NOTE ON A PAPER OF KOBAYASHI AND NAKAGAWA

Blair K. Spearman* and Kenneth S. Williams**

Received June 29, 2000

Abstract. Let $f(x) = x^5+ax^3+bx^2+cx+d \in \mathbb{Z}[x]$ have Galois group $\mathbb{Z}/5\mathbb{Z}$. The set of primes q for which $f(x) \equiv (x+r)^5 \pmod q$ for some $r \in \mathbb{Z}$ is determined. The algorithm of Kobayashi and Nakagawa for solving the quintic equation $x^5+ax^3+bx^2+cx+d = 0$ is discussed in relation to this determination.

1. Introduction. Let $f(x) = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ be irreducible. Let $Gal(f)$ denote the Galois group of $f(x)$ over $\mathbb{Q}$. The quintic equation $f(x) = 0$ is solvable by means of radicals if and only if $Gal(f)$ is a solvable group. Dummit [1], and independently, Kobayashi and Nakagawa [2] have shown how to determine the roots of $f(x) = 0$ explicitly when $Gal(f)$ is solvable. It is known [1, p. 387] that $Gal(f)$ is a solvable group if and only if $Gal(f) \simeq F_{20}$ (the Frobenius group of order 20), D_{10} (the dihedral group of order 10) or $\mathbb{Z}_5$ (the cyclic group of order 5).

In this note we will only be concerned with those quintic polynomials f for which $Gal(f) \simeq \mathbb{Z}_5$. For such a quintic f, Kobayashi and Nakagawa [2, Theorem 1] used the existence of a special prime $q \equiv 1 \pmod 5$ such that $f(x) \equiv (x+r)^5 \pmod q$ for some $r \in \mathbb{Z}$ to obtain the explicit solution of $f(x) = 0$. It is the purpose of this note to describe explicitly the set $S(f)$ of primes q for which $f(x) \equiv (x+r)^5 \pmod q$ for some $r \in \mathbb{Z}$, that is, we determine the set

(1) $$S(f) = \left\{ q \text{ (prime)} \,\middle|\, f(x) \equiv (x+r)^5 \pmod q \text{ for some } r \in \mathbb{Z} \right\}.$$

Before giving our determination of the set $S(f)$, it is convenient to introduce some notation. We let $\theta = \theta_1, \theta_2, \theta_3, \theta_4, \theta_5 \in \mathbb{C}$ be the roots of $f(x)$. We set $K = \mathbb{Q}(\theta)$ so that K is a cyclic quintic field. If there exists a prime p such that

$$p \mid a_4, \ \ p^2 \mid a_3, \ \ p^3 \mid a_2, \ \ p^4 \mid a_1, \ \ p^5 \mid a_0$$

then θ/p is a root of

$$x^5 + (a_4/p)x^4 + (a_3/p^2)x^3 + (a_2/p^3)x^2 + (a_1/p^4)x + (a_0/p^5) \in \mathbb{Z}[x]$$

and $\mathbb{Q}(\theta/p) = K$. Thus we may make the following simplifying assumption:

$$m \mid a_4, \ \ m^2 \mid a_3, \ \ m^3 \mid a_2, \ \ m^4 \mid a_1, \ \ m^5 \mid a_0 \Longrightarrow |m| = 1.$$

We let $f(K)$ denote the conductor of K so that $f(K)$ is the smallest positive integer m such that $K \subseteq \mathbb{Q}(e^{2\pi i/m})$. Since $Gal(f)$ is abelian the existence of such an integer m is guaranteed by the Kronecker-Weber theorem [5, p. 421]. It is well-known that the discriminant of K, denoted by $d(K)$, is related to the conductor of K by $d(K) = f(K)^4$ as $Gal(f) \simeq \mathbb{Z}_5$, see for example [3, p. 831]. We denote the set of rational primes which ramify in K by $C(K)$, that is,

(2) $$C(K) = \{q \text{ (prime)} : q \mid f(K)\}.$$

2000 *Mathematics Subject Classification.* Primary 11R20, 11S05.
Key words and phrases. Solvable quintics.

