Canad. Math. Bull. Vol. **45** (1), 2002 pp. 138–153

The Discriminant of a Dihedral Quintic Field Defined by a Trinomial $X^5 + aX + b$

Blair K. Spearman and Kenneth S. Williams

Abstract. Let $X^5 + aX + b \in Z[X]$ have Galois group D_5. Let θ be a root of $X^5 + aX + b$. An explicit formula is given for the discriminant of $Q(\theta)$.

1 Introduction

Let $f(X) = X^5 + aX + b \in Z[X]$ have Galois group D_5 (the dihedral group of order 10). Let θ be a root of $f(X)$. Set $K = Q(\theta)$. If p is a prime such that $p^4|a$ and $p^5|b$ then θ/p is a root of $X^5 + (a/p^4)X + (b/p^5) \in Z[X]$ and $K = Q(\theta/p)$. Hence we may assume that

(1.1) there does not exist a prime p such that $p^4|a$ and $p^5|b$.

Our objective in this paper is to give an explicit formula for the discriminant $d(K)$ of K in terms of a and b. We prove

Theorem *With the notation of the first paragraph*

$$d(K) = 2^\alpha 5^\beta \prod_{\substack{p\neq 2,5 \\ v_p(b)>v_p(a)=2}} p^2 \prod_{\substack{p\neq 2,5 \\ 1\leq v_p(b)\leq v_p(a)}} p^4,$$

where

$$\alpha = \begin{cases} 4, & \text{if } 2^2 \parallel a, \\ 6, & \text{if } 2 \nmid a, \end{cases}$$

and

$$\beta = \begin{cases} 0, & \text{if } 5 \nmid a, \\ 2, & \text{if } 5^2 \parallel a,\ 5^3|b, \\ 6, & \text{if } 5 \parallel a,\ 5 \nmid b \text{ or } 5^2 \parallel a,\ 5^2 \parallel b, \\ 8, & \text{if } 5^4 \parallel a,\ 5^4 \parallel b. \end{cases}$$

Here and throughout p denotes a prime and if c is a nonzero integer with $p^m|c$, $p^{m+1} \nmid c$ we write $p^m \parallel c$ or $v_p(c) = m$.

Received by the editors January 20, 2000.
The first author's research was supported by a grant from the Natural Sciences and Engineering Research Council of Canada. The second author's research was supported by Natural Sciences and Engineering Research Council of Canada grant A-7233.
AMS subject classification: 11R21, 11R29.
Keywords: dihedral quintic field, trinomial, discriminant.

The starting point of the proof of our theorem is a representation of a and b given by Roland, Yui, and Zagier [4] (see Proposition 2.1). Then in Section 3 we determine the 2-part of $d(K)$, in Section 4 the 5-part of $d(K)$, and in Section 5 the p-part of $d(K)$ for a prime $p \neq 2, 5$. The proof of the Theorem is completed in Section 6. In Section 7 two corollaries to the Theorem are given. In Section 8 a number of numerical examples illustrating the Theorem are given.

2 Representation of a and b

Our first proposition is a formula of Roland, Yui, and Zagier [4, formula (2)]. We remark that their proof needs a slight modification as their change of variable $\lambda = 5(u+1)/(u-1)$ does not yield a rational u when $\lambda = 5$.

Proposition 2.1 *There exist coprime integers m and n, and integers $i, j = 0$ or 1, such that*

$$a = 2^{2-4i} 5^{1-4j} d_2 (m^2 - mn - n^2) E^2 F,$$

$$b = 2^{4-5i} 5^{-5j} d_1 (2m - n)(m + 2n) E^3 F,$$

where d_1^2 is the largest square dividing $m^2 + n^2$, d_2^5 is the largest fifth power dividing $m^2 + mn - n^2$, and

$$E = (m^2 + n^2)/d_1^2, \quad F = (m^2 + mn - n^2)/d_2^5.$$

Roland, Yui, and Zagier [4] do not give the values of i and j explicitly in terms of m and n. As we shall need them we determine i and j explicitly in the next two propositions. We recall that $(m, n) = 1$ so that $m \equiv n \equiv 0 \pmod 2$ does not occur.

Proposition 2.2

$$i = 1 \iff m \equiv n \equiv 1 \pmod 2 \iff 2 \nmid a, 2^2 \parallel b$$

$$i = 0 \iff m \equiv n + 1 \pmod 2 \iff 2^2 \parallel a, 2^5 | b.$$

Proof As $(m, n) = 1$ we have

$$v_2(m^2 + n^2) = \begin{cases} 1, & \text{if } m \equiv n \equiv 1 \pmod 2, \\ 0, & \text{if } m \equiv n + 1 \pmod 2, \end{cases}$$

$$v_2(d_1) = 0,$$

$$v_2(E) = \begin{cases} 1, & \text{if } m \equiv n \equiv 1 \pmod 2, \\ 0, & \text{if } m \equiv n + 1 \pmod 2, \end{cases}$$

$$v_2(m^2 - mn - n^2) = 0,$$

$$v_2(m^2 + mn - n^2) = v_2(d_2) = v_2(F) = 0,$$

$$v_2\big((2m - n)(m + 2n)\big) = \begin{cases} 0, & \text{if } m \equiv n \equiv 1 \pmod 2, \\ \geq 1, & \text{if } m \equiv n + 1 \pmod 2, \end{cases}$$

https://doi.org/10.4153/CMB-2002-017-8 Published online by Cambridge University Press

so that by Proposition 2.1, we see that

$$v_2(a) = \begin{cases} 4 - 4i, & \text{if } m \equiv n \equiv 1 \pmod 2, \\ 2 - 4i, & \text{if } m \equiv n + 1 \pmod 2, \end{cases}$$

and

$$v_2(b) = \begin{cases} 7 - 5i, & \text{if } m \equiv n \equiv 1 \pmod 2, \\ \geq 5 - 5i, & \text{if } m \equiv n + 1 \pmod 2. \end{cases}$$

