Canad. Math. Bull. Vol. **57** (3), 2014 pp. 538–545
http://dx.doi.org/10.4153/CMB-2014-008-1

Infinite Families of A_4-Sextic Polynomials

Joshua Ide and Lenny Jones

Abstract. In this article we develop a test to determine whether a sextic polynomial that is irreducible over $\mathbb{Q}$ has Galois group isomorphic to the alternating group A_4. This test does not involve the computation of resolvents, and we use this test to construct several infinite families of such polynomials.

1 Introduction

The classical inverse Galois problem—to determine if a particular finite group can be realized as a Galois group of some polynomial over $\mathbb{Q}$—dates back at least to 1892, when Hilbert gave families of polynomials having Galois group isomorphic to the symmetric group. However, he was unable to give such a parameterized family of polynomials having Galois group isomorphic to the alternating group. For a good account of the history of this problem and a modern treatment of the techniques, see [MM].

In this article we develop a test to determine whether a sextic polynomial that is irreducible over $\mathbb{Q}$ has Galois group isomorphic to the alternating group A_4. The test is simple to apply and does not involve the computation of resolvents. As an application, we use the test to construct several infinite families of such polynomials. More precisely, we prove the following theorem.

Theorem 1.1 *Let $f(x) \in \mathbb{Z}[x]$ be a sextic polynomial that is irreducible over $\mathbb{Q}$. Suppose that $f(\theta) = 0$ and that $\mathbb{Q}(\theta)$ contains a subfield $\mathbb{Q}(\phi)$ such that $g(\phi) = 0$, where $g(x) \in \mathbb{Z}[x]$ is a cubic polynomial that is irreducible over $\mathbb{Q}$. If both $\Delta(f)$ and $\Delta(g)$ are squares in $\mathbb{Z}$, then* $\mathrm{Gal}(f) \simeq A_4$.

Corollary 1.2 *Let $g(x) \in \mathbb{Z}[x]$ be a monic cubic polynomial such that $f(x) := g(x^2)$ is irreducible over $\mathbb{Q}$. If both $\Delta(f)$ and $\Delta(g)$ are squares in $\mathbb{Z}$, then* $\mathrm{Gal}(f) \simeq A_4$.

We use Theorem 1.1 and Corollary 1.2 to prove the following theorem.

Theorem 1.3 *Let $A, B, m, d \in \mathbb{Z}$ and define the following infinite families of polynomials:*

$$\mathcal{F}_1 = \left\{ x^6 + A^2x^4 - B^2x^2 - m^2 \;\middle|\; AB = 3m \text{ with } m \not\equiv 0 \pmod 3 \right\},$$
$$\mathcal{F}_2 = \left\{ x^6 + (d^2 + d + 4)m^2x^4 + 3m^4x^2 - m^6 \right\},$$

Received by the editors October 8, 2012; revised September 14, 2013.
Published electronically April 15, 2014.
AMS subject classification: **12F10**, 12F12, 11R32, 11R09.
Keywords: Galois group, sextic polynomial, inverse Galois theory, irreducible polynomial.

$$\mathcal{F}_3 = \left\{ x^6 + (d+3m^2)x^4 + dm^2x^2 - m^6 \;\middle|\; m \equiv 1 \pmod 2 \right\}.$$

Let $f \in \mathcal{F}_i$ for any $i \in \{1,2,3\}$. Then $f \in \mathcal{F}_i$ is irreducible over $\mathbb{Q}$ and $\mathrm{Gal}(f) \simeq A_4$.

Theorem 1.4 *Define an infinite family $\mathcal{F}_4$ of polynomials as follows. For $a, b, c \in \mathbb{Z}$, the polynomial $f(x) = x^6 - bx^4 + acx^2 - c^2$ is an element of $\mathcal{F}_4$ if and only if $f(x)$ is irreducible over $\mathbb{Q}$ and $\Delta(g)$ is a square in $\mathbb{Z}$, where $g(x) = x^3 + ax^2 + bx + c$. Then every polynomial $f \in \mathcal{F}_4$ has* $\mathrm{Gal}(f) \simeq A_4$.

