^6, \\
I = I(u,v) &= u^3 + 5u^2v + 10uv^2 + 7v^3, \\
J = J(u,v) &= 12u^5 + 58u^4v + 15u^3v^2 - 130u^2v^3 \\
&\qquad - 175uv^4 + 200v^5, \\
L = L(u,v) &= 3u^3 + 7u^2v + 20uv^2 + 15v^3.
\end{aligned} \tag{16}
$$

Let $\theta$ be a root of $f_t(x)$ and set $K = \mathbf{Q}(\theta)$. As an application of Theorem 1, we prove the following result.

**Theorem 2.** *With the above notation, if $K$ is a cyclic quintic field, then its conductor $f(K)$ is given by*

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

*where $q$ runs through primes, and*

$$
\alpha = \begin{cases} 0 & \text{if } 5 \nmid u, \\ 2 & \text{if } 5 \mid u. \end{cases}
$$

We remark that when $t \in \mathbf{Z}$, equivalently $v = 1$, it is known that $K$ is a cyclic quintic field [**8**]. The special case of Theorem 2 when $E(u,1)$ is squarefree is given in [**3**].

*Proof.* We have

$$
g_t(X) = 5^5 f_t((X - t^2)/5) = X^5 + g_3X^3 + g_2X^2 + g_1X + g_0, \tag{17}
$$

where

$$
\begin{aligned}
g_3 &= -10t^4 - 50t^3 - 150t^2 - 250t - 250, \\
g_2 &= 20t^6 + 150t^5 + 575t^4 + 1375t^3 + 2125t^2 \\
&\quad + 1875t + 625, \\
g_1 &= -15t^8 - 150t^7 - 700t^6 - 2000t^5 - 3500t^4 \\
&\quad - 3125t^3 + 1250t^2 + 6250t + 6250, \\
g_0 &= 4t^{10} + 50t^9 + 275t^8 + 875t^7 + 1625t^6 + 1250t^5 \\
&\quad - 1875t^4 - 6250t^3 - 6250t^2 + 3125.
\end{aligned} \tag{18}
$$

Next we set

$$h_{u,v}(X) = v^{10} g_{u/v}(X/v^2) = X^5 + h_3X^3 + h_2X^2 + h_1X + h_0, \tag{19}$$

where

$$
\begin{aligned}
h_3 &= -10u^4 - 50u^3v - 150u^2v^2 - 250uv^3 - 250v^4 \\
&= -10(u^4 + 5u^3v + 15u^2v^2 + 25uv^3 + 25v^4); \\
h_2 &= 20u^6 + 150u^5v + 575u^4v^2 + 1375u^3v^3 + 2125u^2v^4 \\
&\quad + 1875uv^5 + 625v^6 \\
&= 5(u^4 + 5u^3v + 15u^2v^2 + 25uv^3 + 25v^4)(4u^2 + 10uv + 5v^2); \\
h_1 &= -15u^8 - 150u^7v - 700u^6v^2 - 2000u^5v^3 - 3500u^4v^4 \\
&\quad - 3125u^3v^5 + 1250u^2v^6 + 6250uv^7 + 6250v^8 \\
&= -5(u^4 + 5u^3v + 15u^2v^2 + 25uv^3 + 25v^4) \\
&\quad \times (3u^4 + 15u^3v + 20u^2v^2 - 50v^4); \\
h_0 &= 4u^{10} + 50u^9v + 275u^8v^2 + 875u^7v^3 + 1625u^6v^4 \\
&\quad + 1250u^5v^5 - 1875u^4v^6 - 6250u^3v^7 - 6250u^2v^8 + 3125v^{10} \\
&= (u^4 + 5u^3v + 15u^2v^2 + 25uv^3 + 25v^4) \\
&\quad \times (4u^6 + 30u^5v + 65u^4v^2 - 200u^2v^4 - 125uv^5 + 125v^6);
\end{aligned}
$$