If $m \equiv n \equiv 1 \pmod 2$ then $i = 1$ otherwise $i = 0$ and $v_2(a) = 4$, $v_2(b) = 7$, which contradicts (1.1). In this case $v_2(a) = 0$ and $v_2(b) = 2$. If $m \equiv n + 1 \pmod 2$ then $2 - 4i = v_2(a) \geq 0$ so that $i = 0$. In this case $v_2(a) = 2$ and $v_2(b) \geq 5$. ■

Proposition 2.2 shows that either $2 \nmid a$ or $2^2 \parallel a$.

Proposition 2.3

$j = 0$, *if* $m \not\equiv 2n, 3n \pmod 5$
or
$m \equiv 3n \pmod 5$, $E \not\equiv 0 \pmod 5$
or
$m \equiv 2n \pmod 5$, $m \not\equiv 57n \pmod{125}$
or
$m \equiv 2n \pmod 5$, $m \equiv 57n \pmod{125}$, $E \not\equiv 0 \pmod 5$,

$j = 1$, *if* $m \equiv 3n \pmod 5$, $E \equiv 0 \pmod 5$
or
$m \equiv 2n \pmod 5$, $m \equiv 57n \pmod{125}$, $E \equiv 0 \pmod 5$.

Proof As $(m, n) = 1$ we have

$$v_5(m^2 + mn - n^2) = v_5\big((2m + n)^2 - 5n^2\big) = \begin{cases} 0, & \text{if } m \not\equiv 2n \pmod 5, \\ 1, & \text{if } m \equiv 2n \pmod 5, \end{cases}$$

so that

$$v_5(d_2) = 0$$

and

$$v_5(F) = \begin{cases} 0, & \text{if } m \not\equiv 2n \pmod 5, \\ 1, & \text{if } m \equiv 2n \pmod 5. \end{cases}$$

Similarly

$$v_5(m^2 - mn - n^2) = v_5\big((2m - n)^2 - 5n^2\big) = \begin{cases} 0, & \text{if } m \not\equiv 3n \pmod 5, \\ 1, & \text{if } m \equiv 3n \pmod 5. \end{cases}$$

https://doi.org/10.4153/CMB-2002-017-8 Published online by Cambridge University Press

Next, as E is squarefree, we have

$$v_5(E) = \begin{cases} 0, & \text{if } E \not\equiv 0 \pmod 5, \\ 1, & \text{if } E \equiv 0 \pmod 5, \end{cases}$$

and a simple calculation shows that

$$v_5(d_1) = \begin{cases} 0, & \text{if } m \not\equiv 2n, 3n \pmod 5 \\ & \qquad \text{or} \\ & m \equiv 2n \pmod 5,\, m \not\equiv 57n \pmod{125},\, E \equiv 0 \pmod 5, \\ \geq 0, & \text{if } m \equiv 3n \pmod 5,\, E \equiv 0 \pmod 5, \\ & \\ 1, & \text{if } m \equiv 2n \pmod 5,\, m \not\equiv 57n \pmod{125},\, E \not\equiv 0 \pmod 5, \\ \geq 1, & \text{if } m \equiv 2n \pmod 5,\, m \equiv 57n \pmod{125},\, E \equiv 0 \pmod 5 \\ & \qquad \text{or} \\ & m \equiv 3n \pmod 5,\, E \not\equiv 0 \pmod 5, \\ \geq 2, & \text{if } m \equiv 2n \pmod 5,\, m \equiv 57n \pmod{125},\, E \not\equiv 0 \pmod 5. \end{cases}$$

Also

$$v_5\big((2m-n)(m+2n)\big) = \begin{cases} 0, & \text{if } m \not\equiv 3n \pmod 5, \\ \geq 2, & \text{if } m \equiv 3n \pmod 5. \end{cases}$$

We consider the following seven mutually exclusive and exhaustive cases.

(i) $m \not\equiv 2n, 3n \pmod 5$. From Proposition 2.1 and the above remarks, we have

$$v_5(a) = 1 - 4j, \quad v_5(b) = -5j.$$

As $v_5(b) \geq 0$ and $j = 0$ or 1 we must have $j = 0$.

(ii) $m \equiv 3n \pmod 5$, $E \equiv 0 \pmod 5$. Here

$$v_5(a) = 4 - 4j, \quad v_5(b) \geq 5 - 5j.$$

If $j = 0$ then $v_5(a) = 4$, $v_5(b) \geq 5$, contradicting (1.1). Hence $j = 1$.

(iii) $m \equiv 3n \pmod 5$, $E \not\equiv 0 \pmod 5$. Here

$$v_5(a) = 2 - 4j, \quad v_5(b) \geq 3 - 5j,$$

so that $j = 0$.

(iv) $m \equiv 2n \pmod 5$, $m \equiv 57n \pmod{125}$, $E \equiv 0 \pmod 5$. Here

$$v_5(a) = 4 - 4j, \quad v_5(b) \geq 5 - 5j.$$

If $j = 0$ then $v_5(a) = 4$, $v_5(b) \geq 5$, contradicting (1.1). Hence $j = 1$.

https://doi.org/10.4153/CMB-2002-017-8 Published online by Cambridge University Press

(v) $m \equiv 2n \pmod 5$, $m \equiv 57n \pmod{125}$, $E \not\equiv 0 \pmod 5$. Here

$$v_5(a) = 2 - 4j, \quad v_5(b) \geq 3 - 5j,$$

so that $j = 0$.