2 Definitions and Preliminaries

Throughout this paper, we let $\Delta(f)$ denote the discriminant over $\mathbb{Q}$ of the polynomial $f(x)$, and if $f(x)$ is irreducible over $\mathbb{Q}$, we let $\mathrm{Gal}(f)$ denote its Galois group over $\mathbb{Q}$. For an algebraic number field K, we let $\Delta(K)$ denote the discriminant of K over $\mathbb{Q}$, and we let $\mathbb{Z}_K$ denote the ring of algebraic integers of K. For the sake of brevity, unless stated otherwise, when we say a polynomial is irreducible or reducible, we mean irreducible over $\mathbb{Q}$ or reducible over $\mathbb{Q}$. The following theorems are needed in the sequel.

Theorem 2.1 ([C]) *Suppose that* $\deg(f(x)) = n$. *If $f(x)$ is irreducible, then* $\mathrm{Gal}(f)$ *is isomorphic to a subgroup of the alternating group A_n if and only if $\Delta(f)$ is a square in $\mathbb{Z}$.*

Theorem 2.2 ([C]) *Let $f(x)$ be a sextic polynomial that is irreducible. Suppose that $f(\theta) = 0$ and let $K = \mathbb{Q}(\theta)$. If K contains a cubic subfield and $\Delta(f)$ is a square in $\mathbb{Z}$, then* $\mathrm{Gal}(f) \simeq S_4$ *or* $\mathrm{Gal}(f) \simeq A_4$.

The following theorem is due to Stickelberger.

Theorem 2.3 ([C]) *Let p be an odd prime, and suppose that $f(x) \in \mathbb{F}_p[x]$ is such that* $\deg(f) = n \geq 2$ *and* $\Delta := \Delta(f) \not\equiv 0 \pmod p$. *If k is the number of monic irreducible factors of $f(x)$, then $(\Delta/p) = (-1)^{n-k}$, where (Δ/p) is the Legendre symbol modulo p.*

3 Proof of Theorem 1.1 and Corollary 1.2

3.1 Proof of Theorem 1.1

We have immediately from Theorem 2.2 that $\mathrm{Gal}(f) \simeq S_4$ or $\mathrm{Gal}(f) \simeq A_4$. Since $[\mathbb{Q}(\phi):\mathbb{Q}] = 3$ and $\Delta(g)$ is a square in $\mathbb{Z}$, we deduce from Theorem 2.1 that $\mathbb{Q}(\phi)$ is a normal extension of $\mathbb{Q}$. Thus, $\mathrm{Gal}(f)$ contains a normal subgroup of index 3, and hence $\mathrm{Gal}(f) \simeq A_4$.

3.2 Proof of Corollary 1.2

Suppose that $f(\theta) = 0$. Then $g(\phi) = 0$, where $\phi = \theta^2$. Since $f(x)$ is irreducible, we have that $g(x)$ is irreducible, and hence the corollary follows from Theorem 1.1. ∎

https://doi.org/10.4153/CMB-2014-008-1 Published online by Cambridge University Press

4 Proof of Theorem 1.3

The proof is divided into three sections according to the three cases $f \in \mathcal{F}_i$ for $i \in \{1, 2, 3\}$. In each case, we let $f(x) = g(x^2)$, $F = \mathbb{Q}(\theta)$, and $K = \mathbb{Q}(\theta^2)$, where $f(\theta) = 0$. Using Corollary 1.2, we only need to establish that $f(x)$ is irreducible and that both $\Delta(f)$ and $\Delta(g)$ are squares in $\mathbb{Z}$. Although the proofs in all three cases are similar, we provide the basic details in each situation. The following lemma is useful in all three cases.

