ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 26, Number 2, Spring 1996

# ON SOLVABLE QUINTICS $X^5 + aX + b$ AND $X^5 + aX^2 + b$

BLAIR K. SPEARMAN AND KENNETH S. WILLIAMS

ABSTRACT. Let $a$ and $b$ be nonzero rational numbers. We show that there are an infinite number of essentially different, irreducible, solvable, quintic trinomials $X^5 + aX + b$. On the other hand, we show that there are only five essentially different, irreducible, solvable, quintic trinomials $X^5 + aX^2 + b$, namely, $X^5 + 5X^2 + 3$, $X^5 + 5X^2 - 15$, $X^5 + 25X^2 + 300$, $X^5 + 100X^2 + 1000$, and $X^5 + 250X^2 + 625$.

**1. Introduction.** Let $Q$ denote the field of rational numbers, set $Q^* = Q\backslash\{0\}$, and let $f(X)$ be a monic irreducible quintic polynomial in $Q[X]$. If the equation $f(x) = 0$ is solvable by radicals, the quintic polynomial $f(X)$ is said to be solvable. If $f(X)$ is solvable, its Galois group is solvable and is thus contained in the Frobenius group $F_{20}$ of order 20, and hence is isomorphic to $F_{20}$, $D_5$ (the dihedral group of order 10) or $C_5$ (the cyclic group of order 5). It is also known that the discriminant of a solvable quintic is always positive [1, p. 390].

Now let $f_i(X) = X^5 + aX^i + b \in Q^*[X]$, $i = 1, 2$, be irreducible and solvable. As disc $(f_i(x)) > 0$, $f_i(X)$ has exactly one real root [4, p. 113]. Thus, $f_i(X)$ has nonreal roots and so its Galois group cannot be cyclic and thus must be $F_{20}$ or $D_5$. For $i = 1, 2$, we define $F(i)$ to be the set of irreducible solvable trinomials $X^5 + aX^i + b$ with Galois group isomorphic to $F_{20}$ and $D(i)$ to be the set of irreducible solvable trinomials $X^5 + aX^i + b$ with Galois group isomorphic to $D_5$.

We define an equivalence relation on each of $F(i)$ and $D(i)$ as follows: $X^5 + aX^i + b \in F(i)$, or $D(i)$, and $X^5 + a_1X^i + b_1 \in F(i)$, or $D(i)$, are said to be equivalent (written $X^5 + aX^i + b \sim X^5 + a_1X^i + b_1$) if there exists $t \in Q^*$ such that $a_1 = at^{5-i}$, $b_1 = bt^5$, in which case $X^5 + a_1X^i + b_1 = t^5((X/t)^5 + a(X/t)^i + b)$. We denote the set of equivalence classes of $F(i)$ by $\mathcal{F}(i)$ and those of $D(i)$ by $\mathcal{D}(i)$. In Section 2 we prove

Received by the editors on April 29, 1994.
1991 AMS *Mathematics Subject Classification.* Primary 12D05.
*Key words and phrases.* Solvable, irreducible, quintic trinomials, Galois group.
Research of the second author supported by Natural Sciences and Engineering Research Council of Canada grant A-7233.

**Theorem 1.**

(i) $\operatorname{card} \mathcal{F}(1) = +\infty$,

(ii) $\operatorname{card} \mathcal{D}(1) = +\infty$.

In Section 3, in remarkable contrast to Theorem 1, we prove

**Theorem 2.**

(i) $\operatorname{card} \mathcal{F}(2) = 2$,

(ii) $\operatorname{card} \mathcal{D}(2) = 3$.

The proof of Theorem 1 depends heavily on the following result which was proved in [3].

**Proposition.** *Let $a, b \in Q^*$ be such that the quintic trinomial $X^5 + aX + b$ is irreducible. Then $X^5 + aX + b$ is solvable if and only if there exist rational numbers $\varepsilon(= \pm 1)$, $c(\geq 0)$ and $e(\neq 0)$ such that*

$$a = \frac{5e^4(3 - 4\varepsilon c)}{c^2 + 1}, \qquad b = \frac{-4e^5(11\varepsilon + 2c)}{c^2 + 1}.$$

*Moreover, the Galois group of $X^5 + aX + b$ is isomorphic to $F_{20}$ if $5(c^2 + 1)$ is not a square in $Q$ and to $D_5$ if $5(c^2 + 1)$ is a square in $Q$.*

The proof of Theorem 2 makes use of the theory of rational points on elliptic curves. We actually prove the following theorem from which Theorem 2 follows immediately.

**Theorem 3.** *Let $a, b \in Q^*$ be such that the quintic polynomial $X^5 + aX^2 + b$ is both irreducible and solvable. Then there exists a nonzero rational number $f$ such that*

$$(af^3, bf^5) = (5,3), (5,-15), (25,300), (100,1000) \text{ or } (250,625).$$

*Moreover, the Galois group of $X^5 + aX^2 + b$ is*

$$\begin{cases} D_5 & \text{if } (af^3, bf^5) = (5,3), (5,-15) \text{ or } (25,300), \\ F_{20} & \text{if } (af^3, bf^5) = (100,1000) \text{ or } (250,625). \end{cases}$$

*Let $\omega$ denote a complex fifth root of unity. Then the five solutions of $x^5 + ax^2 + b = 0$ are*

$$x/f = \omega^j u_1 + \omega^{2j} u_2 + \omega^{3j} u_3 + \omega^{4j} u_4, \qquad j = 0, 1, 2, 3, 4,$$