(vi) $m \equiv 2n \pmod 5$, $m \not\equiv 57n \pmod{125}$, $E \equiv 0 \pmod 5$. Here

$$v_5(a) = 4 - 4j, \quad v_5(b) = 4 - 5j,$$

so that $j = 0$.

(vii) $m \equiv 2n \pmod 5$, $m \not\equiv 57n \pmod{125}$, $E \not\equiv 0 \pmod 5$. Here

$$v_5(a) = 2 - 4j, \quad v_5(b) = 2 - 5j,$$

so that $j = 0$. ■

In the course of the proof of Proposition 2.3 we showed the following result.

Proposition 2.4

$$5 \nmid a \iff m \equiv 3n \pmod 5, E \equiv 0 \pmod 5 \text{ or } m \equiv 2n \pmod 5, m \equiv 57n \pmod{125}, E \equiv 0 \pmod 5,$$

$$5 \parallel a, 5 \nmid b \iff m \not\equiv 2n, 3n \pmod 5,$$

$$5^2 \parallel a, 5^2 \parallel b \iff m \equiv 2n \pmod 5, m \not\equiv 57n \pmod{125}, E \not\equiv 0 \pmod 5,$$

$$5^2 \parallel a, 5^3 \mid b \iff m \equiv 3n \pmod 5, E \not\equiv 0 \pmod 5 \text{ or } m \equiv 2n \pmod 5, m \equiv 57n \pmod{125}, E \not\equiv 0 \pmod 5,$$

$$5^4 \parallel a, 5^4 \parallel b \iff m \equiv 2n \pmod 5, m \not\equiv 57n \pmod{125}, E \equiv 0 \pmod 5.$$

We denote by M the splitting field of $f(X)$ and by k the unique quadratic subfield of M. From [4, p. 139] we know that

$$k = Q\left(\sqrt{-5(m^2+n^2)}\right) = Q(\sqrt{-5E}).$$

3 The 2-part of $d(K)$

By Proposition 2.2 we know that either $2 \nmid a$ or $2^2 \parallel a$. We prove

Proposition 3.1

$$2^6 \parallel d(K) \iff 2 \nmid a,$$

$$2^4 \parallel d(K) \iff 2^2 \parallel a.$$

https://doi.org/10.4153/CMB-2002-017-8 Published online by Cambridge University Press

Proof By a result of Roland, Yui, and Zagier [4, p. 139], we have

$$v_2\big(d(K)\big) = 2v_2\big(d(k)\big).$$

If $2 \nmid a$ then, by Proposition 2.2, m and n are both odd so that

$$v_2\big(d(k)\big) = v_2\Big(d\Big(Q\big(\sqrt{-5(m^2+n^2)}\big)\Big)\Big) = 3$$

and

$$v_2\big(d(K)\big) = 6.$$

If $2^2 \parallel a$ then, by Proposition 2.2, m and n are of opposite parity so that

$$v_2\big(d(k)\big) = v_2\Big(d\Big(Q\big(\sqrt{-5(m^2+n^2)}\big)\Big)\Big) = 2$$

and

$$v_2\big(d(K)\big) = 4. \qquad \blacksquare$$

4 The 5-Part of $d(K)$

From Proposition 2.4 we know that only the following possibilities can occur:

$$\begin{array}{ll} \multicolumn{2}{c}{5 \nmid a,} \\ 5 \parallel a, & 5 \nmid b, \\ 5^2 \parallel a, & 5^2 \parallel b, \\ 5^2 \parallel a, & 5^3 \mid b, \\ 5^4 \parallel a, & 5^4 \parallel b. \end{array} \tag{4.1}$$

We determine the power of 5 in $d(K)$ in each of these five cases in the following four propositions.

Proposition 4.1 $5|d(K) \iff 5|a$.

Proof First suppose that $5|d(K)$. We have $5|d(K) \implies 5|\operatorname{disc}\big(f(X)\big) \implies 5|4^4a^5 + 5^5b^4 \implies 5|a$.

Now suppose that $5|a$. We consider two cases according as $5|b$ or $5 \nmid b$.

Case (i): $5|b$. Suppose that $5 \nmid d(K)$. Then $\langle 5 \rangle = P_1 \cdots P_t$ for distinct prime ideals $P_1, \ldots, P_t$ of O_K with $1 \le t \le 5$. Since $a \in P_i$ and $b \in P_i$ for $1 \le i \le t$, we have $\theta^5 = -a\theta - b \in P_i$ and therefore $\theta \in P_i$, $1 \le i \le t$. Hence

$$\langle \theta \rangle = P_1 \cdots P_t Q$$

https://doi.org/10.4153/CMB-2002-017-8 Published online by Cambridge University Press

for some ideal Q in O_K. Hence $5|\theta$ and so $\theta = 5\mu$ for some $\mu \in O_K$. Then

$$\mu^5 + (a/5^4)\mu + (b/5^5) = f(\theta)/5^5 = 0.$$

Since $\mu \in O_K$, $a/5^4 \in Z$ and $b/5^5 \in Z$. This contradicts (1). Hence $5|d(K)$.

