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 \( f(x) \in \mathbb{Z}[x] \) be a defining polynomial for a cyclic extension field \( K \) of the rational number field \( \mathbb{Q} \) with \([K : \mathbb{Q}] = p\). 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 \( \mathbb{Q} \) with \([K : \mathbb{Q}] = p\). 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 \( f(X) = X^p + a_{p-2}X^{p-2} + \cdots + a_1X + a_0 \in \mathbb{Z}[X] \) be such that

\[
\text{Gal}(f) \cong \mathbb{Z}/p\mathbb{Z}
\]

and

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

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 \( f(K) \) of \( K \) is given by

\[
f(K) = p^{\alpha} \prod_{q \equiv 1 \pmod{p}, q | a_i, i=0,1,\ldots,p-2} q,
\]

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.

Copyright \( \odot 2003 \) Rocky Mountain Mathematics Consortium

1101
where $q$ runs through primes, and

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

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 $g(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree $p$ having $\text{Gal}(g) \cong \mathbb{Z}/p\mathbb{Z}$. Let $\theta \in \mathbb{C}$ be a root of $g(X)$ and set $K = \mathbb{Q}(\theta)$. 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 $\mathbb{Q}$, 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 $r \in \mathbb{Z}$ such that

$$(5) \quad \theta \equiv r \pmod{Q}.$$ 

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

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

Hence,

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

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

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

**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,

$$X^p + a_{p-2}X^{p-2} + \cdots + a_1X + a_0$$

$$\equiv X^p - prX^{p-1} + \left(\frac{p}{2}\right)r^2X^{p-2}$$

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

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

so that

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

(b) Now suppose that

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

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 $i = 1, \ldots, t$. As $Q_i$ is a prime ideal, we deduce that $Q_i \mid \theta$ for $i = 1, \ldots, t$, and so $q \mid \theta$. This shows that $\theta/q \in O_K$. The minimal polynomial of $\theta/q$ over $\mathbb{Q}$ 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 $\mathbb{Z}[X]$. Hence we have

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

contradicting (2). Hence $q$ ramifies in $K$. □

**Lemma 3.** If

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

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

$$X^p + a_{p-2}X^{p-2} + \cdots + a_1X + a_0 \equiv X^p - r \pmod{p}$$

and thus

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

which is a contradiction. Hence $p$ does not ramify in $K$. \(\square\)

Lemma 4. If

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

and

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

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 $Q_i, i = 1, \ldots, t$, of $K$. Now

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

$$\equiv \theta^p + a_0^p \equiv (\theta + a_0)^p \pmod{p}$$

so that $Q_i \mid (\theta + a_0)^p$ and thus $Q_i \mid \theta + a_0$ for $i = 1, \ldots, t$. Hence $Q_1Q_2 \cdots Q_t \mid \theta + a_0$ and so $p \mid \theta + a_0$. By conjugation, as $K$ is a normal extension of $\mathbb{Q}$, we deduce that

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

Hence

$$p \mid \theta_i - \theta_j, \quad 1 \leq i < j \leq p,$$
and so
\[ p^{p(p-1)} \mid \prod_{1 \leq i < j \leq p} (\theta_i - \theta_j)^2, \]
that is,
\[ p^{p(p-1)} \mid \text{disc}(f), \]
contradicting \( p^{p(p-1)} \nmid \text{disc}(f) \). This proves that \( p \) ramifies in \( K \).

Lemma 5. If
\[ p^{-1} \| a_0, p^{-1} \mid a_1, p^{p+1-i} \mid a_i, \quad i = 2, \ldots, p-2, \]
then