We prove

Theorem. *Let*

$$f(x) = x^5 + ax^3 + bx^2 + cx + d \tag{3}$$

be an irreducible polynomial in $\mathbb{Z}[x]$ *satisfying*

$$m^2 \mid a, \ \ m^3 \mid b, \ \ m^4 \mid c, \ \ m^5 \mid d \ \ \Longrightarrow |m| = 1 \tag{4}$$

and

$$Gal(f) \simeq \mathbb{Z}_5. \tag{5}$$

Let $\theta \in \mathbb{C}$ *be a root of* $f(x)$. *Set* $K = \mathbb{Q}(\theta)$. *Then*

$$S(f) = \begin{cases} C(K) \cup \{5\}, & \text{if } 5^{20} \mid disc(f); \\ & 5 \mid a, \ 5 \mid b, \ 5 \mid c, \ 5 \mid d; \\ & \text{and } 5^3 \mid a, \ 5^4 \mid b, \ 5^4 \mid c, \ 5^4 \parallel d \\ & \qquad \text{does not hold.} \\ C(K), & \text{otherwise.} \end{cases} \tag{6}$$

Our Theorem shows that the statement in [2, p. 884]: "*Further by virtue of normal basis theory, we can find a prime number* $q = 5t + 1$ *such that* $f(x) \equiv (x + r)(x + r) \cdots (x + r)$ $\pmod q$, *where r is some natural number.*" is not quite correct as it stands. Example 1 illustrates this.

Example 1. *Let*

$$f(x) = x^5 - 25x^3 + 50x^2 - 25.$$

Then

$$\begin{array}{rcll} Gal(f) & \simeq & \mathbb{Z}_5, & \text{[MAPLE]} \\ disc(f) & = & 5^{12}7^2, & \text{[MAPLE]} \\ d(K) & = & 390625 = 5^8, & \text{[PARI]} \\ f(K) & = & 5^2, & \\ C(K) & = & \{5\}, & \end{array}$$

and, by the Theorem, we have

$$S(f) = \{5\}$$

so there does not exist a prime $q \equiv 1 \pmod 5$ *in* $S(f)$.

The assertion $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\omega_q)$ in [2 , p. 884] holds for $q = f(K)$ but q may not be a prime. We illustrate this in Example 2.

Example 2. *Let*

$$f(x) = x^5 - 88660x^3 + 16437905x^2 - 1133736340x + 27615008971.$$

Then

$$\begin{array}{rcll} Gal(f) & \simeq & \mathbb{Z}_5, & \text{[MAPLE]} \\ disc(f) & = & 5^{20}11^4 13^2 31^4 431^2, & \text{[MAPLE]} \\ d(K) & = & 13521270961 = 11^4 31^4, & \text{[PARI]} \\ f(K) & = & 11 \cdot 31, & \end{array}$$

so

$$\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\omega_{11\cdot 31})$$

but

$$\mathbb{Q}(\alpha) \nsubseteq \mathbb{Q}(\omega_{11}), \quad \mathbb{Q}(\alpha) \nsubseteq \mathbb{Q}(\omega_{31}).$$

We note that the algorithm of Kobayashi and Nakagawa is valid if their use of the prime q is replaced by the conductor $f(K)$ [2 , p. 884].

Our Theorem shows that if $f(x)$ contains no x^4 term then the set $S(f)$ consists of the prime divisors of the conductor $f(K)$ together with the prime 5 in certain cases. However, if $f(x)$ has a nonzero coefficient of the x^4 term then $S(f)$ may contain primes not dividing the conductor and in fact we can construct $f(x)$ so that $S(f)$ contains an arbitrary number of such primes. We illustrate this in Example 3.