*where $u_1, u_2, u_3$ and $u_4$ are given as follows:*

(i) $(af^3, bf^5) = (5, 3)$

$$u_1 = \left( -\frac{1}{4} + \frac{1}{20}\sqrt{5} - \frac{1}{100}\sqrt{150 + 30\sqrt{5}} + \frac{1}{50}\sqrt{150 - 30\sqrt{5}} \right)^{1/5},$$
$$u_2 = \left( -\frac{1}{4} - \frac{1}{20}\sqrt{5} - \frac{1}{50}\sqrt{150 + 30\sqrt{5}} - \frac{1}{100}\sqrt{150 - 30\sqrt{5}} \right)^{1/5},$$
$$u_3 = \left( -\frac{1}{4} - \frac{1}{20}\sqrt{5} + \frac{1}{50}\sqrt{150 + 30\sqrt{5}} + \frac{1}{100}\sqrt{150 - 30\sqrt{5}} \right)^{1/5},$$
$$u_4 = \left( -\frac{1}{4} + \frac{1}{20}\sqrt{5} + \frac{1}{100}\sqrt{150 + 30\sqrt{5}} - \frac{1}{50}\sqrt{150 - 30\sqrt{5}} \right)^{1/5};$$

(ii) $(af^3, bf^5) = (5, -15)$

$$u_1 = \left( \frac{5}{4} + \frac{13}{20}\sqrt{5} - \frac{7}{100}\sqrt{750 + 330\sqrt{5}} \right)^{1/5},$$
$$u_2 = \left( \frac{5}{4} - \frac{13}{20}\sqrt{5} - \frac{7}{100}\sqrt{750 - 330\sqrt{5}} \right)^{1/5},$$
$$u_3 = \left( \frac{5}{4} - \frac{13}{20}\sqrt{5} + \frac{7}{100}\sqrt{750 - 330\sqrt{5}} \right)^{1/5},$$
$$u_4 = \left( \frac{5}{4} + \frac{13}{20}\sqrt{5} + \frac{7}{100}\sqrt{750 + 330\sqrt{5}} \right)^{1/5};$$

(iii) $(af^3, bf^5) = (25, 300)$

$$u_1 = \left( -\frac{25}{2} - \frac{5}{2}\sqrt{5} - \frac{5}{2}\sqrt{30 + 6\sqrt{5}} \right)^{1/5},$$

$$u_2 = \left( -\frac{25}{2} + \frac{5}{2}\sqrt{5} - \frac{5}{2}\sqrt{30 - 6\sqrt{5}} \right)^{1/5},$$

$$u_3 = \left( -\frac{25}{2} + \frac{5}{2}\sqrt{5} + \frac{5}{2}\sqrt{30 - 6\sqrt{5}} \right)^{1/5},$$

$$u_4 = \left( -\frac{25}{2} - \frac{5}{2}\sqrt{5} + \frac{5}{2}\sqrt{30 + 6\sqrt{5}} \right)^{1/5};$$

(iv) $(af^3, bf^5) = (100, 1000)$

$$u_1 = -2^{6/5}, \qquad u_2 = -2^{7/5}, \qquad u_3 = 2^{3/5}, \qquad u_4 = -2^{4/5};$$

(v) $(af^3, bf^5) = (250, 625)$

$$u_1 = (-125 + 50\sqrt{5})^{1/5}, \qquad u_2 = \left( \frac{-375 - 175\sqrt{5}}{2} \right)^{1/5},$$

$$u_3 = \left( \frac{-375 + 175\sqrt{5}}{2} \right)^{1/5}, \qquad u_4 = (-125 - 50\sqrt{5})^{1/5}.$$

## 2. Solvable quintics $X^5 + aX + b$.

*Proof of Theorem* 1(i). We let $L$ be the set of positive integers $l$ such that $25000l + 21603$ is prime. As $\mathrm{GCD}\,(25000, 21603) = 1$, the set $L$ is an infinite set by Dirichlet's theorem. For $l \in L$, we let

$$p_l = 25000l + 21603 \text{ (prime)},$$
$$c_l = 12500l + 10807,$$
$$\varepsilon_l = -1,$$

and $e_l$ is the smallest positive integer $e$ such that $e^4/(c_l^2 + 1)$ is an integer. Clearly the prime $p_l$ satisfies $p_l \equiv 3 \pmod 4$, $p_l \equiv 3 \pmod 5$,

and $11\varepsilon_l + 2c_l = p_l$. Further, $c_l \equiv 1432 \pmod{3125}$ so that $c_l^2 + 1 \equiv 1432^2 + 1 \equiv 625 \pmod{3125}$, that is, $5^4 \| c_l^2 + 1$, and hence $5 \| e_l$. As $e_l^4/(c_l^2 + 1)$ is an integer not divisible by 5, the rational numbers

$$a_l = \frac{5e_l^4(3 - 4\varepsilon_l c_l)}{c_l^2 + 1}, \qquad b_l = \frac{-4e_l^5(11\varepsilon_l + 2c_l)}{c_l^2 + 1},$$

are in fact integers satisfying $5|a_l$, $5\|b_l$, so that $X^5 + a_l X + b_l$ is 5-Eisenstein, and thus irreducible. By the Proposition in Section 1, $X^5 + a_l X + b_l$ is solvable. Moreover, $5^5 \| 5(c_l^2 + 1)$, so $5(c_l^2 + 1)$ is not a square, and thus $X^5 + a_l X + b_l$ has Galois group $F_{20}$. Finally, we show that if $l(\in L)$ and $l_1(\in L)$ are distinct, then $X^5 + a_l X + b_l \not\sim X^5 + a_{l_1} X + b_{l_1}$. This proves that card $(\mathcal{F}(1)) = +\infty$ as $L$ is an infinite set. Suppose on the contrary that $l \neq l_1$ but $X^5 + a_l X + b_l \sim X^5 + a_{l_1} X + b_{l_1}$. Then there exist nonzero coprime integers $r$ and $s$ such that

$$a_{l_1} = a_l \left(\frac{r}{s}\right)^4, \qquad b_{l_1} = b_l \left(\frac{r}{s}\right)^5.$$