(a) \( p \) ramifies in \( K \)

and

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

Proof. We define \( b_0, \ldots, b_{p-2} \in \mathbb{Z} \) by
\[ b_0 = a_0/p^{p-1}, b_1 = a_1/p^{p-1}, b_i = a_i/p^{p+1-i}, \quad i = 2, \ldots, p-2. \]
Clearly \( p \nmid b_0 \). We set
\[ h(X) = X^p + pb_1 X^{p-1} + \sum_{i=2}^{p-2} p^2 b_0^{i-1} b_i X^{p-i} + p b_0^{p-1} \in \mathbb{Z}[X]. \]
Then
\[ h(b_0 pX) \]
\[ = b_0^{p-1} p^p X^p + b_0^{p-1} b_1 p^p X^{p-1} + \sum_{i=2}^{p-2} b_0^{p-1} b_i p^{p+2-i} X^{p-i} + p b_0^{p-1} \]
\[ = b_0^{p-1} p^p \left( b_0 p^{p-1} + b_1 \frac{p^{p-1}}{X} + \sum_{i=2}^{p-2} b_i \frac{p^{p+1-i}}{X^i} + \frac{1}{X^p} \right) \]
\[ = b_0^{p-1} p^p f \left( \frac{1}{X} \right). \]
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 $\wp^k \parallel \theta$. Then by conjugation we have $\wp^k \parallel \theta_i$, $i = 1, 2, \ldots, p$. Hence,

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

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

Further,

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

We have

$$\wp^{p+(p-1)^2} \parallel p\theta^{p-1},$$ 

$$\wp^{p+(p+1-i)+(p-1)(i-1)} \parallel ia_i \theta^{i-1}, \quad i = 2, \ldots, p-2,$$

$$\wp^{p(p-1)} \parallel a_1.$$ 

As

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

and

$$p(p + 1 - i) + (p-1)(i-1) = p^2 - i + 1 \geq p^2 - (p-2) + 1 = p^2 - p + 3 > p(p-1),$$

we see that

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

By conjugation we deduce that

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

so that

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

that is,

\[ p^{p(p-1)} \mid \text{disc } (f). \]

This completes the proof of Lemma 5. \[\square\]

**Lemma 6.** If

\[ p^{p(p-1)} \mid \text{disc } (f) \]

and

\[ p^{p-1} | a_0, p^{p-1} | a_1, p^{p+1-i} | a_i, \quad i = 2, \ldots, p - 2, \]

does not hold,

then \( p \) does not ramify in \( K \).

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

\[ \theta \equiv r \pmod{\varphi}. \]

We consider two cases.

**Case (i):** \( r = 0 \). In this case \( \varphi \mid \theta \) so that \( \varphi^k \mid \theta \) 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 \( \mathbb{Q} \) 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 \( \mathbb{Z}[X] \). Hence we have

\[ p^{p-i} \mid a_i, \quad i = 0, 1, \ldots, p - 2, \]

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

Next we define the nonnegative integer \( l \) by \( \varphi^l \mid f'(\theta) \). By conjugation we have \( \varphi^l \mid f'(\theta_i), \quad i = 1, 2, \ldots, p \). Hence

\[ \varphi^{pl} \mid \prod_{i=1}^{p} f'(\theta_i) = \pm \text{disc } (f). \]
But $\wp^{p^2(p-1)} = p^{p(p-1)} \mid \text{disc}(f)$, so we must have $pl \geq p^2(p-1)$, that is, $l \geq p(p-1)$. Hence

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

Now

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

where

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

and

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

Clearly,

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

and

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

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

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

and

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

Thus

(8) $p + (p - 1)k \geq p(p - 1)$

and

(9) $v_\wp(a_{p-i}) + (p - i - 1)k \geq p(p - 1), \quad i = 2, \ldots, p - 1.$
From (8) we deduce that \( k \geq p - 1 \). As \( 1 \leq k \leq p - 1 \), we must have \( k = p - 1 \) so \( \wp^{p-1} \mid \theta \). 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

\[
\wp^{p(p-1)} \mid \theta^p
\]

\[
\wp^{p(i+1)+(p-i)(p-1)} \mid a_{p-i}\theta^{p-i}, \quad i = 2, \ldots, p - 2,
\]

\[
\wp^{p(p-1)+(p-1)} \mid a_1\theta,
\]

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 \( p^{p-1} \mid a_0 \), contradicting the second assumption of the lemma.

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

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

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

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

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, $k = 1, 2, \ldots, p - 1$.