Example 3. *Let*

$$f(x) = x^5 + x^4 - 12x^3 - 21x^2 + x + 5.$$

Here

$$\begin{array}{rcll} Gal(f) & \simeq & \mathbb{Z}_5, & \text{[MAPLE]} \\ disc(f) & = & 5^2 31^4, & \text{[MAPLE]} \\ d(K) & = & 923521 = 31^4, & \text{[PARI]} \\ f(K) & = & 31, & \\ C(K) & = & \{31\}. & \end{array}$$

By factoring $f(x)$ modulo each prime dividing disc(f), we find that

$$S(K) = \{31\}.$$

Let $p_1,\ p_2, \ldots, p_N$ denote N distinct primes different from 5 and 31. Let $r \in \mathbb{Z}$. Set

$$p = p_1 \cdots p_N$$

and

$$f_p(x) = p^5 f((x+r)/p) = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,$$

where

$$\begin{array}{rcl} a_4 & = & 5r + p, \\ a_3 & = & 10r^2 + 4pr - 12p^2, \\ a_2 & = & 10r^3 + 6pr^2 - 36p^2r - 21p^3, \\ a_1 & = & 5r^4 + 4pr^3 - 36p^2r^2 - 42p^3r + p^4, \\ a_0 & = & r^5 + pr^4 - 12p^2r^3 - 21p^3r^2 + p^4r + 5p^5. \end{array}$$

Since a_0 is a quintic polynomial in r, which is primitive, has no fixed divisors, and has nonzero discriminant, by a theorem of Nagel [4] *we can choose infinitely many $r \in \mathbb{Z}$ so that a_0 is fifth power free. Hence $f_p(x)$ satisfies the simplifying assumption* (4)*. Also*

$$Gal(f_p) = Gal(f) \simeq \mathbb{Z}_5.$$

Moreover, for $i = 1, 2, \ldots, N$ *we have*

$$f_p(x) \equiv x^5 + 5rx^4 + 10r^2x^3 + 10r^3x^2 + 5r^4x + r^5 \equiv (x+r)^5 \pmod{p_i},$$

so that

$$p_i \in S(f_p), \quad i = 1, 2, \ldots, N.$$

Example 3 shows that the algorithm of Kobayashi and Nakagawa should only be applied to quintic polynomials with no x^4 term.

Our Theorem is proved in Section 5 after some preliminary results are proved in Sections 2, 3 and 4. From this point on we assume the notation of the Theorem.

2. A necesssary and sufficient condition for a prime $q \neq 5$ to belong to $S(f)$. With the notation of the theorem we prove the following result.

Proposition 2.1. *Let q be a prime with $q \neq 5$. Then*

$$q \in S(f) \Leftrightarrow q \in C(K).$$

Proof. Let $q \neq 5$ be a prime in $S(f)$. Suppose that $q \notin C(K)$. Then q does not ramify in K. Thus $q = Q_1 \cdots Q_t$ $(t = 1, 5)$ for distinct prime ideals $Q_1, \ldots, Q_t$. As $q \in S(f)$ there exists an integer r such that $f(x) \equiv (x+r)^5 \pmod{q}$. Comparing coefficients of x^4, we obtain $5r^4 \equiv 0 \pmod{q}$, so that, as $q \neq 5$, we have $q \mid r$. Hence $f(x) \equiv x^5 \pmod{q}$ and so $0 = f(\theta) \equiv \theta^5 \pmod{q}$. Thus $Q_i \mid \theta^5$ for $i = 1, \ldots, t$ and so, as Q_i is a prime ideal, $Q_i \mid \theta$ for $i = 1, \ldots, t$. Since the Q_i are distinct prime ideals, we deduce that $Q_1 Q_2 \cdots Q_t \mid \theta$, that is, $q \mid \theta$. This proves that $\theta/q \in O_K$. The minimal polynomial of θ/q over $\mathbb{Q}$ is

$$x^5 + (a/q^2)x^3 + (b/q^3)x^2 + (c/q^4)x + (d/q^5),$$

which must belong in $\mathbb{Z}[x]$. Hence we have

$$q^2 \mid a, \ q^3 \mid b, \ q^4 \mid c, \ q^5 \mid d,$$

which contradicts (4). Hence $q \in C(K)$.