From the second of these equations, we obtain

$$\frac{-4e_{l_1}^5(11\varepsilon_{l_1} + 2c_{l_1})}{c_{l_1}^2 + 1} = \frac{-4e_l^5(11\varepsilon_l + 2c_l)}{c_l^2 + 1} \frac{r^5}{s^5},$$

that is,

$$e_{l_1}^5 p_{l_1}(c_l^2 + 1)s^5 = e_l^5 p_l(c_{l_1}^2 + 1)r^5.$$

As $l \neq l_1$ we have $p_l \neq p_{l_1}$. Further, as $p_l \equiv 3 \pmod 4$, we see that $p_l \nmid c_l^2 + 1$, so $p_l \nmid e_l$, and $p_l \nmid c_{l_1}^2 + 1$, so $p_l \nmid e_{l_1}$. Hence,

$$v_{p_l}(e_{l_1}^5 p_{l_1}(c_l^2 + 1)s^5) = 5v_{p_l}(s) \equiv 0 \pmod 5$$

and

$$v_{p_l}(e_l^5 p_l(c_{l_1}^2 + 1)r^5) = 1 + 5v_{p_l}(r) \equiv 1 \pmod 5,$$

a contradiction. This completes the proof that card $\mathcal{F}(1) = +\infty$. □

*Proof of Theorem* 1(ii). We let

$$P = \text{set of primes } p \equiv 17 \pmod{20}. \tag{2.1}$$

By Dirichlet's theorem $P$ is an infinite set. Let $p \in P$. Clearly, $p \neq 5$. As $p \equiv 1 \pmod 4$, there exist unique integers $a$ and $b$ such that

$$p = a^2 + b^2, \quad a > 0, b > 0, a \text{ odd }, b \text{ even}. \tag{2.2}$$

As $p \equiv 2 \pmod 5$, we have $a^2 \equiv b^2 \equiv 1 \pmod 5$ so that $5 \nmid a$ and $5 \nmid b$. If $3a + 4b \not\equiv 0 \pmod 5$, we set $\varepsilon = 1$. If $3a + 4b \equiv 0 \pmod 5$, then $3a - 4b \equiv -8b \not\equiv 0 \pmod 5$, and we set $\varepsilon = -1$. Hence, $3a + \varepsilon 4b \not\equiv 0 \pmod 5$. Define integers $u$ and $v$ by

$$u = 3a + \varepsilon 4b, \qquad v = 4a - \varepsilon 3b. \tag{2.3}$$

Then, appealing to (2.2) and (2.3), we see that

$$u^2 + v^2 = 25p, \quad 5 \nmid u, 5 \nmid v. \tag{2.4}$$

Further, from (2.3), we deduce

$$3u^2 + 8uv - 3v^2 = 75a^2 + 200\varepsilon ab - 75b^2 \equiv 0 \pmod 5,$$

so that by (2.4)

$$3u^2 - 8uv - 3v^2 \equiv -16uv \not\equiv 0 \pmod 5. \tag{2.5}$$

Also, by (2.3), we see that

$$u - 2v = -5a + 10\varepsilon b \equiv 0 \pmod 5,$$

so that, as $5 \nmid v$, we deduce

$$5 || (u - 2v)^2 - 5v^2,$$

that is,

$$5 || u^2 - 4uv - v^2, \tag{2.6}$$

and hence

$$u^2 + 4uv - v^2 \equiv 8uv \not\equiv 0 \pmod 5. \tag{2.7}$$

We also note that

$$2u^2 + 2uv - 2v^2 = (1/2)((2u+v)^2 - 5v^2) \neq 0,$$
$$u^2 - 4uv - v^2 = (u-2v)^2 - 5v^2 \neq 0.$$

Hence, we can define rationals $c_p, \varepsilon_p$ and $e_p$ by

$$c_p = \left| \frac{2u^2 + 2uv - 2v^2}{u^2 - 4uv - v^2} \right| > 0,$$
$$\varepsilon_p = \operatorname{sgn}\left( \frac{2u^2 + 2uv - 2v^2}{u^2 - 4uv - v^2} \right) = \pm 1,$$
$$e_p = \frac{1}{5}\varepsilon_p(u^2 + v^2) = 5\varepsilon_p p.$$

Clearly,

$$\varepsilon_p c_p = \frac{2u^2 + 2uv - 2v^2}{u^2 - 4uv - v^2}, \qquad c_p^2 + 1 = \frac{5(u^2+v^2)^2}{(u^2 - 4uv - v^2)^2}.$$

Now set

$$a_p = \frac{5e_p^4(3 - 4\varepsilon_p c_p)}{c_p^2 + 1}, \qquad b_p = \frac{-4e_p^5(11\varepsilon_p + 2c_p)}{c_p^2 + 1},$$

so that

$$a_p = -5p^2(u^2 + 4uv - v^2)(u^2 - 4uv - v^2) \in Z,$$
$$b_p = -20p^3(u^2 - 4uv - v^2)(3u^2 - 8uv - 3v^2) \in Z.$$

We claim that the polynomial $f_p(x) = X^5 + a_p X + b_p$ is irreducible in $Q[X]$. Suppose on the contrary that $f_p(X)$ is reducible in $Q[X]$. Then either (a) $f_p(X)$ has an integral root $r$ or (b) $f_p(X)$ is the product of an irreducible quadratic and an irreducible cubic. Suppose (a) holds. Then

$$(2.8) \quad r^5 - 5p^2(u^2 + 4uv - v^2)(u^2 - 4uv - v^2)r - 20p^3(u^2 - 4uv - v^2)(3u^2 - 8uv - 3v^2) = 0,$$

and clearly $5|r$. Now, appealing to (2.5), (2.6) and (2.7),

$$v_5(r^5) \geq 5,$$
$$v_5(-5p^2(u^2+4uv-v^2)(u^2-4uv-v^2)r) \geq 1+0+0+1+1 = 3,$$
$$v_5(-20p^3(u^2-4uv-v^2)(3u^2-8uv-3v^2)) = 1+0+1+0 = 2,$$

contradicting (2.8). Hence, (a) cannot occur. If (b) holds, let $E$ denote the splitting field of $f_p(X)$ over $Q$. As $f_p(X)$ has an irreducible cubic factor we must have $3|[E:Q]$. However, by the theorem in [3] we see that $E/Q$ can be constructed using only square roots and fifth roots, so that $[E:Q] = 2^k5^m$ for some nonnegative integers $k$ and $m$, a contradiction. Hence (b) cannot occur. Thus, $f_p(X)$ is irreducible in $Q[X]$ and, by the Proposition in Section 1, $f_p(X)$ is solvable with Galois group $D_5$ since $5(c_p^2+1)$ is a square in $Q$.