Lemma 4.1 *Let $a, b, c \in \mathbb{Z}$. Let $g(x) = x^3 + ax^2 + bx - c^2$ and $f(x) = g\left(x^2\right)$. Then $\Delta(f)$ is a square in $\mathbb{Z}$.*

Proof A simple calculation gives

$$\Delta(f) = 2^6 c^2 (4b^3 + 27c^4 + 18abc^2 - a^2b^2 - 4a^3c^2)^2. \qquad \blacksquare$$

4.1 The Proof of Theorem 1.3 for $\mathcal{F}_1$

We wish to show that $f(x)$ is irreducible. To do this, we first show that $g(x)$ is irreducible. In general, the irreducibility of $g(x)$ is not equivalent to the irreducibility of $f(x)$. However, in this situation the irreducibility of $f(x)$ follows from the irreducibility of $g(x)$. We prove a lemma that is slightly more general than needed, but it is of some interest in its own right. The irreducibility of $g(x)$ will then follow as a special case.

Lemma 4.2 *Let $A, B, m \in \mathbb{Z}$ with $AB \equiv 0 \pmod 3$, but $AB \not\equiv 0 \pmod 9$, and $m \not\equiv 0 \pmod 3$. Then $g(x) = x^3 + A^2x^2 - B^2x - m^2$ is irreducible.*

Proof By way of contradiction, assume that $g(x)$ is reducible and write

$$g(x) = (x - a)(x^2 + bx + c) = x^3 + (b - a)x^2 - (ab - c)x - ac.$$

Equating coefficients yields the system of Diophantine equations:

$$m^2 = ac, \tag{4.1}$$

$$B^2 = ab - c, \tag{4.2}$$

$$A^2 = b - a. \tag{4.3}$$

Since $m \not\equiv 0 \pmod 3$, we have from (4.1) that $a \equiv c \equiv 1 \pmod 3$ or $a \equiv c \equiv 2 \pmod 3$. Note that the hypotheses on A and B imply that

$$A^2 + B^2 \equiv 1 \pmod 3.$$

Hence, from (4.3) and (4.2), we have that

$$b - a + ab - c \equiv 1 \pmod 3, \tag{4.4}$$

which yields a contradiction if $a \equiv c \equiv 2 \pmod 3$. Therefore, $a \equiv c \equiv 1 \pmod 3$, and it follows from (4.4) that $b \equiv 0 \pmod 3$. But then we see from (4.2) that $B^2 \equiv 2 \pmod 3$, which is impossible. $\blacksquare$

https://doi.org/10.4153/CMB-2014-008-1 Published online by Cambridge University Press

The special case of Lemma 4.2 that is of interest to us here is $g(x) = x^3 + A^2x^2 - B^2x - m^2$ with $AB = 3m$ and $m \not\equiv 0 \pmod 3$. We therefore assume these conditions hold for the remainder of this section. Without loss of generality, we assume that $A, B, m \in \mathbb{Z}^+$.

We are now in a position to establish the irreducibility of $f(x)$ over $\mathbb{Q}$. Assume that $f(x)$ is reducible over $\mathbb{Q}$ so that $[F:\mathbb{Q}] < 6$. Since $g(x)$ is irreducible, we have that $[K:\mathbb{Q}] = 3$, and since $[K:\mathbb{Q}]$ divides $[F:\mathbb{Q}]$, we conclude that $[F:\mathbb{Q}] = 3$. Thus, θ is a zero of an irreducible cubic $h(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$. Note that $-\theta$ is a zero of $h(-x)$ and $f(x)$. Since $h(-x) \neq -h(x)$, it follows that

$$f(x) = -h(x)h(-x) = x^6 + (2b - a^2)x^4 - (2ac - b^2)x^2 - c^2.$$

Equating coefficients and including the restriction that $AB = 3m$ results in the following system of Diophantine equations:

$$A^2 = 2b - a^2, \tag{4.5}$$

$$B^2 = 2am - b^2, \tag{4.6}$$

$$AB = 3m. \tag{4.7}$$

Solving for b in (4.5) and for m in (4.7), and then substituting into (4.6) gives the single equation