Conversely suppose that q $(\neq 5)$ is a prime in $C(K)$. Thus q ramifies in K. As K is a cyclic quintic field, we have $q = Q^5$ for some prime ideal Q with $N(Q) = q$. Thus $N(O_K/Q) = q$ and so as $\theta \in O_K$ there exists an integer r such that $\theta \equiv r \pmod{Q}$. Taking conjugates we obtain

$$\theta_i \equiv r \pmod{Q} \quad (i = 1, 2, 3, 4, 5).$$

Hence

$$f(x) = \prod_{i=1}^{5} (x - \theta_i) \equiv (x - r)^5 \pmod{Q}.$$

Since $f(x) \in \mathbb{Z}[x]$, $(x-r)^5 \in \mathbb{Z}[x]$ and $q = Q^5$, we must have

$$f(x) \equiv (x-r)^5 \pmod{q},$$

proving that $q \in S(f)$. □

3. A necessary and sufficient condition for 5 to belong to $S(f)$.

Proposition 3.1. $5 \in S(f) \Leftrightarrow 5 \mid a, \ 5 \mid b, \ 5 \mid c.$

Proof. If $5 \in S(f)$ then there exists $r \in \mathbb{Z}$ such that

$$f(x) \equiv (x+r)^5 \pmod{5},$$

that is

$$\begin{aligned} x^5 + ax^3 + bx^2 + cx + d &\equiv x^5 + 5rx^4 + 10r^2x^3 + 10r^3x^2 + 5r^4x + r^5 \\ &\equiv x^5 + r \pmod{5}, \end{aligned}$$

so that $5 \mid a,\ 5 \mid b,\ 5 \mid c$.

Conversely suppose that $5 \mid a,\ 5 \mid b,\ 5 \mid c$. Then

$$x^5 + ax^3 + bx^2 + cx + d \equiv x^5 + d \equiv (x+d)^5 \pmod{5},$$

so that $5 \in S(f)$. □

4. A necessary and sufficient condition for 5 to belong to $C(K)$. In this section we relate the conditions,

$$5 \mid a,\ 5 \mid b,\ 5 \mid c, \tag{7}$$

$$5^3 \mid a,\ 5^4 \mid b,\ 5^4 \mid c,\ 5^4 \parallel d, \tag{8}$$

and

$$5^{20} \mid disc(f), \tag{9}$$

to one another, as well as to the condition

$$5 \in C(K). \tag{10}$$

Clearly

$$(8) \Rightarrow (7). \tag{11}$$

Lemma 4.1. (8) ⇒ (9).

Proof. By the symmetric function theorem, we have

$$disc(f) = \sum_{2e+3f+4g+5h=20} c(e,f,g,h) a^e b^f c^g d^h, \tag{12}$$

where the sum is over nonnegative integers $e,\ f,\ g,\ h$ satisfying the stated equality and $c(e,f,g,h) \in \mathbb{Z}$. Appealing to (8) we see that

$$a^e b^f c^g d^h \equiv 0 \pmod{5^{3e+4f+4g+4h}}, \tag{13}$$

for each term in the sum in (12). The summation condition in (12) implies that $h = 0,1,2,3$ or 4. Hence we can rewrite (12) as