Finally we show that if $p(\in P)$ and $p_1(\in P)$ are distinct, then $X^5+a_pX+b_p \not\sim X^5+a_{p_1}X+b_{p_1}$. This then proves that card $\mathcal{D}(1) = +\infty$. Suppose, however, that $X^5+a_pX+b_p \sim X^5+a_{p_1}X+b_{p_1}$. Then there exist nonzero coprime integers $r$ and $s$ such that

$$a_{p_1} = a_p\left(\frac{r}{s}\right)^4, \qquad b_{p_1} = b_p\left(\frac{r}{s}\right)^5. \tag{2.9}$$

Let $u_1$ and $v_1$ be the values of $u$ and $v$ corresponding to $p_1$. From the first equation in (2.9), we see that

$$p_1^2(u_1^2+4u_1v_1-v_1^2)(u_1^2-4u_1v_1-v_1^2)s^4 = p^2(u^2+4uv-v^2)(u^2-4uv-v^2)r^4. \tag{2.10}$$

As $p \equiv 2 \pmod 5$, we have, by the law of quadratic reciprocity, $(5/p) = (p/5) = (2/5) = -1$. Hence, as $p \nmid v$, we see that $p \nmid (u \pm 2v)^2 - 5v^2$, that is,

$$p \nmid u^2 \pm 4uv - v^2.$$

As $u_1^2+v_1^2 = 25p_1$ and $p \neq 5$ or $p_1$, we see that at last one of $u_1$ and $v_1$ is not divisible by $p$. If $p \nmid u_1$, then $p \nmid 5u_1^2-(v_1 \mp 2u_1)^2$, as $(5/p) = -1$, so

$$p \nmid u_1^2 \pm 4u_1v_1 - v_1^2.$$

If $p \nmid v_1$, then $p \nmid (u_1 \pm 2v_1)^2 - 5v_1^2$, as $(5/p) = -1$, so again we have

$$p \nmid u_1^2 \pm 4u_1v_1 - v_1^2.$$

Then from (2.10) we see that $p \mid s$ and thus $p \nmid r$. Hence,

$$v_p(p_1^2(u_1^2 + 4u_1v_1 - v_1^2)(u_1^2 - 4u_1v_1 - v_1^2)s^4) = 4v_p(s) \geq 4$$

and

$$v_p(p^2(u^2 + 4uv - v^2)(u^2 - 4uv - v^2)r^4) = 2,$$

a contradiction. This completes the proof that $\operatorname{card} \mathcal{D}(1) = +\infty$. □

**3. Solvable quintics $X^5 + aX^2 + b$.** Let $a, b \in Q^*$ be such that the quintic polynomial $X^5 + aX^2 + b$ is both irreducible and solvable. Its discriminant is

$$d = 108a^5b + 3125b^4 > 0. \tag{3.1}$$

We first show that there exists $f \in Q^*$ such that

$$(af^3, bf^5) = (5,3), (5,-15), (25,300), (100,1000) \text{ or } (250,625). \tag{3.2}$$

As $X^5 + aX^2 + b$ is a solvable quintic, its resolvent sextic

$$X^6 - 50abX^4 - 2a^4X^3 + 625a^2b^2X^2 + (-58a^5b - 3125b^4)X + a^8 \tag{3.3}$$

has exactly one rational root $R$ [1, Theorem 1]. Hence,

$$R^6 - 50abR^4 - 2a^4R^3 + 625a^2b^2R^2 + (-58a^5b - 3125b^4)R + a^8 = 0, \tag{3.4}$$

which shows that $R \neq 0$ as $a \neq 0$. Moreover, from (3.1) and (3.4), we deduce

$$(R^3 - 25abR - a^4)^2 = dR, \tag{3.5}$$

so that $R > 0$, and $d$ is a perfect square if and only if $R$ is a perfect square. We set

$$U = 50bR^2 - 6a^3R - 125ab^2 \tag{3.6}$$

and

$$V = 5R^3 - 25abR + a^4. \tag{3.7}$$

Using MAPLE one can verify that

$$aRU^2 - 4R^2UV + (-5a^3 + 40bR)V^2 = 0 \tag{3.8}$$

and

$$5R^2U^4 - 50a^2RU^2V^2 + 64aR^2UV^3 + (125a^4 - 16R^3)V^4 = 0. \tag{3.9}$$

We show next that $V \neq 0$. Suppose $V = 0$. From (3.8) we see that $U = 0$. then

$$(3125ab^3 - 18a^6)R - 625a^4b^2 = (25bR + 3a^3)U - 250b^2V = 0.$$

As $a \neq 0$, $b \neq 0$, $R \neq 0$, we see that $3125ab^3 - 18a^6 \neq 0$, and so

$$R = \frac{625a^3b^2}{3125b^3 - 18a^5}.$$

Using this value of $R$ in (3.6) with $U = 0$, we obtain

$$216a^{10} + 175000a^5b^3 - 9765625b^6 = 0,$$

so that

$$\frac{a^5}{125b^3} = \frac{-350 \pm 125\sqrt{10}}{108},$$

which contradicts that $a^5/125b^3$ is rational. This proves that $V \neq 0$, and so we can define a rational number $A$ by

$$A = \frac{U}{V} = \frac{50bR^2 - 6a^3R - 125ab^2}{5R^3 - 25abR + a^4}. \tag{3.10}$$

From (3.8) and (3.9), we deduce that

$$4AR/5 - A^2a/5 + a^3/R = 8b \tag{3.11}$$

and

$$\left(\frac{A^2}{4} - \frac{5a^2}{4R}\right)^2 = -\frac{4Aa}{5} + \frac{R}{5}. \tag{3.12}$$

We now treat the possibility that $A = 0$. In this case (3.11) and (3.12) become

$$\frac{a^3}{R} = 8b, \qquad \frac{25a^4}{16R^2} = \frac{R}{5}.$$

Eliminating $R$ we deduce $a^5 = 4000b^3$, so that for some rational number $f$ we have $af^3 = 250$, $bf^5 = 625$, which is the last possibility in (3.2).