Case (ii): $5 \nmid b$. Suppose $5 \nmid d(K)$. We have

$$\begin{aligned} g(y) = f(y-b) &= (y-b)^5 + a(y-b) + b \\ &= y^5 - 5by^4 + 10b^2y^3 - 10b^3y^2 + (5b^4+a)y - (b^5+ab-b). \end{aligned}$$

As $5 \nmid d(K)$, we have $\langle 5 \rangle = P_1 \cdots P_t$, where $P_1, \ldots, P_t$ are t $(1 \leq t \leq 5)$ distinct prime ideals in O_K. Let $\gamma = \theta + b$ so that $\gamma \in O_K$ is a root of $g(y)$. For $1 \leq i \leq t$ we have $5 \in P_i$ so that $5b^4 + a \in P_i$ and $b^5 + ab - b \in P_i$. Thus

$$\gamma^5 = 5b\gamma^4 - 10b^2\gamma^3 + 10b^3\gamma^2 - (5b^4+a)\gamma + (b^5+ab-b) \in P_i$$

and so $\gamma \in P_i$ $(1 \leq i \leq t)$. Hence $P_1 \cdots P_t | \langle \gamma \rangle$ and so $5|\gamma$, say $\gamma = 5\mu$ with $\mu \in O_K$ and

$$\mu^5 - b\mu^4 + \frac{2b^2}{5}\mu^3 - \frac{2b^3}{5^2}\mu^2 + \frac{(5b^4+a)}{5^4}\mu - \frac{(b^5+ab-b)}{5^5} = 0.$$

Since $\mu \in O_K$ we must have $2b^2/5 \in Z$. This contradicts that $5 \nmid b$. Hence $5|d(K)$. ∎

Proposition 4.2 $5^2 \parallel d(K) \Longleftrightarrow 5^2 \parallel a$, $5^3|b$.

Proof Suppose that $5^2 \parallel d(K)$. Then, by [1, Theorem 4.2.6 (ii)], 5 ramifies in k but not in M/k. Hence, by [1, Lemma 4.2.2], we have

$$\langle 5 \rangle = P_1 P_2^2 P_3^2$$

for distinct prime ideals of O_K. By Proposition 4.1 we have $5|a$. We consider two cases according as $5 \nmid b$ or $5|b$.

Case (i): $5 \nmid b$. Since $4^4a^5 + 5^5b^4$ is a perfect square we have $5 \parallel a$. We consider $g(y) = f(y-b)$ whose root $\gamma = \theta + b$ is such that $Q(\gamma) = Q(\theta) = K$ and

$$\gamma^5 - 5b\gamma^4 + 10b^2\gamma^3 - 10b^3\gamma^2 + (5b^4+a)\gamma - (b^5+ab-b) = 0. \tag{4.2}$$

Since 5 divides $-5b$, $10b^2$, $-10b^3$, $5b^4 + a$, and $b^5 + ab - b$, we have $5|\gamma^5$ so that $P_1P_2P_3|\langle \gamma \rangle$. If $5|\gamma$ then $\gamma = 5\mu$ where $\mu \in O_K$ and

$$\mu^5 - b\mu^4 + \frac{2b^2}{5}\mu^3 - \frac{2b^3}{5^2}\mu^2 + \frac{(5b^4+a)}{5^4}\mu - \frac{(b^5+ab-b)}{5^5} = 0.$$

Thus $2b^2/5 \in Z$, contradicting $5 \nmid b$. Hence $5 \nmid \gamma$ and so not both of P_2^2 and P_3^2 can divide γ. Without loss of generality we may suppose that $P_2^2 \nmid \langle\gamma\rangle$. Now $N_{K/Q}(P_1P_2P_3)|N_{K/Q}(\langle\gamma\rangle)$ so that $5^3|b^5 + ab - b$ and thus $v_{P_2}(b^5 + ab - b) \geq 6$. Also

$$v_{P_2}(\gamma^5) = 5, \quad v_{P_2}(5b\gamma^4) = 6, \quad v_{P_2}(10b^2\gamma^3) = 5, \quad v_{P_2}(10b^3\gamma^2) = 4,$$

and

$$v_{P_2}\big((5b^4 + a)\gamma\big) = 2t + 1$$

for some $t \in Z$ with $t \geq 1$. This clearly contradicts (4.2).

Case (ii): $5 \mid b$. From $\theta^5 + a\theta + b = 0$ we see that $5 \nmid \theta^5$ so that $P_1P_2P_3|\langle\theta\rangle$. Now $N_{K/Q}(P_1P_2P_3) \mid N_{K/Q}(\langle\theta\rangle)$ so that $5^3 \mid b$. Since $4^4a^5 + 5^5b^4$ is a perfect square, we must have in view of (4.1) either $5^2 \parallel a$ or $5^4 \parallel a$, $5^4 \parallel b$. The latter case implies that $5^4 \mid d(K)$, see [3, question 28(c), p. 90], contradicting $5^2 \parallel d(K)$. Thus we must have $5^2 \parallel a$, $5^3 \mid b$.