$$disc(f) = \sum_{h=0}^{4} S_h(f), \tag{14}$$

where

(15) $$S_h(f) = \sum_{2e+3f+4g=20-5h} c(e,f,g,h)a^e b^f c^g d^h.$$

First we consider $S_0(f)$. The summation condition is $2e+3f+4g=20$ so

$$3e+4f+4g \geq 2e+3f+4g = 20$$

and thus

$$a^e b^f c^g \equiv 0 \pmod{5^{20}}$$

giving

$$S_0(f) \equiv 0 \pmod{5^{20}}.$$

Secondly we consider $S_1(f)$. Here $2e+3f+4g=15$ so

$$3e+4f+4g+4 \geq 2e+3f+4g+4 = 19$$

and thus

$$a^e b^f c^g d \equiv 0 \pmod{5^{19}}$$

giving

$$S_1(f) \equiv 0 \pmod{5^{19}}.$$

Thirdly we consider $S_2(f)$. Here $2e+3f+4g=10$ so that $e+f \geq 1$ and thus

$$3e+4f+4g+8 \geq 2e+3f+4g+9 = 19.$$

Hence

$$a^e b^f c^g d^2 \equiv 0 \pmod{5^{19}}$$

giving

$$S_2(f) \equiv 0 \pmod{5^{19}}.$$

Fourthly we consider $S_3(f)$. Here $2e+3f+4g=5$ so that $e=f=1$, $g=0$ and thus

$$3e+4f+4g+12 = 19.$$

Hence

$$a^e b^f c^g d^3 \equiv 0 \pmod{5^{19}}$$

giving

$$S_3(f) \equiv 0 \pmod{5^{19}}.$$

Finally we consider $S_4(f)$. Here $2e+3f+4g=0$ so that $e=f=g=0$. Thus

$$S_4(x^5+ax^3+bx^2+cx+d) = S_4(f) = c(0,0,0,4)d^4.$$

Since

$$disc(x^5+d) = 5^5 d^4,$$

we have

$$S_4(x^5+d) = 5^5 d^4,$$

so that $c(0,0,0,4) = 5^5$, and thus

$$S_4(f) = 5^5 d^4 \equiv 0 \pmod{5^{21}}.$$

Hence $disc(f) \equiv 0 \pmod{5^{19}}$. Since $Gal(f) \simeq \mathbb{Z}_5$, $disc(f)$ is a perfect square, and so $disc(f) \equiv 0 \pmod{5^{20}}$ as asserted. □

Lemma 4.2. (8) $\Rightarrow 5 \in C(K)$.

Proof. We define a', b', c', $d' \in \mathbb{Z}$ by

$$a' = a/5^3,\ b' = b/5^4,\ c' = c/5^4,\ d' = d/5^4.$$

Clearly $5 \nmid d'$. We set

$$h(x) = x^5 + 5c'x^4 + 5^2b'd'x^3 + 5^2a'd'^2x^2 + 5d'^4 \in \mathbb{Z}[x].$$

Then

$$\begin{aligned} h(5d'x) &= 5^5d'^5x^5 + 5^5c'd'^4x^4 + 5^5b'd'^4x^3 + 5^4a'd'^4x^2 + 5d'^4 \\ &= 5d'^4x^5(5^4d' + 5^4c'/x + 5^4b'/x^2 + 5^3a'/x^3 + 1/x^5) \\ &= 5d'^4x^5(d + c/x + b/x^2 + a/x^3 + 1/x^5) \\ &= 5d'^4x^5f(1/x). \end{aligned}$$

Hence $h(x)$ can be taken as the defining polynomial for the field K. Since $h(x)$ is 5 - Eisenstein we have $5 = \wp^5$ for some prime ideal $\wp$ in K, see for example [5 , Prop. 4.18, p. 181]. Thus 5 ramifies in K and so $5 \in C(K)$. □

Lemma 4.3. *If* (8) *does not hold and* (9) *holds then* $5 \notin C(K)$.

Proof. Suppose that $5 \in C(K)$. Then 5 ramifies in K. Hence $5 = \wp^5$ for some prime ideal in K. As $N(\wp) = 5$ there exists $r \in \mathbb{Z}$ $(r = 0, 1, 2, 3, 4)$ such that

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

We consider two cases.

Case (i): $r = 0$. In this case $\wp \mid \theta$ so that $\wp^k \parallel \theta$ for some positive integer k. Suppose that $k \geq 5$. Then $5 \mid \theta$ and thus $\theta/5 \in O_K$. The minimal polynomial of $\theta/5$ over $\mathbb{Q}$ is

$$x^5 + (a/5^2)x^3 + (b/5^3)x^2 + (c/5^4)x + (d/5^5),$$

which must belong in $\mathbb{Z}[x]$. Hence we have

$$5^2 \mid a,\ 5^3 \mid b,\ 5^4 \mid c,\ 5^5 \mid d,$$

contradicting (4). Thus $k = 1, 2, 3$ or 4.