Hence we can now suppose that $A \neq 0$, and define the nonzero rational number $x$ by

$$x = -\frac{aA}{R}. \tag{3.13}$$

Replacing $a$ by $-xR/A$ in (3.12), we obtain

$$\left(\frac{A^2}{4} - \frac{5x^2R}{4A^2}\right)^2 = \frac{4xR}{5} + \frac{R}{5}. \tag{3.14}$$

Expanding the square in (3.14) and rearranging, we deduce

$$\left(\frac{25x^4}{16A^4}\right)R^2 - \left(\frac{5x^2}{8} + \frac{4x}{5} + \frac{1}{5}\right)R + \frac{A^4}{16} = 0. \tag{3.15}$$

Solving the quadratic equation (3.15) for $R$, we have

$$R = \frac{8A^4}{25x^4}\left(\frac{5x^2}{8} + \frac{4x}{5} + \frac{1}{5} \pm \sqrt{x^3 + \frac{89}{100}x^2 + \frac{8}{25}x + \frac{1}{25}}\right). \tag{3.16}$$

Since $R$, $A$ and $x$ are all rational numbers, the quantity

$$\pm\sqrt{x^3 + (89/100)x^2 + (8/25)x + (1/25)}$$

in (3.16) must be a rational number, say $y$, that is

$$y = \pm\sqrt{x^3 + \frac{89}{100}x^2 + \frac{8}{25}x + \frac{1}{25}}, \tag{3.17}$$

and so

$$y^2 = x^3 + \frac{89}{100}x^2 + \frac{8}{25}x + \frac{1}{25}. \tag{3.17$'$}$$

From (3.16) and (3.17), we see that

$$R = \frac{8A^4}{25x^4}\left(\frac{5x^2}{8} + \frac{4x}{5} + \frac{1}{5} + y\right). \tag{3.18}$$

We note from (3.13) and (3.18) that

$$\frac{a}{A^3} = -\frac{8}{25x^3}\left(\frac{5x^2}{8} + \frac{4x}{5} + \frac{1}{5} + y\right), \tag{3.19}$$

and from (3.11), (3.18) and (3.19) that

$$\frac{b}{A^5} = \left(\frac{4}{125x^4} + \frac{1}{125x^3}\right)\left(\frac{5x^2}{8} + \frac{4x}{5} + \frac{1}{5} + y\right) - \frac{8}{625x^5}\left(\frac{5x^2}{8} + \frac{4x}{5} + \frac{1}{5} + y\right)^2.$$

We now turn to the problem of determining all pairs $(x, y) \in Q^* \times Q$ satisfying (3.17)′. We define rational numbers $Z$ and $Y$ by

$$Z = 100x(\neq 0), \qquad Y = 1000y. \tag{3.21}$$

Replacing $x$ by $Z/100$ and $y$ by $Y/1000$ in (3.17)′, we see that

$$Y^2 = Z^3 + 89Z^2 + 3200Z + 40000. \tag{3.22}$$

Now define a rational number $X$ by

$$X = Z + 25. \tag{3.23}$$

Replacing $Z$ by $X - 25$ in (3.22), we obtain

$$Y^2 = X^3 + 14X^2 + 625X. \tag{3.24}$$

The cubic equation

$$X^3 + 14X^2 + 625X = 0 \tag{3.25}$$

has three distinct roots, namely, 0 and $-7 \pm 24\sqrt{-1}$, so that the curve

$$C = \{(X, Y) \in R^2 \mid Y^2 = X^3 + 14X^2 + 625X\} \tag{3.26}$$

is a nonsingular elliptic curve. As (3.25) has exactly one real root, $C$ consists of one real component. We denote the group of rational points of $C$ by $\Gamma$. By Mordell's theorem [**2**, p. 22] we know that $\Gamma$ is a finitely generated abelian group. Let $r$ denote the rank of $\Gamma$. We use the method explained in [**2**, pp. 89–98] to show that $r = 0$.

From [**2**, p. 91] we see that

$$2^r = \frac{\alpha\beta}{4}, \tag{3.27}$$

where $\alpha = 1 +$ number of $b_1 \not\equiv 625 \pmod{Q^{*2}}$, where $b_1$ runs through the positive and negative divisors of 625, such that the equation

$$N^2 = b_1 M^4 + 14M^2e^2 + (625/b_1)e^4 \tag{3.28}$$

is solvable in integers $M(\neq 0), e, N$ satisfying the conditions

$$\begin{aligned} &\mathrm{GCD}\,(M,e) = \mathrm{GCD}\,(N,e) = \mathrm{GCD}\,(b_1,e) \\ &\qquad = \mathrm{GCD}\,(M,625/b_1) = \mathrm{GCD}\,(M,N) = 1 \end{aligned} \tag{3.29}$$

and $\beta = 1 +$ number of $b_1 \not\equiv -2304 \pmod{Q^{*2}}$, where $b_1$ runs through the positive and negative divisors of $-2304$, such that the equation

$$N^2 = b_1 M^4 - 28M^2e^2 - (2304/b_1)e^4 \tag{3.30}$$

is solvable in integers $M(\neq 0), e, N$ satisfying

$$\begin{aligned} &\mathrm{GCD}\,(M,e) = \mathrm{GCD}\,(N,e) = \mathrm{GCD}\,(b_1,e) \\ &\qquad = \mathrm{GCD}\,(M,-2304/b_1) = \mathrm{GCD}\,(M,N) = 1. \end{aligned} \tag{3.31}$$