Now suppose that $5^2 \parallel a$, $5^3 \mid b$. We show that $5^2 \parallel d(K)$. By Proposition 2.4 we have $E \not\equiv 0 \pmod 5$. Hence 5 ramifies in $k = Q(\sqrt{-5E})$, so that $\langle 5\rangle = P^2$ for some prime ideal P in O_k. We show next that P is unramified in M/k. Set $\phi = E\theta/\sqrt{-5E}$. Clearly $\phi \in M$ and satisfies

$$\phi^5 + \frac{aE^2}{25}\phi - \frac{bE^2}{125}\sqrt{-5E} = 0.$$

Since

$$X^5 + \frac{aE^2}{25}X - \frac{bE^2}{125}\sqrt{-5E} \in O_k[X],$$

any prime ideal of O_k ramifying in O_M must divide the discriminant

$$4^4\left(\frac{aE^2}{25}\right)^5 + 5^5\left(\frac{-bE^2\sqrt{-5E}}{125}\right)^4$$

of this polynomial. As $5^2 \parallel a$ and $5 \nmid E$ we see that P does not divide this discriminant and so is unramified in O_M. Then, by [1, Theorem 4.2.6 (iii)], we must have $v_5\big(d(K)\big) = 2$. ∎

Proposition 4.3 $5^8 \parallel d(K) \iff 5^4 \parallel a$, $5^4 \parallel b$.

Proof We assume first that $5^8 \parallel d(K)$. By [1, Theorem 4.2.6 (iii)] either 5 is ramified in M/k but not in k or is totally ramified in M. In either case we have $\langle 5\rangle = P^5$ for some prime ideal P of O_K with $N_{K/Q}(P) = 5$. By Proposition 4.1 we have $5|a$. We consider two cases according as $5 \nmid b$ or $5|b$.

Case (i): $5 \nmid b$. As $4^4a^5 + 5^5b^4$ is a perfect square we have $5 \parallel a$. We set $g(y) = f(y - b)$ and $\phi = \theta + b$ so that $g(\phi) = 0$ and $Q(\phi) = Q(\theta) = K$. Then

$$\phi^5 - 5b\phi^4 + 10b^2\phi^3 - 10b^3\phi^2 + (5b^4 + a)\phi - (b^5 + ab - b) = 0. \tag{4.3}$$

https://doi.org/10.4153/CMB-2002-017-8 Published online by Cambridge University Press

Clearly $5b$, $10b^2$, $10b^3$, $5b^4 + a$ and $b^5 + ab - b$ are all divisible by 5, so that $5|\phi^5$ and $P|\langle\phi\rangle$. Suppose that $P^5|\langle\phi\rangle$. Then $5|\phi$ and we can write $\phi = 5\mu$, where $\mu \in O_K$, and

$$\mu^5 - b\mu^4 + \frac{2b^2}{5}\mu^3 - \frac{2b^3}{5^2}\mu^2 + \frac{(5b^4 + a)}{5^4}\mu - \frac{(b^5 + ab - b)}{5^5} = 0.$$

Thus $2b^2/5 \in Z$, contradicting $5 \nmid b$. Hence $P^t \parallel \langle\phi\rangle$, where $1 \le t \le 4$. Thus $5^t \parallel N_{K/Q}(\langle\phi\rangle) = \pm(b^5 + ab - b)$, so that

$$\nu_P(b^5 + ab - b) = 5t.$$

Further

$$\begin{aligned} \nu_P\big((5b^4 + a)\phi\big) &= 5l + t, \quad l \in Z^+, \\ \nu_P(10b^3\phi^2) &= 5 + 2t, \\ \nu_P(10b^2\phi^3) &= 5 + 3t, \\ \nu_P(5b\phi^4) &= 5 + 4t, \\ \nu_P(\phi^5) &= 5t. \end{aligned}$$

The equation (4.3) implies that there are two values among $5t, 5l+t, 5+2t$ equal and minimal. This is not the case if $t = 2, 3$ or 4 since

$$\begin{aligned} \{5t, 5l + t, 5 + 2t\} &= \{10, 7 \text{ or } \ge 12, 9, 10\}, \quad \text{if } t = 2, \\ &= \{15, 8 \text{ or } \ge 13, 11, 15\}, \quad \text{if } t = 3, \\ &= \{20, 9 \text{ or } \ge 14, 13, 20\}, \quad \text{if } t = 4. \end{aligned}$$

Hence $t = 1$ and $5 \parallel b^5 + ab - b$. As $5^8 \mid d(K)$ we have $5^8 \mid 4^4a^5 + 5^5b^4$ so that

$$4^4\Big(\frac{a}{5}\Big)^5 + b^4 \equiv 0 \pmod{5^3}.$$

Taking this congruence modulo 5, we see that $a/5 \equiv -1 \pmod 5$, so that there is an integer z such that $a = 25z - 5$. Hence

$$\begin{aligned} b^4 + a - 1 &\equiv -4^4\Big(\frac{a}{5}\Big)^5 + a - 1 \pmod{5^2} \\ &\equiv -4^4(5z - 1)^5 + (25z - 6) \pmod{5^2} \\ &\equiv 6 - 6 \equiv 0 \pmod{5^2} \end{aligned}$$

and thus $5^2 \mid b^5 + ab - b$, contradicting $5 \parallel b^5 + ab - b$. Thus case (i) cannot occur.

Case (ii): *$5 \mid b$.* As $5 \mid a$ and $5 \mid b$, by (4.1), we have $5^2 \parallel a$, $5^2 \mid b$ or $5^4 \parallel a$, $5^4 \parallel b$. If $5^2 \parallel a$, $5^3 \mid b$, by Proposition 4.2, we have $5^2 \parallel d(K)$, contradicting $5^8 \parallel d(K)$. If

$5^2 \parallel a$, $5^2 \parallel b$, then $P^{10} \parallel \langle a\rangle$, $P^{10} \parallel \langle b\rangle$, and so from $\theta^5 + a\theta + b = 0$, we see that $P^2 \parallel \langle\theta\rangle$. Thus $1, \theta, \theta^2, \theta^3/5$ and $\theta^4/5 \in O_K$, and their discriminant satisfies

$$\begin{aligned} v_5\big(\operatorname{disc}(1,\theta,\theta^2,\theta^3/5,\theta^4/5)\big) &= v_5\big(\operatorname{disc}(1,\theta,\theta^2,\theta^3,\theta^4)\big) - 4 \\ &= v_5(4^4a^5 + 5^5b^4) - 4 = 10 - 4 = 6, \end{aligned}$$

contradicting that $v_5\big(d(K)\big) = 8$. Hence $5^4 \parallel a$, $5^4 \parallel b$ as asserted.