Next we define the nonnegative integer l by $\wp^l \parallel f'(\theta)$. By conjugation we have $\wp^l \parallel f'(\theta_i)$ $(i = 1, 2, 3, 4, 5)$. Hence

$$\wp^{5l} \parallel \prod_{i=1}^{5} f'(\theta_i) = \pm disc(f).$$

But $\wp^{100} = 5^{20} \mid disc(f)$, so we must have $5l \geq 100$, that is, $l \geq 20$. Hence

$$\wp^{20} \mid f'(\theta). \tag{16}$$

Now

$$f'(\theta) = 5\theta^4 + 3a\theta^2 + 2b\theta + c, \tag{17}$$

where

$$v_\wp(5\theta^4) = 5 + 4k \equiv 4k \pmod{5}, \tag{18}$$

$$v_\wp(3a\theta^2) = v_\wp(a) + 2k \equiv 2k \pmod{5}, \tag{19}$$

$$v_\wp(2b\theta) = v_\wp(b) + k \equiv k \pmod{5}, \tag{20}$$

$$v_\wp(c) \equiv 0 \pmod{5}. \tag{21}$$

As $k = 1, 2, 3$ or 4, we see that $v_\wp(5\theta^4)$, $v_\wp(3a\theta^2)$, $v_\wp(2b\theta)$, $v_\wp(c)$ are all distinct modulo 5, and thus they must all be different. Hence, by (16) and (17), we have

$$v_\wp(5\theta^4) \geq 20,\ v_\wp(3a\theta^2) \geq 20,\ v_\wp(2b\theta) \geq 20,\ v_\wp(c) \geq 20. \tag{22}$$

From (18) and (22), we deduce that $5 + 4k \geq 20$, so that $k \geq 4$. But $k = 1, 2, 3$ or 4 so we must have $k = 4$. Hence

$$\wp^4 \parallel \theta. \tag{23}$$

Next, appealing to (19), (22) and (23), we deduce that $v_\wp(a) + 8 = v_\wp(3a\theta^2) \geq 20$, so that $v_\wp(a) \geq 12$. Thus $v_5(a) \geq 12/5$ so that

$$v_5(a) \geq 3. \tag{24}$$

Further, from (20), (22) and (23), we obtain $v_\wp(b) + 4 = v_\wp(2b\theta) \geq 20$, so that $v_\wp(b) \geq 16$. Thus $v_5(b) \geq 16/5$ so that

$$v_5(b) \geq 4. \tag{25}$$

Also, from (22), we have $v_\wp(c) \geq 20$ so that $v_5(c) \geq 20/5$, that is

$$v_5(c) \geq 4. \tag{26}$$

Further we have

$$\wp^{20} \parallel \theta^5,\ \ \wp^{24} \mid a\theta^3,\ \ \wp^{24} \mid b\theta^2,\ \ \wp^{24} \mid c\theta,$$

so that

$$\wp^{20} \parallel -\theta^5 - a\theta^3 - b\theta^2 - c\theta = d,$$

and thus

$$5^4 \parallel d. \tag{27}$$

Clearly (24) - (27) contradict that (8) does not hold.

Case (ii): $r = 1, 2, 3, 4$. We set

$$\begin{cases} g(x) = f(x+r) \\ \qquad = (x+r)^5 + a(x+r)^3 + b(x+r)^2 + c(x+r) + d \\ \qquad = x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 \in \mathbb{Z}[x], \end{cases} \tag{28}$$

where

$$(29)\qquad \begin{cases} b_4 = 5r, \\ b_3 = 10r^2 + a, \\ b_2 = 10r^3 + 3ar + b, \\ b_1 = 5r^4 + 3ar^2 + 2br + c, \\ b_0 = r^5 + ar^3 + br^2 + cr + d. \end{cases}$$