$$\frac{3A^4 + 12B^2 + 6a^2A^2 + 3a^4}{4} = 2aAB. \tag{4.8}$$

Observe that $b > 0$ from (4.5), and $a > 0$ from (4.6), since $m > 0$. Hence, from (4.6) we have

$$3am > 2am = B^2 + b^2 > B^2. \tag{4.9}$$

Then, using the arithmetic-geometric mean inequality, (4.7) and (4.9), it follows that

$$\begin{aligned}\frac{3A^4 + 12B^2 + 6a^2A^2 + 3a^4}{4} &\geq \sqrt[4]{3A^4 \cdot 12B^2 \cdot 6a^2A^2 \cdot 3a^4} \\ &= 3\left(\sqrt[4]{8}\right) aA\left(\sqrt{aAB}\right) \\ &= 3\left(\sqrt[4]{8}\right) aA\left(\sqrt{3am}\right) \\ &> 3\left(\sqrt[4]{8}\right) aAB > 2aAB,\end{aligned}$$

which contradicts (4.8). Thus, $f(x)$ is irreducible.

We show now that $\Delta(g)$ is a square in $\mathbb{Z}$. Using the fact that $B = 3m/A$, we have

$$\begin{aligned}\Delta(g) &= -27m^4 + 18m^2A^2B^2 + A^4B^4 + 4A^6m^2 + 4B^6 \\ &= 216m^4 + 4A^6m^2 + 4\left(\frac{729m^6}{A^6}\right) \\ &= 4\left(\frac{m^2A^{12} + 54m^4A^6 + 729m^6}{A^6}\right) = 4\left(\frac{mA^6 + 27m^3}{A^3}\right)^2 \\ &= 4\left(mA^3 + \left(\frac{3m}{A}\right)^3\right)^2 = 4(mA^3 + B^3)^2,\end{aligned}$$

so that $\Delta(g)$ is a square in $\mathbb{Z}$.

https://doi.org/10.4153/CMB-2014-008-1 Published online by Cambridge University Press

Finally, $\Delta(f)$ is a square in $\mathbb{Z}$ by Lemma 4.1, and hence $\mathrm{Gal}(f) \simeq A_4$ by Corollary 1.2. This completes the proof for $\mathcal{F}_1$.

4.2 The Proof of Theorem 1.3 for $\mathcal{F}_2$

Let $d, m \in \mathbb{Z}$ and let $g(x) = x^3 + (d^2 + d + 4)m^2x^2 + 3m^4x - m^6$. Since

$$\widehat{g}(x) := (1/m^6)g(m^2x) = x^3 + (d^2 + d + 4)x^2 + 3x - 1$$

is irreducible by the Rational Zero theorem, it follows that $g(x)$ is also irreducible. To see that $f(x)$ is irreducible, we show that

$$\widehat{f}(x) := \widehat{g}(x^2) = x^6 + (d^2 + d + 4)x^4 + 3x^2 - 1 = (1/m^6)f(mxt)$$

is irreducible. It is easy to check that $\widehat{f}(x)$ is irreducible if $d \in \{-1, 0\}$. So, suppose that $d \notin \{-1, 0\}$ and assume, by way of contradiction, that $\widehat{f}(x)$ is reducible. Since $\widehat{g}(x)$ is irreducible, we may write, as in the proof for $\mathcal{F}_1$, that $\widehat{f}(x) = -h(x)h(-x)$, where $h(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$. Thus,

$$\widehat{f}(x) = -h(x)h(-x) = x^6 + (2b - a^2)x^4 - (2ac - b^2)x^2 - c^2.$$

Equating coefficients gives the following system of Diophantine equations:

$$c^2 = 1,$$

$$b^2 - 2ac = 3, \tag{4.10}$$

$$2b - a^2 = d^2 + d + 4. \tag{4.11}$$

Subtracting (4.11) from (4.10) and adding $c^2 + 1$ to both sides, we obtain

$$(b - 1)^2 + (c - a)^2 = -d^2 - d + 1,$$

which is impossible, since $-d^2 - d + 1 < 0$ for all $d \notin \{-1, 0\}$. Thus, $\widehat{f}(x)$, and hence $f(x)$, is irreducible.