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

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

Suppose that $\wp^i|g'(\alpha)$. By conjugation we have $\wp^i|g'(\alpha_i)$, $i = 1, 2, \ldots, p$. Hence,

$$\wp^p \prod_{i=1}^{p} g'(\alpha_i).$$

Further

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

and

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

$$v_{\wp}(rp(p - 1)\alpha^{p-2}) = p + (p - 2)k,$$

$$v_{\wp}(ib_i\alpha^{i-1}) = v_{\wp}(b_i) + (i - 1)k, \quad i = 1, \ldots, p - 2.$$
Since
\[ v_\varphi(p\alpha^{p-1}), v_\varphi(rp(p-1)\alpha^{p-2}), v_\varphi(ib_i\alpha^{i-1}), \quad i = 1, \ldots, p - 2, \]
are all distinct modulo \( p \), they must all be different. From (10) and (11), we deduce
\[
\left\{ \begin{array}{l}
\varphi^p(p-1) | p\alpha^{p-1}, \\
\varphi^p(p-1) | rp(p-1)\alpha^{p-2}, \\
\varphi^p(p-1) | ib_i\alpha^{i-1}, \quad i = 1, \ldots, p - 2.
\end{array} \right.
\]
From the first of these, we have
\[ p(p-1) \leq p + (p-1)k \]
so that
\[ k \geq \frac{p^2 - 2p}{p - 1}. \]
As \( k \in \mathbb{Z} \) we must have \( k \geq p - 1 \). Since \( k \in \{1, 2, \ldots, p - 1\} \), we deduce that \( k = p - 1 \). Then, from the second divisibility condition in (12), we deduce that
\[ p(p-1) \leq p + (p-2)k = p + (p-2)(p-1) = p^2 - 2p + 2, \]
which is impossible.

In both cases we have been led to a contradiction. Thus \( p \) does not ramify in \( K \). \( \Box \)

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

\[ \prod_{q \equiv 1 \text{ (mod } p) \text{ and } q \text{ ramifies in } K} q = \prod_{q \equiv 1 \text{ (mod } p) \text{ and } q | a_i, i=0,1,...,p-2} q. \]

Finally we treat the prime \( p \). We consider four cases.

(I) \( p^p(p-1) \not| \ \text{disc}(f) \), \( p | a_i, i = 1, \ldots, p-2 \), does not hold,

(II) \( p^p(p-1) \not| \ \text{disc}(f) \), \( p | a_i, i = 1, \ldots, p-2 \), holds,

(III) \( p^p(p-1) | \ \text{disc}(f) \), \( p^{p-1} | a_0, p^{p-1} | a_1, p^{p+1-i} | a_i, i = 2, \ldots, p-2 \), holds,

(IV) \( p^p(p-1) | \ \text{disc}(f) \), \( p^{p-1} | a_0, p^{p-1} | a_1, p^{p+1-i} | a_i, i = 2, \ldots, p-2 \), 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. \( \square \)

We conclude this section by looking at the case \( p = 3 \) in some detail.

Let \( f(X) = X^3 + aX + b \in \mathbb{Z}[X] \) be such that \( \text{Gal}(f) \simeq \mathbb{Z}/3\mathbb{Z} \) and suppose that there does not exist a prime \( q \) such that \( q^2 | a \) and \( q^3 | b \). Here \( \text{disc}(f) = -4a^3 - 27b^2 \). As \( \text{Gal}(f) \simeq \mathbb{Z}/3\mathbb{Z} \), we have

\[ -4a^3 - 27b^2 = c^2 \]

for some positive integer \( c \). Since \( 3^2 | a, 3^3 | b \) 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)’ \( 3^6 \nmid \text{disc}(f), 3 \nmid a \);
(ii) is equivalent to
   
   \[
   (ii)' \ 3^6 \mid \text{disc}(f), \ 3 \mid a;
   \]

(iii) is equivalent to

   \[
   (iii)' \ 3^6 \mid \text{disc}(f), \ 3\|a;
   \]

(iv) is equivalent to

   \[
   (iv)' \ 3^6 \mid \text{disc}(f), \ 3^2 \mid a, \ 3^2\|b.
   \]

By Theorem 1, we have

   \[
   f(K) = 3^\alpha \prod_{q \equiv 1 \pmod{3}} q,
   \]

where \( q \) runs through primes, and

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

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 \( t \in \mathbb{Q} \) 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

   \[
   \begin{align*}
   a_4(t) &= t^2, \\
   a_3(t) &= -(2t^3 + 6t^2 + 10t + 10), \\
   a_2(t) &= t^4 + 5t^3 + 11t^2 + 15t + 5, \\
   a_1(t) &= t^3 + 4t^2 + 10t + 10, \\
   a_0(t) &= 1.
   \end{align*}
   \]