Further we set $\alpha = \theta - r$ so that $\alpha \equiv 0 \pmod{\wp}$. Moreover $g(\alpha) = f(\alpha + r) = f(\theta) = 0$ so that $\alpha \in \mathbb{C}$ is a root of $g(x)$. Define the positive integer k by $\wp^k \parallel \alpha$. If $k \geq 5$ then $\alpha/5 \in O_K$ and, as the minimal polynomial of $\alpha/5$ is

$$h(x) = x^5 + \frac{b_4}{5}x^4 + \frac{b_3}{5^2}x^3 + \frac{b_2}{5^3}x^2 + \frac{b_1}{5^4}x + \frac{b_0}{5^5},$$

we must have $b_4/5,\ b_3/5^2,\ b_2/5^3,\ b_1/5^4,\ b_0/5^5 \in \mathbb{Z}$. As $\alpha/5 \in O_K$ and $|O_K/\wp| = N(\wp) = 5$, there exists $s \in \mathbb{Z}$ such that $\alpha/5 \equiv s \pmod{\wp}$. Set $\alpha_i = \theta_i - r$ $(i = 1,2,3,4,5)$ so that $\alpha_1 = \alpha$. The roots of $h(x)$ are $\alpha_i/5$ $(i = 1,2,3,4,5)$. By conjugation we have $\alpha_i/5 \equiv s \pmod{\wp}$ $(i = 1,2,3,4,5)$. Hence

$$h(x) = \prod_{i=1}^{5}(x - \alpha_i/5) \equiv \prod_{i=1}^{5}(x - s) \equiv (x - s)^5 \pmod{\wp}.$$

Thus

$$r = b_4/5 = \text{ coefficient of } x^4 \text{ in } h(x) \equiv -5s \equiv 0 \pmod{\wp},$$

contradicting $r = 1,2,3,4$. Hence $k = 1,2,3,4$.

Since $\alpha = \alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4,\ \alpha_5 \in \mathbb{C}$ are the roots of $g(x)$, we have

$$\wp^{100} = 5^{20} \mid disc(f) = disc(g) = \pm\prod_{i=1}^{5} g'(\alpha_i).$$

Suppose that $\wp^t \parallel g'(\alpha)$. By conjugation we have $\wp^t \parallel g'(\alpha_i)$ $(i = 1,2,3,4,5)$. Hence

$$\wp^{5t} \parallel \prod_{i=1}^{5} g'(\alpha_i).$$

Thus $5t \geq 100$ and so $t \geq 20$, that is,

$$(30)\qquad \wp^{20} \mid g'(\alpha).$$

Further, from (28) and (29), we have

$$(31)\qquad g'(\alpha) = 5\alpha^4 + 20r\alpha^3 + 3b_3\alpha^2 + 2b_2\alpha + b_1,$$

and

$$\begin{aligned} v_\wp(5\alpha^4) &= 5 + 4k \equiv 4k \pmod{5}, \\ v_\wp(20r\alpha^3) &= 5 + 3k \equiv 3k \pmod{5}, \\ v_\wp(3b_3\alpha^2) &= v_\wp(b_3) + 2k \equiv 2k \pmod{5}, \\ v_\wp(2b_2\alpha) &= v_\wp(b_2) + k \equiv k \pmod{5}, \\ v_\wp(b_1) &\equiv 0 \pmod{5}, \end{aligned}$$

showing that $v_\wp(5\alpha^4)$, $v_\wp(20r\alpha^3)$, $v_\wp(3b_3\alpha^2)$, $v_\wp(2b_2\alpha)$, $v_\wp(b_1)$ are all distinct modulo 5. Hence they must all be different. From (30) and (31) we deduce that

$$\wp^{20} \mid 5\alpha^4,\ \wp^{20} \mid 20r\alpha^3,\ \wp^{20} \mid 3b_3\alpha^2,\ \wp^{20} \mid 2b_2\alpha,\ \wp^{20} \mid b_1.$$

From the second of these we have $5 + 3k \geq 20$ so that $k \geq 5$. This contradicts $k = 1, 2, 3$ or 4.

In both Case (i) and Case (ii) we have arrived at a contradiction. Thus $5 \notin C(K)$. □

Lemma 4.4. *If* (7) *does not hold then* $5 \notin C(K)$.