From Lemma 4.1, we have that $\Delta(f)$ is a square in $\mathbb{Z}$, and a simple computation gives

$$\Delta(g) = m^{12}(d^2 + d + 7)^2(2d + 1)^2,$$

which completes the proof for $\mathcal{F}_2$.

4.3 The Proof of Theorem 1.3 for $\mathcal{F}_3$

Let $d, m \in \mathbb{Z}$ with m odd, and let $g(x) = x^3 + (d + 3m^2)x^2 + dm^2x - m^6$. We show first that $g(x)$ is irreducible. Let $\Delta := \Delta(g)$ and let p be an odd prime such that $p \nmid \Delta$. Since

$$\Delta = m^4(d^2 + 3dm^2 + 9m^4)^2,$$

we have that $(\Delta/p) = 1$. On the other hand, Theorem 2.3 implies that $(\Delta/p) = (-1)^{3-k}$, where k is the number of irreducible monic factors of $g(x)$ modulo p. Thus $k = 1$ or $k = 3$. If $k = 1$, then $g(x)$ is irreducible modulo p, and hence irreducible over $\mathbb{Q}$. So, assume that $k = 3$ for all odd primes $p \nmid \Delta$. That is, $g(x)$ factors

https://doi.org/10.4153/CMB-2014-008-1 Published online by Cambridge University Press

completely into linear factors modulo all such primes. Therefore, by the Chebotarëv density theorem, $g(x)$ factors completely into linear factors in $\mathbb{Z}[x]$. Thus

$$g(x) = (x-a)(x-b)(x-c) = x^3 - (a+b+c)x^2 + (ab+ac+bc)x - abc$$

for some $a, b, c \in \mathbb{Z}$. Equating coefficients gives the system of Diophantine equations:

$$m^6 = abc, \tag{4.12}$$

$$dm^2 = ab + ac + bc, \tag{4.13}$$

$$d + 3m^2 = -(a+b+c), \tag{4.14}$$

Since m is odd, we see from (4.12) that a, b, and c are odd, which implies that $a+b+c$ and $ab+ac+bc$ are also odd. Thus, if d is odd, then $d+3m^2$ is even, which contradicts (4.14), and if d is even, then dm^2 is even, which contradicts (4.13). Hence, $g(x)$ is irreducible.

To establish the irreducibility of $f(x)$, we assume that $f(x)$ is reducible and proceed as in the previous cases. Since $g(x)$ is irreducible, we may write $f(x) = -h(x)h(-x)$, where $h(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$. Thus,

$$f(x) = -h(x)h(-x) = x^6 + (2b - a^2)x^4 - (2ac - b^2)x^2 - c^2$$

and, equating coefficients, we arrive at the following system of Diophantine equations:

$$m^6 = c^2, \tag{4.15}$$

$$dm^2 = b^2 - 2ac, \tag{4.16}$$

$$d + 3m^2 = 2b - a^2. \tag{4.17}$$

Subtracting (4.16) from (4.17) we get

$$d + 3m^2 - dm^2 = 2b - a^2 - b^2 + 2ac. \tag{4.18}$$

Note from (4.15) that c is odd, since m is odd. Hence, reduction modulo 4 of (4.18) yields

$$3 \equiv 2b - a^2 - b^2 + 2a \pmod 4,$$

which can be rewritten as

$$3 \equiv (a-1)^2 + (b-1)^2 \pmod 4. \tag{4.19}$$

Since (4.19) is easily seen to be impossible, we deduce that $f(x)$ is irreducible.