Now we suppose that $5^4 \parallel a$, $5^4 \parallel b$. By Proposition 2.4 we have $5 \parallel E$. Hence 5 does not ramify in $k = Q(\sqrt{-5E})$. As $5 \mid a$, by Proposition 4.1, $5 \mid d(K)$, and so 5 ramifies in K and thus in M. Hence 5 ramifies in M/k. Then, by [1, Theorem 4.2.6 (iii)], we have $v_5\big(d(K)\big) = 8$ as asserted. ∎

Proposition 4.4 *$5^6 \parallel d(K) \iff 5 \parallel a$, $5 \nmid b$ or $5^2 \parallel a$, $5^2 \parallel b$.*

Proof By [1, Theorem 4.2.6 (iii)] we have

$$v_5\big(d(K)\big) = 0, 2, 6 \text{ or } 8.$$

If $5 \parallel a$, $5 \nmid b$ or $5^2 \parallel a$, $5^2 \parallel b$, by Propositions 4.1–4.3, we have $v_5\big(d(K)\big) \neq 0, 2$ or 8. Hence $v_5\big(d(K)\big) = 6$. On the other hand if $v_5\big(d(K)\big) = 6$ then by Propositions 4.1–4.3, a and b do *not* satisfy any of

$$5 \nmid a; \quad 5^2 \parallel a,\ 5^3 \mid b; \quad 5^4 \parallel a,\ 5^4 \parallel b.$$

Hence by (4.1) we have $5 \parallel a$, $5 \nmid b$ or $5^2 \parallel a$, $5^2 \parallel b$. ∎

5 The p-Part of $d(K)$, $p \neq 2, 5$

Let p be a prime $\neq 2, 5$. Clearly p falls into one and only one of the following cases:

(i) $p \nmid b$,
(ii) $p \mid b$, $p \nmid a$,
(iii) $1 \leq v_p(b) \leq v_p(a)$,
(iv) $1 \leq v_p(a) < v_p(b)$.

By (1.1) we have

$$\begin{aligned} v_p(b) &< 5 \quad \text{in case (iii)}, \\ v_p(a) &< 4 \quad \text{in case (iv)}. \end{aligned}$$

In the course of the proof of the next proposition we see that we must have $v_p(a) = 2$ in case (iv).

Proposition 5.1 *Let p be a prime $\neq 2, 5$. Then*

$$\begin{aligned} p^4 \parallel d(K) &\iff 1 \leq v_p(b) \leq v_p(a), \\ p^2 \parallel d(K) &\iff 2 = v_p(a) < v_p(b), \\ p \nmid d(K) &\iff v_p(a) = 0 \text{ or } v_p(b) = 0. \end{aligned}$$

https://doi.org/10.4153/CMB-2002-017-8 Published online by Cambridge University Press

Proof By Llorente, Nart and Vila [2, Theorem 1] we have

$$v_p\big(d(K)\big) = \begin{cases} 4-\big(4, v_p(a)\big), & \text{if } 5v_p(a) < 4v_p(b), \\ 5-\big(5, v_p(b)\big), & \text{if } 5v_p(a) \geq 4v_p(b). \end{cases}$$

In case (i) we have $v_p\big(d(K)\big) = 5-(5,0) = 5-5 = 0$. In case (ii) we have $v_p\big(d(K)\big) = 4-(4,0) = 4-4 = 0$. In case (iii) we have $v_p\big(d(K)\big) = 5-\big(5, v_p(b)\big) = 5-1 = 4$, as $v_p(b) = 1, 2, 3$ or 4. In case (iv) we show that $5v_p(a) < 4v_p(b)$. Suppose not. Then $5v_p(a) \geq 4v_p(b)$ and so

$$v_p(b) - 1 \geq v_p(a) \geq \frac{4}{5} v_p(b),$$

so that $v_p(b) \geq 5$. Thus $v_p(a) \geq 4v_p(b)/5 \geq 4$, contradicting (1.1). Hence $5v_p(a) < 4v_p(b)$ and so

$$v_p(4^4a^5 + 5^5b^4) = 5v_p(a) \equiv 0 \pmod 2,$$

as $4^4a^5 + 5^5b^4$ is a perfect square. Thus $v_p(a) \equiv 0 \pmod 2$. As $1 \leq v_p(a) < 4$ we must have $v_p(a) = 2$. Then $v_p\big(d(K)\big) = 4-(4,2) = 4-2 = 2$. ■

We close this section by proving the following result.

Proposition 5.2 *Let $p \neq 2, 5$ be a prime. Then*

$$p \mid E \iff 2 = v_p(a) < v_p(b), \quad \textit{(case (iv))}$$
$$p \mid F \iff 1 \leq v_p(b) \leq v_p(a), \quad \textit{(case (iii))}$$
$$p \nmid E, p \nmid F \iff v_p(a) = 0 \text{ or } v_p(b) = 0 \quad \textit{(cases (i), (ii))}.$$

Proof As m and n are coprime, p cannot divide both E and F.