Proof. Suppose that (7) does not hold, but $5 \in C(K)$. Then 5 ramifies in K. Thus $5 = \wp^5$ for some prime ideal $\wp$ of K. Hence

$$|O_K/\wp| = N(\wp) = 5,$$

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

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

Taking conjugates we obtain

$$\theta_i \equiv r \pmod{\wp} \ \ (i = 1, 2, 3, 4, 5).$$

Hence

$$f(x) = \prod_{i=1}^{5}(x - \theta_i) \equiv \prod_{i=1}^{5}(x - r) \equiv (x - r)^5 \pmod{\wp}.$$

Since $f(x) \in \mathbb{Z}[x]$, $(x - r)^5 \in \mathbb{Z}[x]$ and $5 = \wp^5$, we deduce that

$$f(x) \equiv (x - r)^5 \pmod{5}.$$

Thus

$$x^5 + ax^3 + bx^2 + cx + d \equiv x^5 - r \pmod{5},$$

so

$$5 \mid a,\ 5 \mid b,\ 5 \mid c,$$

which is a contradiction as (7) does not hold. Hence $5 \notin C(K)$. □

Lemma 4.5. *If* (7) *holds and* (9) *does not hold then* $5 \in C(K)$.

Proof. Suppose $5 \notin C(K)$. Then

$$5 = Q_1 \cdots Q_t \ \ (t = 1 \text{ or } 5)$$

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

$$\begin{aligned} 0 = f(\theta) &= \theta^5 + a\theta^3 + b\theta^2 + c\theta + d \\ &\equiv \theta^5 + d \equiv \theta^5 + d^5 \equiv (\theta + d)^5 \pmod{5} \end{aligned}$$

so that $Q_i \mid (\theta + d)^5$ and thus $Q_i \mid \theta + d$ for $i = 1, \ldots, t$. Hence $Q_1 \cdots Q_t \mid \theta + d$ and so $5 \mid \theta + d$. By conjugation we have

$$5 \mid \theta_i + d \ \ (i = 1, 2, 3, 4, 5).$$

Hence

$$5 \mid \theta_i - \theta_j \ \ (1 \le i < j \le 5)$$

and so

$$5^{20} \mid \prod_{1 \le i < j \le 5} (\theta_i - \theta_j)^2,$$

that is

$$5^{20} \mid disc(f),$$

a contradiction as (9) does not hold. Hence $5 \in C(K)$. □

Appealing to (11) and Lemmas 4.1 - 4.5 we obtain the following table, which we give for convenience as a proposition.

Proposition 4.1.

(7) holds	(8) holds	(9) holds	Conclusion	Reason
yes	yes	yes	$5 \in C(K)$	Lemma 4.2
no	yes	yes	cannot occur	(11)
yes	no	yes	$5 \notin C(K)$	Lemma 4.3
no	no	yes	$5 \notin C(K)$	Lemma 4.3 or 4.4
yes	yes	no	cannot occur	Lemma 4.1
no	yes	no	cannot occur	(11) or Lemma 4.1
yes	no	no	$5 \in C(K)$	Lemma 4.5
no	no	no	$5 \notin C(K)$	Lemma 4.4

5. Proof of Theorem. The Theorem follows immediately from Propositions 2.1, 3.1 and 4.1. □

References

[1] David S. Dummit, *Solving solvable quintics,* Math. Comp. **57** (1991), 387–401.

[2] Sigeru Kobayashi and Hiroshi Nakagawa, *Resolution of solvable quintic equation,* Math. Japonica **37** (1992), 883–886.

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

[4] T. Nagel, *Zur Arithmetik der Polynome*, Abh. Math. Sem. Hamburg **1** (1922), 179–194.

[5] Wladyslaw Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers,* Second edition, Springer-Verlag Berlin-Heidleberg-New York and PWN-Polish Scientific Publishers, Warsaw, 1990.

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

**School of Mathematics and Statistics, Carleton University, Ottawa, Ont ario,Canada K1S 5B6
E-mail address: williams@math.carleton.ca