An easy computation gives

$$\Delta(g) = m^4(d^2 + 3dm^2 + 9m^4)^2,$$

and $\Delta(f)$ is also a square in $\mathbb{Z}$ by Lemma 4.1. This case then follows from Corollary 1.2, which completes the proof of the theorem. ∎

Remark 4.3 The family $\mathcal{F}_3$ is given in [S] but the proof uses resolvents. A proper subset of $\mathcal{F}_3$ is handled in [ESW] without the use of resolvents.

https://doi.org/10.4153/CMB-2014-008-1 Published online by Cambridge University Press

5 Proof of Theorem 1.4

Let $a, b, c \in \mathbb{Z}$. Let $f(x) = x^6 - bx^4 + acx^2 - c^2$, and assume that $f(x)$ is irreducible. Let $g(x) = x^3 + ax^2 + bx + c$ and assume that $\Delta(g)$ is a square in $\mathbb{Z}$. Let ϕ_1, ϕ_2 and ϕ_3 be the zeros of $g(x)$, so that

$$\begin{aligned} a &= -(\phi_1 + \phi_2 + \phi_3), \\ b &= \phi_1\phi_2 + \phi_1\phi_3 + \phi_2\phi_3, \\ c &= -\phi_1\phi_2\phi_3. \end{aligned}$$

Then

$$\begin{aligned} f\big(\sqrt{\phi_1\phi_2}\big) &= (\phi_1\phi_2)^3 - b(\phi_1\phi_2)^2 + ac(\phi_1\phi_2) - c^2 \\ &= (\phi_1\phi_2)^3 - (\phi_1\phi_2 + \phi_1\phi_3 + \phi_2\phi_3)(\phi_1\phi_2)^2 \\ &\quad + (\phi_1 + \phi_2 + \phi_3)(\phi_1\phi_2\phi_3)(\phi_1\phi_2) - (\phi_1\phi_2\phi_3)^2 = 0, \end{aligned}$$

which implies that

$$\big[\mathbb{Q}\big(\sqrt{\phi_1\phi_2}\big) : \mathbb{Q}\big] = 6, \tag{5.1}$$

since $f(x)$ is irreducible.

We show now that $g(x)$ is irreducible. By way of contradiction, assume that $g(x)$ is reducible. Since $\Delta(g)$ is a square in $\mathbb{Z}$, we have by Theorem 2.1 that $g(x)$ splits completely over $\mathbb{Q}$ so that $\phi_1, \phi_2, \phi_3 \in \mathbb{Q}$. But then $[\mathbb{Q}(\sqrt{\phi_1\phi_2}) : \mathbb{Q}] \leq 2$, which contradicts (5.1). Hence, $g(x)$ is irreducible.

Note that $\mathbb{Q}(\sqrt{\phi_1\phi_2})$ contains $-c/\phi_1\phi_2 = \phi_3$, and since $g(x)$ is irreducible, we have that $\mathbb{Q}(\phi_3)$ is a cubic subfield of $\mathbb{Q}(\sqrt{\phi_1\phi_2})$. Finally, since

$$\Delta(f) = 2^6c^6(27c^2 + 4b^3 + 4a^3c - 18abc - a^2b^2)^2,$$

it follows from Theorem 1.1 that $\mathrm{Gal}(f) \simeq A_4$.

To complete the proof of the theorem, we must show that the set $\mathcal{F}_4$ is infinite. Observe that $x^6 + 9x^4 - 16x^2 - 16 \in \mathcal{F}_4 \cap \mathcal{F}_1$. On the other hand, $x^6 + 9x^4 - 256x^2 - 256 \in \mathcal{F}_4 - \mathcal{F}_1$. In fact, we claim that $f(x) = x^6 + 9x^4 - c^2x^2 - c^2 \in \mathcal{F}_4 - \mathcal{F}_1$ for all $c \in \mathbb{Z}$ with $c \not\equiv 0 \pmod 3$. It is clear that $f(x) \notin \mathcal{F}_1$. To establish the claim, it is then enough to show that $f(x)$ is irreducible, since $\Delta(g) = 4(c^2 + 27)^2$, where $g(x) = x^3 + cx^2 - 9x - c$.