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

   \[
   t = u/v, \ u \in \mathbb{Z}, \ v \in \mathbb{Z}, \quad (u, v) = 1, \ v > 0.
   \]
It is convenient to define

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

Let \( \theta \) be a root of \( f_t(x) \) and set \( K = \mathbb{Q}(\theta) \). 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

\[
f(K) = 5^\alpha \prod_{\substack{q \equiv 1 \pmod{5} \\ q | E \\ v_q(E) \neq 0 \pmod{5}}} q,
\]

where \( q \) runs through primes, and

\[
\alpha = \begin{cases} 
0 & \text{if } 5 \nmid u, \\
2 & \text{if } 5 | u.
\end{cases}
\]

We remark that when \( t \in \mathbb{Z} \), 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

\[
g_t(X) = 5^5 f_t((X - t^2)/5) = X^5 + g_3X^3 + g_2X^2 + g_1X + g_0,
\]
where
\begin{align*}
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{align*}

Next we set
\begin{align*}
(19) \quad h_{u,v}(X) &= v^{10}g_{u/v}(X/v^2) = X^5 + h_3X^3 + h_2X^2 + h_1X + h_0,
\end{align*}
where
\begin{align*}
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^3v^4 - 125uv^5 + 125v^6);
\end{align*}
so that by (16) we have
\begin{align*}
(20) \quad h_3 &= -10E, \quad h_2 = 5EF, \quad h_1 = -5EG, \quad h_0 = EH.
\end{align*}

Next let \( m \) denote the largest positive integer such that
\begin{align*}
(21) \quad m^2|h_3, \quad m^3|h_2, \quad m^4|h_1, \quad m^5|h_0,
\end{align*}
and set

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

where

\[(23) \quad k_3 = h_3/m^2, \quad k_2 = h_2/m^3, \quad k_1 = h_1/m^4, \quad k_0 = h_0/m^5.\]

Appealing to MAPLE, we find

\[(24) \quad \text{disc}(k_{u,v}) = 5^{20}E^4I^2v^{18}/m^{20}\]

and

\[(25) \quad EJ - HL = 5^5v^9.\]

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

\[(26) \quad f(K) = 5^\alpha \prod_{q \equiv 1 \pmod{5}} q, \quad q|k_0, q|k_1, q|k_2, q|k_3\]

where \(q\) runs through primes, and

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

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

\[q \mid E, \quad v_q(E) \not\equiv 0 \pmod{5}.\]
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
\[ q^{5w} \parallel h_3, \ q^{5w} \mid h_2, \ q^{5w} \mid h_1, \ q^{5w} \parallel h_0, \]
so that by (21) we have
\[ q^w \parallel m. \]
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
\[ q \equiv 1 \pmod{5}, \ q \mid E, \ v_q(E) \not\equiv 0 \pmod{5}. \]
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 \( q^{5z+r} \parallel E \), where \( z \) is a nonnegative integer and \( r = 1, 2, 3, 4 \). Thus by (20) we have
\[ q^{5z+r} \parallel h_3, \ q^{5z+r} \mid h_2, \ q^{5z+r} \mid h_1, \ q^{5z+r} \parallel h_0. \]
This shows by (21) that
\[ q^z \parallel m \]
so that by (23)
\[ q^{3z+r} \parallel k_3, \ q^{3z+r} \mid k_2, \ q^{3z+r} \mid k_1, \ q^r \parallel k_0, \]
proving
\[ q \mid k_3, \ q \mid k_2, \ q \mid k_1, \ q \mid k_0. \]
We have shown that

\[(28) \prod_{q \equiv 1 \pmod{5}, q | k_0, q | k_1, q | k_2, q | k_3} q = \prod_{q \equiv 1 \pmod{5}, q | E, q | E} q.\]

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

\[(29) \alpha = \begin{cases} 0 & \text{if } 5 \nmid u, \\ 2 & \text{if } 5 | u. \end{cases}\]

If \(5 | u\), 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

\[5^8 || \text{disc}(k_{u,v}).\]

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
\[ 5^{20} | \text{disc}(k_{u,v}). \]
Thus, by (27), \( \alpha = 0 \).