First we show that $\alpha = 2$. The divisors $b_1$ of 625 are

$$b_1 = \pm 1, \pm 5, \pm 25, \pm 125, \pm 625.$$

As $\pm 25, \pm 125, \pm 625$ differ from $\pm 1, \pm 5, \pm 1$ respectively by squares, we need only consider

$$b_1 = \pm 1, \pm 5,$$

and $b_1 \not\equiv 625 \pmod{Q^{*2}}$ eliminates $b_1 = 1$. When $b_1 = -1$ the equation (28) $N^2 = -M^4 + 14M^2e^2 - 625e^4$ has no integral solutions with $M \neq 0$ as, for $M \neq 0$,

$$-M^4 + 14M^2e^2 - 625e^4 = -((6Me)^2 + (M^2 - 25e^2)^2) < 0.$$

When $b_1 = 5$ the equation (3.28) $N^2 = 5M^4 + 14M^2e^2 + 125e^4$ has the solution $(M, e, N) = (1, 1, 12)$ which satisfies (3.29). When $b_1 = -5$ the equation (3.28) $N^2 = -5M^4 + 14M^2e^2 - 125e^4$ has no integral solutions with $M \neq 0$ as, for $M \neq 0$,

$$-5M^4 + 14M^2e^2 - 125e^4 = -((6Me)^2 + 5(M^2 - 5e^2)^2) < 0.$$

This completes the proof that $\alpha = 1 + 1 = 2$.

Next we show that $\beta = 2$. There are $2(8+1)(2+1) = 54$ positive and negative divisors of $2304 = 2^8 \times 3^2$. Each of these 54 divisors differs by a square from exactly one of

$$b_1 = \pm 1, \pm 2, \pm 3, \pm 6,$$

and $b_1 \not\equiv -2304 \pmod{Q^{*2}}$ eliminates $b_1 = -1$. The equation (3.30) becomes

(A) $b_1 = 1$ $N^2 = M^4 - 28M^2e^2 - 2304e^4$,

(B) $b_1 = 2$ $N^2 = 2M^4 - 28M^2e^2 - 1152e^4$,

(C) $b_1 = 3$ $N^2 = 3M^4 - 28M^2e^2 - 768e^4$,

(D) $b_1 = 6$ $N^2 = 6M^4 - 28M^2e^2 - 384e^4$,

(E) $b_1 = -2$ $N^2 = -2M^4 - 28M^2e^2 + 1152e^4$,

(F) $b_1 = -3$ $N^2 = -3M^4 - 28M^2e^2 + 768e^4$,

(G) $b_1 = -6$ $N^2 = -6M^4 - 28M^2e^2 + 384e^4$.

Equation (A) has the solution $(M, e, N) = (1, 0, 1)$ which satisfies the conditions (3.31).

Any solution of (B) in integers $M, e, N$ has $N$ even and thus $M$ odd as $\mathrm{GCD}(M,N) = 1$. But modulo 4 (B) gives $0 \equiv 2 \pmod 4$, a contradiction. Thus (B) has no solution in integers satisfying (3.31).

In exactly the same way, we can show that the equations (D), (E), (G) do not have solutions in integers satisfying (3.31).

An integral solution of (C) must have $M$ and $N$ both odd as $\mathrm{GCD}(M,N) = 1$. Then (C) modulo 4 gives the contradiction $1 \equiv 3 \pmod 4$. Thus (C) has no solutions in integers satisfying (3.31).

Thus,

$$\beta = \begin{cases} 2 & \text{if (F) has no solution in integers satisfying (3.31),} \\ 3 & \text{if (F) has a solution in integers satisfying (3.31).} \end{cases}$$

But $\beta$ must be a power of 2 [2, p. 91], so we have $\beta = 2$ and (F) does not have a solution in integers satisfying (3.31).

From (3.27), we deduce

$$2^r = \frac{2 \times 2}{4} = 1,$$

that is, $r = 0$.

We have now shown that $\Gamma$ is a finite abelian group. Thus, every rational point $(X, Y)$ on $C$ has finite order. By the Nagell-Lutz theorem (see, for example, [2, p. 56]) $X$ and $Y$ must both be integers and either (i) $Y = 0$ or (ii) $Y \neq 0$, $Y^2 \mid D$, where $D$ is the discriminant of the cubic polynomial $X^3 + 14X^2 + 625X$, that is, $D = -2^8 \cdot 3^2 \cdot 5^8$. Thus, the possible values of $Y \neq 0$ are the (positive and negative) divisors of $2^4 \cdot 3 \cdot 5^4 = 30,000$. There are $2(4+1)(1+1)(4+1) = 100$ such values of $Y$. A simple computer search shows that the only values of $Y$ for which there is a value of $X$ with $X^3 + 14X^2 + 625X = Y^2$ are $Y = \pm 60, \pm 200, \pm 1500$. Appealing to (3.19), (3.20) and (3.23), we obtain the following table.

| $X$ | $Y$ | $Z = X - 25$ | $x = Z/100$ | $y = Y/1000$ | $f$ | $af^3$ | $bf^5$ |
|---|---|---|---|---|---|---|---|
| 0 | 0 | −25 | −1/4 | 0 | $5/A$ | 100 | 1000 |
| 5 | 60 | −20 | −1/5 | 3/50 | 1/A | 5 | 3 |
| 5 | −60 | −20 | −1/5 | −3/50 | $5/A$ | 25 | 300 |
| 25 | 200 | 0 | 0* | | | | |
| 25 | −200 | 0 | 0* | | | | |
| 125 | 1500 | 100 | 1 | 3/2 | $-1/A$ | 1 | 0** |
| 125 | −1500 | 100 | 1 | −3/2 | $-5/A$ | 5 | −15 |

* inadmissible as $x \neq 0$

** inadmissible as $b \neq 0$

We have now arrived at the remaining four quintic trinomials listed in (3.2). It remains to show that each quintic trinomial in (3.2) is irreducible and solvable, and to find the solutions.