so that by (16) we have

$$h_3 = -10E,\ h_2 = 5EF,\ h_1 = -5EG,\ h_0 = EH. \tag{20}$$

Next let $m$ denote the largest positive integer such that

$$m^2|h_3,\ m^3|h_2,\ m^4|h_1,\ m^5|h_0, \tag{21}$$

and set

$$k_{u,v}(X) = h_{u,v}(mX)/m^5 = X^5 + k_3X^3 + k_2X^2 + k_1X + k_0, \tag{22}$$

where

$$k_3 = h_3/m^2,\ k_2 = h_2/m^3,\ k_1 = h_1/m^4,\ k_0 = h_0/m^5. \tag{23}$$

Appealing to MAPLE, we find

$$\mathrm{disc}\,(k_{u,v}) = 5^{20}E^4I^2v^{18}/m^{20} \tag{24}$$

and

$$EJ - HL = 5^5v^9. \tag{25}$$

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

$$f(K) = 5^{\alpha} \prod_{\substack{q\equiv 1 \pmod 5 \\ q|k_0,\ q|k_1,\ q|k_2,\ q|k_3}} q, \tag{26}$$

where $q$ runs through primes, and

$$\alpha = \begin{cases} 0 & \text{if } 5^{20} \nmid \mathrm{disc}\,(k_{u,v}) \text{ and } 5 \mid k_1,\ 5 \mid k_2,\ 5 \mid k_3 \\ & \text{does not hold, or} \\ & 5^{20} \mid \mathrm{disc}\,(k_{u,v}) \text{ and } 5^4 \| k_0, 5^4 \mid k_1, 5^4 \mid k_2, 5^3 \mid k^3 \\ & \text{does not hold,} \\ 2 & \text{if } 5^{20} \nmid \mathrm{disc}\,(k_{u,v}) \text{ and } 5 \mid k_1, 5 \mid k_2, 5 \mid k_3, \\ & \text{or } 5^{20} \mid \mathrm{disc}\,(k_{u,v}) \text{ and } 5^4 \| k_0, 5^4 \mid k_1, 5^4 \mid k_2, 5^3 \mid k_3. \end{cases} \tag{27}$$

Let $q$ be a prime with

$$q \equiv 1 \pmod 5, \quad q \mid k_3,\ q \mid k_2,\ q \mid k_1,\ q \mid k_0.$$

We show that

$$q \mid E,\ v_q(E) \not\equiv 0 \pmod 5.$$

By (23) we have

$$q \mid h_3,\ q \mid h_2,\ q \mid h_1,\ q \mid h_0.$$

As $q \equiv 1 \pmod 5$, we have $q \neq 2, 5$. Thus, from (20), we deduce that $q \mid E$. Suppose next that $q \mid v$. Then, from the definition of $E$ in (16) we see that $q \mid u$, contradicting $(u, v) = 1$. Hence $q \nmid v$. Then, from (25), we deduce that $q \nmid H$. If $v_q(E) \equiv 0 \pmod 5$, say $v_q(E) = 5w$, $w \geq 1$, then by (20) we have

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

so that by (21) we have

$$q^w \| m.$$

Thus by (23),

$$q \nmid h_0/m^5 = k_0,$$

a contradiction. Hence $v_q(E) \not\equiv 0 \pmod 5$.

Conversely, let $q$ be a prime with

$$q \equiv 1 \pmod 5, \quad q \mid E, \quad v_q(E) \not\equiv 0 \pmod 5.$$

We show that

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

Suppose that $q \mid v$. Then, by the definition of $E$ in (16), we have $q \mid u$, contradicting $(u, v) = 1$. Hence $q \nmid v$. Thus, by (25), we see that $q \nmid H$. As $v_q(E) \not\equiv 0 \pmod 5$, we have $q^{5z+r} \| E$, where $z$ is a nonnegative integer and $r = 1, 2, 3, 4$. Thus by (20) we have

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

This shows by (21) that

$$q^z \| m$$

so that by (23)

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

proving

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

We have shown that

$$\prod_{\substack{q\equiv 1 \pmod 5\\ q|k_0,\ q|k_1,\ q|k_2,\ q|k_3}} q = \prod_{\substack{q\equiv 1 \pmod 5\\ q|E\\ v_q(E)\not\equiv 0 \pmod 5}} q. \tag{28}$$

Finally, to complete the proof of Theorem 2, we show that

$$\alpha = \begin{cases} 0 & \text{if } 5 \nmid u, \\ 2 & \text{if } 5 \mid u. \end{cases} \tag{29}$$

If $5 \mid u$, then by (15), $5 \nmid v$ and, by (16),

$$5^2 \| E,\ 5 \| F,\ 5^2 \| G,\ 5^3 \| H,\ 5 \nmid I.$$

Hence, by (20),

$$5^3 \| h_3,\ 5^4 \| h_2,\ 5^5 \| h_1,\ 5^5 \| h_0,$$

so that, by (21),

$$5 \| m.$$

This shows by (23) that

$$5 \| k_3,\ 5 \| k_2,\ 5 \| k_1,\ 5 \nmid k_0,$$

and by (24) that

$$5^8 \| \operatorname{disc}(k_{u,v}).$$

Thus by (27) $\alpha = 2$.