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

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
\[
\text{Gal}(f_{5/6}) \simeq \mathbb{Z}/5\mathbb{Z}.
\]
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. \( f(X) = X^5 - 110X^3 - 55X^2 + 2310X + 979 \). \( a_0 = 11 \times 89 \), \( a_1 = 2 \times 3 \times 5 \times 7 \times 11 \), \( a_2 = -5 \times 11 \), \( a_3 = -2 \times 5 \times 11 \). \( \text{Gal}(f) \simeq \mathbb{Z}/5\mathbb{Z} \), \( \text{disc}(f) = 5^{20} \times 11^4 \). [MAPLE, PARI] \( 5^{20} | \text{disc}(f) \), \( 5 \nmid a_0 \), so that \( \alpha = 0 \). Theorem 1 gives \( f(K) = 11 \), \( d(K) = 11^4 \), in agreement with PARI.

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

Example 3. \( f(X) = X^5 - 375X^3 - 3750X^2 - 10000X - 625 \). \( a_0 = -5^4 \), \( a_1 = -2^4 \times 5^4 \), \( a_2 = -2 \times 3 \times 5^4 \), \( a_3 = -3 \times 5^3 \). \( \text{Gal}(f) \simeq \mathbb{Z}/5\mathbb{Z} \), \( \text{disc}(f) = 5^{20} \times 7^6 \) [MAPLE, PARI] \( 5^{20} \mid \text{disc}(f) \), \( 5^4 \mid a_0 \), \( 5^4 \mid a_1 \),
$5^4 \mid a_2, 5^3 \mid a_3$, so that $\alpha = 2$. Theorem 1 gives $f(K) = 5^2$, $d(K) = 5^8$, in agreement with PARI.

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

**Example 5.** $f(X) = X^7 - 609X^5 + 609X^4 + 70847X^3 + 25172X^2 - 1321124X + 2048647$. $a_0 = 29 \times 41 \times 1723$, $a_1 = -2^2 \times 7 \times 29 \times 1627$, $a_2 = 2^2 \times 7 \times 29 \times 31$, $a_3 = 7 \times 29 \times 349$, $a_4 = 3 \times 7 \times 29$, $a_5 = -3 \times 7 \times 29$. $\text{Gal}(f) \simeq \mathbb{Z}/7\mathbb{Z}$, $\text{disc}(f) = 7^{12} \times 17^2 \times 29^6$ [MAPLE] $7^{12} \nmid \text{disc}(f)$, $\nmid a_0$, so that $\alpha = 0$. Theorem 1 now gives $f(K) = 29$, $d(K) = 29^6$, in agreement with PARI.

**Example 6.** $f(X) = X^{13} - 78X^{11} - 65X^{10} + 2080X^9 + 2457X^8 - 24128X^7 - 27027X^6 + 137683X^5 + 110214X^4 - 376064X^3 - 128206X^2 + 363883X - 12167$. $a_0 = -23^3$, $a_1 = 13 \times 23 \times 2717$, $a_2 = -2 \times 13 \times 4931$, $a_3 = -2^8 \times 13 \times 113$, $a_4 = 2 \times 3^3 \times 13 \times 157$, $a_5 = 7 \times 13 \times 17 \times 89$, $a_6 = -3^3 \times 7 \times 11 \times 13$, $a_7 = -2^6 \times 13 \times 29$, $a_8 = 3^3 \times 7 \times 13$, $a_9 = 2^5 \times 5 \times 13$, $a_{10} = -5 \times 13$, $a_{11} = -2 \times 3 \times 13$. $\text{disc}(f) = 13^{24} \times 196^6 \times 23^{10} \times 337^2 \times 832^2 \times 7121^2 \times 21317^2$ [MAPLE] $13^{156} \nmid \text{disc}(f)$, $13 \mid a_i$, $i = 1, 2, \ldots, 11$, so that $\alpha = 2$. Theorem 1 gives $f(K) = 13^2$, $d(K) = 13^{24}$ in agreement with [1].

**REFERENCES**


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