If $p|E$ then $p \parallel E$, $p \nmid m^2 \pm mn - n^2$, $p \nmid 2m - n$, $p \nmid m + 2n$, $p \nmid F$, $p \nmid d_2$ so that, by Proposition 2.1, we have

$$v_p(a) = 2, \quad v_p(b) = v_p(d_1) + 3,$$

and thus

https://doi.org/10.4153/CMB-2002-017-8 Published online by Cambridge University Press

$$2 = v_p(a) < v_p(b).$$

If $p|F$ then $p \nmid m^2 - mn - n^2$, $p \nmid m^2 + n^2$, $p \nmid d_1$, $p \nmid E$, $p \nmid 2m - n$, $p \nmid m + 2n$ so that, by Proposition 2.1, we have

$$v_p(a) = v_p(d_2) + v_p(F), \quad v_p(b) = v_p(F),$$

and thus

$$v_p(a) \geq v_p(b) \geq 1.$$

If $p \nmid E$, $p \nmid F$ then, by Proposition 2.1, we have

$$v_p(a) = v_p(d_2) + v_p(m^2 - mn - n^2),$$
$$v_p(b) = v_p(d_1) + v_p(2m - n) + v_p(m + 2n).$$

As m and n are coprime at most one of $v_p(d_1)$, $v_p(d_2)$, $v_p(m^2 - mn - n^2)$, $v_p(2m - n)$, $v_p(m + 2n)$ can be nonzero so that either $v_p(a) = 0$ or $v_p(b) = 0$. ■

From Propositions 5.1 and 5.2 we have

Proposition 5.3 *If p is a prime $\neq 2, 5$ then*

$$p^4 \parallel d(K) \iff p \mid F,$$
$$p^2 \parallel d(K) \iff p \mid E,$$
$$p \nmid d(K) \iff p \nmid E \text{ and } p \nmid F.$$

6 Proof of Theorem

The Theorem now follows from Propositions 3.1, 4.1, 4.2, 4.3, 4.4 and 5.1 as $d(K) > 0$.

7 Two Corollaries

From the Theorem, Proposition 2.2, Proposition 2.4 and Proposition 5.3, we obtain the formulation of $d(K)$ in terms of m and n.

Corollary 1

$$d(K) = 2^\alpha 5^\beta \prod_{\substack{p \neq 2,5 \\ p|E}} p^2 \prod_{\substack{p \neq 2,5 \\ p|F}} p^4,$$

where

$$\alpha = \begin{cases} 4, & \text{if } m \equiv n + 1 \pmod 2, \\ 6, & \text{if } m \equiv n \equiv 1 \pmod 2, \end{cases}$$

https://doi.org/10.4153/CMB-2002-017-8 Published online by Cambridge University Press

and

$$\beta = \begin{cases} 0, & \text{if } m \equiv 3n \pmod 5,\ E \equiv 0 \pmod 5 \\ & \quad \text{or} \\ & m \equiv 2n \pmod 5,\ m \equiv 57n \pmod{125},\ E \equiv 0 \pmod 5, \\ 2, & \text{if } m \equiv 3n \pmod 5,\ E \not\equiv 0 \pmod 5 \\ & \quad \text{or} \\ & m \equiv 2n \pmod 5,\ m \equiv 57n \pmod{125},\ E \not\equiv 0 \pmod 5, \\ 6, & \text{if } m \not\equiv 2n, 3n \pmod 5 \\ & \quad \text{or} \\ & m \equiv 2n \pmod 5,\ m \not\equiv 57n \pmod{125},\ E \not\equiv 0 \pmod 5, \\ 8, & \text{if } m \equiv 2n \pmod 5,\ m \not\equiv 57n \pmod{125},\ E \equiv 0 \pmod 5. \end{cases}$$

Corollary 2 $d(K) = d(k)^2 f^4$, *where*

$$f = 5^\theta \prod_{1 \le v_p(b) \le v_p(a)} p,$$

and

$$\theta = \begin{cases} 0, & \text{if } 5 \nmid a \text{ or } 5^2 \parallel a,\ 5^3 \mid b, \\ 1, & \text{if } 5 \parallel a,\ 5 \nmid b \text{ or } 5^2 \parallel a,\ 5^2 \parallel b, \\ 2, & \text{if } 5^4 \parallel a,\ 5^4 \parallel b. \end{cases}$$

Proof From the proof of Proposition 3.1 we have

$$v_2\big(d(k)\big) = \alpha/2.$$

As $k = Q(\sqrt{-5E})$ we have

$$v_5\big(d(k)\big) = \begin{cases} 0, & \text{if } 5 \parallel E, \\ 1, & \text{if } 5 \nmid E. \end{cases}$$

Thus, by Proposition 2.4, we obtain $v_5\big(d(k)\big) = \gamma$, where

(7.1)
$$\gamma = \begin{cases} 0, & \text{if } 5 \nmid a \text{ or } 5^4 \parallel a,\ 5^4 \parallel b, \\ 1, & \text{if } 5 \parallel a,\ 5 \nmid b \text{ or } 5^2 \parallel a,\ 5^2 \mid b. \end{cases}$$

For $p \neq 2, 5$ we have

$$v_p\big(d(k)\big) = \begin{cases} 0, & \text{if } p \mid E, \\ 1, & \text{if } p \nmid E. \end{cases}$$

https://doi.org/10.4153/CMB-2002-017-8 Published online by Cambridge University Press