If $5 \nmid u$, then by (16)

$$5 \nmid E,\ 5 \nmid F,\ 5 \nmid G,\ 5 \nmid H.$$

Hence by (20)

$$5 \| h_3,\ 5 \| h_2,\ 5 \| h_1,\ 5 \nmid h_0,$$

so that by (21)

$$5 \nmid m.$$

This shows by (23) that

$$5 \| k_3,\ 5 \| k_2,\ 5 \| k_1,\ 5 \nmid k_0,$$

and, by (24), that

$$5^{20}|\operatorname{disc}(k_{u,v}).$$

Thus, by (27), $\alpha = 0$.

Theorem 2 now follows from (26), (27), (28) and (29). $\square$

We conclude this section with a numerical example to illustrate Theorem 2. We choose $u = 5$, $v = 6$, so that $t = 5/6$ and

$$f_{5/6}(X) = X^5 + \frac{25}{36}X^4 - \frac{2555}{108}X^3 + \frac{36955}{1296}X^2 + \frac{4685}{216}X + 1.$$

MAPLE confirms that

$$\operatorname{Gal}(f_{5/6}) \simeq \mathbf{Z}/5\mathbf{Z}.$$

Now $E = 5^2 \times 11 \times 281$, so that by Theorem 2,

$$f(K) = 5^2 \times 11 \times 281, \quad d(K) = 5^8 \times 11^4 \times 281^4$$

in agreement with PARI.

**4. Numerical examples.** We conclude with six numerical examples.

*Example* 1. $f(X) = X^5 - 110X^3 - 55X^2 + 2310X + 979$. $a_0 = 11 \times 89$, $a_1 = 2 \times 3 \times 5 \times 7 \times 11$, $a_2 = -5 \times 11$, $a_3 = -2 \times 5 \times 11$. $\operatorname{Gal}(f) \simeq \mathbf{Z}/5\mathbf{Z}$, $\operatorname{disc}(f) = 5^{20} \times 11^4$. [MAPLE, PARI] $5^{20} \mid \operatorname{disc}(f)$, $5 \nmid a_0$, so that $\alpha = 0$. Theorem 1 gives $f(K) = 11$, $d(K) = 11^4$, in agreement with PARI.

*Example* 2. $f(X) = X^5 - 25X^3 + 50X^2 - 25$. $a_0 = -5^2$, $a_1 = 0$, $a_2 = 2 \times 5^2$, $a_3 = -5^2$. $\operatorname{Gal}(f) \simeq \mathbf{Z}/5\mathbf{Z}$, $\operatorname{disc}(f) = 5^{12} \times 7^2$. [MAPLE, PARI] $5^{20} \nmid \operatorname{disc}(f)$, $5 \mid a_1$, $5 \mid a_2$, $5 \mid a_3$, so that $\alpha = 2$. Theorem 1 gives $f(K) = 5^2$, $d(K) = 5^8$, in agreement with PARI.

*Example* 3. $f(X) = X^5 - 375X^3 - 3750X^2 - 10000X - 625$. $a_0 = -5^4$, $a_1 = -2^4 \times 5^4$, $a_2 = -2 \times 3 \times 5^4$, $a_3 = -3 \times 5^3$. $\operatorname{Gal}(f) \simeq \mathbf{Z}/5\mathbf{Z}$, $\operatorname{disc}(f) = 5^{20} \times 7^6$ [MAPLE, PARI] $5^{20} \mid \operatorname{disc}(f)$, $5^4 \| a_0$, $5^4 \mid a_1$,

$5^4 \mid a_2$, $5^3 \mid a_3$, so that $\alpha = 2$. Theorem 1 gives $f(K) = 5^2$, $d(K) = 5^8$, in agreement with PARI.