We proceed as in the proof of Theorem 1.3 and show first that $g(x)$ is irreducible. By way of contradiction, assume that $g(x)$ is reducible and write

$$g(x) = (x + r)(x^2 + sx + t) = x^3 + (r + s)x^2 + (rs + t)x + rt,$$

for some $r, s, t \in \mathbb{Z}$. Equating coefficients gives the system of Diophantine equations:

$$rt = -c, \tag{5.2}$$

$$rs + t = -9, \tag{5.3}$$

$$r + s = c. \tag{5.4}$$

Combining (5.2) and (5.4) to eliminate c, solving for s, and substituting back into (5.3) yields $r^2 = 1 + 8/(t + 1)$, which implies that $t + 1$ divides 8 and $t \geq 0$. Clearly, $g(0) \neq 0$, so $t \neq 0$. Hence, $t \in \{1, 3, 7\}$. But then $r^2 \in \{5, 3, 2\}$, which is impossible. Thus, $g(x)$ is irreducible.

https://doi.org/10.4153/CMB-2014-008-1 Published online by Cambridge University Press

Recall from above that if ϕ_1, ϕ_2, and ϕ_3 are the zeros of $g(x)$, then $f(\sqrt{\phi_1\phi_2}) = 0$. Also, F contains K, where $F = \mathbb{Q}(\sqrt{\phi_1\phi_2})$ and $K = \mathbb{Q}(\phi_3)$. Assume that $f(x)$ is reducible so that $[F:\mathbb{Q}] < 6$. Since $g(x)$ is irreducible, we have that $[K:\mathbb{Q}] = 3$, and since $[K:\mathbb{Q}]$ divides $[F:\mathbb{Q}]$, we conclude that $[F:\mathbb{Q}] = 3$. Thus, $\sqrt{\phi_1\phi_2}$ is a zero of an irreducible cubic $h(x) = x^3 + rx^2 + sx + t \in \mathbb{Z}[x]$. Note that $-\sqrt{\phi_1\phi_2}$ is a zero of $h(-x)$ and $f(x)$. Since $h(-x) \neq -h(x)$, it follows that

$$f(x) = -h(x)h(-x) = x^6 + (2s - r^2)x^4 - (2rt - s^2)x^2 - t^2.$$

Equating coefficients results in the following system of Diophantine equations:

$$t^2 = c^2, \tag{5.5}$$

$$2rt - s^2 = c^2, \tag{5.6}$$

$$2s - r^2 = 9. \tag{5.7}$$

Equating (5.5) and (5.6), adding the resulting equation to (5.7), and completing the square on s, and then on r and t gives

$$-(s-1)^2 - (r-t)^2 = 8,$$

which is impossible. Hence, $f(x)$ is irreducible, and the proof of the theorem is complete. ∎

Acknowledgments The authors thank the referee for providing suggestions that helped to shorten some proofs.

References

[C] H. Cohen, *A course in computational algebraic number theory*. Graduate Texts in Mathematics, 138, Springer-Verlag, Berlin, 2000.

[ESW] D. Eloff, B. K. Spearman, and K. S. Williams, *A_4-sextic fields with a power basis*. Missouri J. Math. Sci. **19**(2007), no. 3, 188–194.

[MM] G. Malle and B. H. Matzat, *Inverse Galois theory*. Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999.

[S] G. W. Smith, *Some polynomials over $\mathbb{Q}(t)$ and their galois groups*. Math. Comp. **69**(2000), no. 230, 775–796. http://dx.doi.org/10.1090/S0025-5718-99-01160-6

Department of Mathematics, Shippensburg University, Shippensburg, PA 17257, USA
e-mail: joshua.ide12@gmail.com lkjone@ship.edu