Hence, since $d(k) < 0$, we have

$$d(k) = -2^{\alpha/2} 5^{\gamma} \prod_{\substack{p \neq 2,5 \\ p \mid E}} p.$$

Thus, by Corollary 1, we obtain

$$\frac{d(K)}{d(k)^2} = 5^{\beta - 2\gamma} \prod_{\substack{p \neq 2,5 \\ p \mid F}} p^4.$$

From the Theorem and (7.1) we deduce that

$$\beta - 2\gamma = \begin{cases} 0, & \text{if } 5 \nmid a \text{ or } 5^2 \parallel a, 5^3 \mid b, \\ 4, & \text{if } 5 \parallel a, 5 \nmid b \text{ or } 5^2 \parallel a, 5^2 \parallel b, \\ 8, & \text{if } 5^4 \parallel a, 5^4 \parallel b, \end{cases}$$

so that

$$\beta - 2\gamma = 4\theta.$$

Finally, by Proposition 5.2, we have

$$d(K) = d(k)^2 f^4,$$

where

$$f = 5^{\theta} \prod_{\substack{p \neq 2,5 \\ p \mid F}} p = 5^{\theta} \prod_{\substack{p \neq 2,5 \\ 1 \leq v_p(b) \leq v_p(a)}} p.$$

8 Some Numerical Examples

We close with a few examples illustrating the Theorem.

$X^5 + aX + b$	$d(K)$
$a = -2^2 \times 5^2 \times 19$ $b = 2^5 \times 5^2 \times 11$	$2^4 \times 5^6$
$a = -2^2 \times 5^2 \times 19$ $b = 2^5 \times 5^3 \times 19$	$2^4 \times 5^2 \times 19^4$
$a = 2^2 \times 5^4$ $b = 2^6 \times 3 \times 5^4$	$2^4 \times 5^8$

https://doi.org/10.4153/CMB-2002-017-8 Published online by Cambridge University Press

$X^5 + aX + b$	$d(K)$
$a = 2^2 \times 5 \times 11^3 \times 59 \times 3150376609 \times 255718143721^2$ $b = 2^5 \times 11 \times 37 \times 97^2 \times 890957 \times 255718143721^3$	$2^4 \times 5^6 \times 11^4 \times 255718143721^2$
$a = 5 \times 11^2 \times 17^2 \times 149^2 \times 1699 \times 1973^2 \times 5821$ $b = -2^2 \times 11 \times 17^3 \times 73 \times 149^3 \times 1973^3 \times 7069$	$2^6 \times 5^6 \times 11^4 \times 17^2 \times 149^2 \times 1973^2$
$a = 2^2 \times 5 \times 11^2 \times 61 \times 109^2$ $b = 2^8 \times 11^2 \times 17 \times 109^3$	$2^4 \times 5^6 \times 11^4 \times 109^2$
$a = -2^2 \times 5 \times 11^3 \times 29 \times 41 \times 2521^2$ $b = 2^5 \times 11^3 \times 37 \times 53 \times 2521^3$	$2^4 \times 5^6 \times 11^4 \times 2521^2$
$a = -2^2 \times 5 \times 11^3 \times 29 \times 331 \times 9479 \times 116116717^2$ $b = 2^6 \times 11^2 \times 991 \times 23767 \times 116116717^3$	$2^4 \times 5^6 \times 11^4 \times 116116717^2$
$a = -5^2 \times 11^4 \times 131 \times 8081 \times 257111845279 \times 31058167967208281^2$ $b = 2^2 \times 5^3 \times 11 \times 37 \times 59 \times 197 \times 293 \times 1289 \times 195869 \times 31058167967208281^3$	$2^6 \times 5^2 \times 11^4 \times 31058167967208281^2$
$a = 2^2 \times 11^4 \times 865661 \times 28602901 \times 27267702368057^2$ $b = -2^7 \times 11^2 \times 137 \times 379 \times 1301 \times 4001 \times 27267702368057^3$	$2^4 \times 5^6 \times 11^4 \times 27267702368057^2$
$a = 5 \times 11^4 \times 13^2 \times 66169109^2 \times 1657799551$ $b = -2^2 \times 11^3 \times 13^3 \times 29 \times 109 \times 92693 \times 66169109^3$	$2^6 \times 5^6 \times 11^4 \times 13^2 \times 66169109^2$
$a = -5 \times 11^4 \times 53^2 \times 157^2 \times 401$ $b = 2^2 \times 11^4 \times 13 \times 19 \times 53^3 \times 149 \times 157^3$	$2^6 \times 5^6 \times 11^4 \times 53^2 \times 157^2$

https://doi.org/10.4153/CMB-2002-017-8 Published online by Cambridge University Press

References

[1] D. Liu, *Dihedral polynomial congruences and binary quadratic forms: a class field theory approach.* Ph.D. thesis, Carleton University, Ottawa, Ontario, Canada, 1992.
[2] P. Llorente, E. Nart and N. Vila, *Discriminants of number fields defined by trinomials.* Acta Arith. **43**(1984), 367–373.
[3] D. A. Marcus, *Number Fields.* Springer-Verlag, New York-Heidelberg-Berlin, 1977.
[4] G. Roland, N. Yui and D. Zagier, *A parametric family of quintic polynomials with Galois group* D_5. J. Number Theory **15**(1982), 137–142.

Department of Mathematics and Statistics
Okanagan University College
Kelowna, BC
V1V 1V7
email: bkspearm@okuc02.okanagan.bc.ca

Centre for Research in Algebra and Number Theory
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario
K1S 5B6
email: williams@math.carleton.ca

https://doi.org/10.4153/CMB-2002-017-8 Published online by Cambridge University Press