*Example* 4. $f(X) = X^5 - 2483X^3 - 7449X^2 + 3247X - 191$. $a_0 = 191$, $a_1 = 17 \times 191$, $a_2 = -3 \times 13 \times 191$, $a_3 = -13 \times 191$. $\mathrm{Gal}\,(f) \simeq \mathbf{Z}/5\mathbf{Z}$, $\mathrm{disc}\,(f) = 5^{10} \times 41^2 \times 191^4 \times 1039^2$ [MAPLE, PARI] $5^{20} \nmid \mathrm{disc}\,(f)$, $5 \nmid a_1$, so that $\alpha = 0$. Theorem 1 gives $f(K) = 191$, $d(K) = 191^4$, in agreement with PARI.

*Example* 5. $f(X) = X^7 - 609X^5 + 609X^4 + 70847X^3 + 25172X^2 - 1321124X + 2048647$. $a_0 = 29 \times 41 \times 1723$, $a_1 = -2^2 \times 7 \times 29 \times 1627$, $a_2 = 2^2 \times 7 \times 29 \times 31$, $a_3 = 7 \times 29 \times 349$, $a_4 = 3 \times 7 \times 29$, $a_5 = -3 \times 7 \times 29$. $\mathrm{Gal}\,(f) \simeq \mathbf{Z}/7\mathbf{Z}$, $\mathrm{disc}\,(f) = 7^{42} \times 17^2 \times 29^6$ [MAPLE] $7^{42} \mid \mathrm{disc}\,(f)$, $7 \nmid a_0$, so that $\alpha = 0$. Theorem 1 now gives $f(K) = 29$, $d(K) = 29^6$, in agreement with PARI.

*Example* 6. $f(X) = X^{13} - 78X^{11} - 65X^{10} + 2080X^9 + 2457X^8 - 24128X^7 - 27027X^6 + 137683X^5 + 110214X^4 - 376064X^3 - 128206X^2 + 363883X - 12167$. $a_0 = -23^3$, $a_1 = 13 \times 23 \times 2717$, $a_2 = -2 \times 13 \times 4931$, $a_3 = -2^8 \times 13 \times 113$, $a_4 = 2 \times 3^3 \times 13 \times 157$, $a_5 = 7 \times 13 \times 17 \times 89$, $a_6 = -3^3 \times 7 \times 11 \times 13$, $a_7 = -2^6 \times 13 \times 29$, $a_8 = 3^3 \times 7 \times 13$, $a_9 = 2^5 \times 5 \times 13$, $a_{10} = -5 \times 13$, $a_{11} = -2 \times 3 \times 13$. $\mathrm{disc}\,(f) = 13^{24} \times 19^6 \times 23^{10} \times 337^2 \times 823^2 \times 7121^2 \times 21317^2$ [MAPLE] $13^{156} \nmid \mathrm{disc}\,(f)$, $13 \mid a_i$, $i = 1, 2, \dots, 11$, so that $\alpha = 2$. Theorem 1 gives $f(K) = 13^2$, $d(K) = 13^{24}$ in agreement with [**1**].

## REFERENCES

**1.** Vincenzo Acciaro, *Local global methods in number theory*, Ph.D. Thesis, Carleton University, Ottawa, Canada, 1995.

**2.** H. Darmon, *Note on a polynomial of Emma Lehmer*, Math. Comp. **56** (1991), 795–800.

**3.** István Gaál and Michael Pohst, *Power integral bases in a parametric family of totally real cyclic quintics*, Math. Comp. **66** (1997), 1689–1696.

**4.** James G. Huard, Blair K. Spearman and Kenneth S. Williams, *A short proof of the formula for the conductor of an abelian cubic field*, Norske Vid. Selsk. Skr. **2** (1994), 3–7.

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

**6.** Daniel C. Mayer, *Multiplicities of dihedral discriminants*, Math. Comp. **58** (1992), 831–847.

**7.** Wladyslaw Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 2nd ed., Springer-Verlag, New York; PWN-Polish Scientific Publishers, Warsaw, 1990.

**8.** René Schoof and Lawrence C. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. **50** (1988), 543–556.

Department of Mathematics and Statistics, Okanagan University College, Kelowna, BC, Canada V1V 1V7
*E-mail address:* bkspearm@okuc02.okanagan.bc.ca

Centre for Research in Algebra and Number Theory, School of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada K1S 5B6
*E-mail address:* williams@math.carleton.ca