Clearly, $X^5 + aX^2 + b$ is irreducible if and only if $X^5 + af^3X^2 + bf^5$ is irreducible. Further, $X^5 + 5X^2 + 3$ is irreducible as $(X+2)^5 + 5(X+2)^2 + 3$ is 5-Eisenstein, $X^5 + 5X^2 - 15$ is irreducible as $X^5 + 5X^2 - 15$ is 5-Eisenstein, $X^5 + 25X^2 + 300$ is irreducible as $X^5 + 25X^2 + 300$ is irreducible (mod 7), $X^5 + 100X^2 + 1000$ is irreducible as $X^5 + 100X^2 + 1000$ is irreducible (mod 11), and $X^5 + 250X^2 + 625$ is irreducible as $X^5 + 250X^2 + 625$ is irreducible (mod 11).

Finally, we determine the solutions of $x^5 + ax^2 + b = 0$ in radical form showing that $X^5 + aX^2 + b$ is solvable. Recall that $R > 0$ is the unique rational root of the resolvent sextic (3.3), and set

$$H = R/125 > 0. \tag{3.32}$$

From (3.12) we see that

$$\left(\frac{A^2}{4} + \frac{a^2}{100H}\right)^2 - \left(\frac{Aa}{10H} - 4\right)^2 H = 9H \tag{3.33}$$

so that

$$\frac{A^2}{4} + \frac{a^2}{100H} > \left|\frac{Aa}{10H} - 4\right|\sqrt{H}. \tag{3.34}$$

Hence we can define real numbers $v_1, v_2, v_3, v_4$ by

$$
\begin{aligned}
v_1 &= \frac{A}{4} - \frac{a}{20H}\sqrt{H} + \frac{1}{2}\sqrt{\frac{A^2}{4} + \frac{a^2}{100H} - \left(\frac{Aa}{10H} - 4\right)\sqrt{H}}, \\
v_2 &= \frac{A}{4} + \frac{a}{20H}\sqrt{H} - \frac{1}{2}\sqrt{\frac{A^2}{4} + \frac{a^2}{100H} + \left(\frac{Aa}{10H} - 4\right)\sqrt{H}}, \\
v_3 &= \frac{A}{4} + \frac{a}{20H}\sqrt{H} + \frac{1}{2}\sqrt{\frac{A^2}{4} + \frac{a^2}{100H} + \left(\frac{Aa}{10H} - 4\right)\sqrt{H}}, \\
v_4 &= \frac{A}{4} - \frac{a}{20H}\sqrt{H} - \frac{1}{2}\sqrt{\frac{A^2}{4} + \frac{a^2}{100H} - \left(\frac{Aa}{10H} - 4\right)\sqrt{H}}.
\end{aligned} \tag{3.35}
$$

Clearly,

$$
v_1 v_4 = -\sqrt{H}, \qquad v_2 v_3 = \sqrt{H}, \qquad v_1 v_4 = -v_2 v_3, \tag{3.36}
$$

so $v_1, v_2, v_3, v_4$ are all nonzero as $H \neq 0$. Further,

$$
\begin{aligned}
&(v_4 - v_1)(v_3 - v_2) \\
&= -\sqrt{\left(\frac{A^2}{4} + \frac{a^2}{100H} - \left(\frac{Aa}{10H} - 4\right)\sqrt{H}\right)\left(\frac{A^2}{4} + \frac{a^2}{100H} + \left(\frac{Aa}{10H} - 4\right)\sqrt{H}\right)} \\
&= -\sqrt{\left(\frac{A^2}{4} + \frac{a^2}{100H}\right)^2 - \left(\frac{Aa}{10H} - 4\right)^2 H} \\
&= -\sqrt{9H}, \qquad \text{(by (3.33))} \\
&= -3\sqrt{H},
\end{aligned}
$$

that is, by (3.36),

$$
(v_4 - v_1)(v_3 - v_2) = 3v_1 v_4. \tag{3.37}
$$

Further, we have by (3.35) and (3.36),

$$
v_1 v_4 (v_3 - v_4 - v_1 + v_2) = (-\sqrt{H})\left(\frac{4a}{20H}\sqrt{H}\right) = -\frac{a}{5} \tag{3.38}
$$

and

$$(3.39)\quad v_1^2v_3 - v_2^2v_1 - v_3^2v_4 + v_4^2v_2 = \left(-\frac{A^2a}{40H} + \frac{a^3}{1000H^2} + \frac{5A}{2}\right)\sqrt{H}.$$

Hence,

$$\begin{aligned}
&10(v_1v_4)^2(v_1+v_2+v_3+v_4) - (v_1v_4)(v_1^2v_3 - v_2^2v_1 - v_3^2v_4 + v_4^2v_2)\\
&= 10HA + H\left(-\frac{A^2a}{40H} + \frac{a^3}{1000H^2} + \frac{5A}{2}\right) \qquad \text{(by (3.35), (3.36), (3.39))}\\
&= \frac{25HA}{2} - \frac{A^2a}{40} + \frac{a^3}{1000H}\\
&= \frac{AR}{10} - \frac{A^2a}{40} + \frac{a^3}{8R},
\end{aligned}$$

that is, by (3.11),

$$(3.40)\quad 10(v_1v_4)^2(v_1+v_2+v_3+v_4) - (v_1v_4)(v_1^2v_3 - v_2^2v_1 - v_3^2v_4 + v_4^2v_2) = b.$$

Next we define nonzero real numbers $u_1, u_2, u_3, u_4$ by

$$(3.41)\quad \begin{aligned}
u_1 &= v_1^{3/5}v_3^{1/5}v_4^{1/5},\\
u_2 &= v_2^{1/5}v_3^{3/5}v_4^{1/5},\\
u_3 &= v_1^{1/5}v_2^{3/5}v_3^{1/5},\\
u_4 &= v_1^{1/5}v_2^{1/5}v_4^{3/5}.
\end{aligned}$$

Hence,

$$(3.42)\quad \begin{aligned}
u_1u_4 + u_2u_3 &= (v_1v_2v_3v_4)^{1/5}((v_1v_4)^{3/5} + (v_2v_3)^{3/5})\\
&\qquad \text{(by (3.41))}\\
&= (-H)^{1/5}(-H^{3/10} + H^{3/10}) \qquad \text{(by (3.36))}\\
&= 0;
\end{aligned}$$

$$(3.43)\quad \begin{aligned}
&u_1u_2^2 + u_2u_4^2 + u_3u_1^2 + u_4u_3^2\\
&\qquad = (v_1v_4)(v_3 - v_4 - v_1 + v_2) \qquad \text{(by (3.36) and (3.41))}\\
&\qquad = -a/5 \qquad \text{(by (3.38));}
\end{aligned}$$

$$
\begin{aligned}
(3.44)\quad & u_1^2u_4^2 + u_2^2u_3^2 - u_1^3u_2 - u_2^3u_4 - u_3^3u_1 - u_4^3u_3 - u_1u_2u_3u_4 \\
&= -u_1^3u_2 - u_2^3u_4 - u_3^3u_1 - u_4^3u_3 - 3u_1u_2u_3u_4 \qquad \text{(by (3.42))} \\
&= -v_1v_4\{(v_3 - v_2)(v_4 - v_1) - 3v_1v_4\} \qquad \text{(by (3.36) and (3.41))} \\
&= 0 \qquad \text{(by (3.37))};
\end{aligned}
$$

and

$$
\begin{aligned}
(3.45)\quad & 5(u_1^3u_3u_4 + u_2^3u_1u_3 + u_3^3u_2u_4 + u_4^3u_1u_2 - u_1u_3^2u_4^2 \\
&\qquad - u_2u_1^2u_3^2 - u_3u_2^2u_4^2 - u_4u_1^2u_2^2) - (u_1^5 + u_2^5 + u_3^5 + u_4^5) \\
&= 10(v_1v_4)^2(v_1 + v_2 + v_3 + v_4) \\
&\quad - (v_1v_4)(v_1^2v_2 - v_2^2v_1 - v_3^2v_4 + v_4^2v_2) \qquad \text{(by (3.36) and (3.41))} \\
&= b \qquad \text{(by (3.40))}.
\end{aligned}
$$

Appealing to the identity [**3**, equations (5) and (6)], we obtain by (3.42), (3.43), (3.44) and (3.45),

$$
\begin{aligned}
&\prod_{j=0}^{4}(x - (\omega^j u_1 + \omega^{2j}u_2 + \omega^{3j}u_3 + \omega^{4j}u_4)) \\
&\quad = x^5 - 5(u_1u_4 + u_2u_3)x^3 \\
&\qquad - 5(u_1u_2^2 + u_2u_4^2 + u_3u_1^2 + u_4u_3^2)x^2 \\
&\qquad + 5(u_1^2u_4^2 + u_2^2u_3^2 - u_1^3u_2 - u_2^3u_4 - u_3^3u_1 - u_4^3u_3 - u_1u_2u_3u_4)x \\
&\qquad + 5(u_1^3u_3u_4 + u_2^3u_1u_3 + u_3^3u_2u_4 + u_4^3u_1u_2 \\
&\qquad\qquad - u_1u_3^2u_4^2 - u_2u_1^2u_3^2 - u_3u_2^2u_4^2 - u_4u_1^2u_2^2) \\
&\qquad - (u_1^5 + u_2^5 + u_3^5 + u_4^5) \\
&\quad = x^5 + ax^2 + b,
\end{aligned}
$$

where $\omega$ denotes a complex fifth root of unity. Hence, the roots of

$$
x^5 + ax^2 + b = 0 \tag{3.46}
$$

are

$$
x = \omega^j u_1 + \omega^{2j}u_2 + \omega^{3j}u_3 + \omega^{4j}u_4, \qquad j = 0, 1, 2, 3, 4. \tag{3.47}
$$

We now examine each of the five possibilities listed in (3.2). Note that the roots of $x^5 + af^3x^2 + bf^5 = 0$ are obtained from those of (3.46) by dividing by $f$.

| $x^5+ax^2+b=0$ | $a$ | $b$ | $R$ | $H$ | $A$ | Galois group |
|---|---|---|---|---|---|---|
| $x^5+5x^2+3=0$ | 5 | 3 | 25 | 1/5 | 1 | $D_5$ |
| $x^5+5x^2-15=0$ | 5 | −15 | 25 | 1/5 | −5 | $D_5$ |
| $x^5+25x^2+300=0$ | 25 | 300 | 625 | 5 | 5 | $D_5$ |
| $x^5+100x^2+1000=0$ | 100 | 1000 | 2000 | 16 | 5 | $F_{20}$ |
| $x^5+250x^2+625=0$ | 250 | 625 | 3125 | 25 | 0 | $F_{20}$ |

In each case $R$ is the unique rational root of (3.4). $H$ is given by (3.32). $A$ is given by (3.10). The values of $v_1, v_2, v_3, v_4$ follow from (3.35), and the values of $u_1, u_2, u_3, u_4$ are given in Theorem 3 from (3.41). Thus, $x^5+ax^2+b$ is solvable in each of the five cases with roots as given in the statement of Theorem 3.

This completes the proof of Theorem 3 and thus of Theorem 2. □

**Acknowledgments.** The authors would like to acknowledge the help of Laura Spearman, who did some computing for them in connection with this research.

## REFERENCES

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

2. J.H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer-Verlag, New York, 1992.

3. B.K. Spearman and K.S. Williams, *Characterization of solvable quintics* $x^5+ax+b$, Amer. Math. Monthly **101** (1994), 986–992.

4. J.V. Uspensky, *Theory of equations*, McGraw-Hill Book Company, Inc., New York, 1948.

DEPARTMENT OF MATHEMATICS AND STATISTICS, OKANAGAN UNIVERSITY COLLEGE, KELOWNA, B.C. V1V 1V7, CANADA

DEPARTMENT OF MATHEMATICS AND STATISTICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO K1S 5B6, CANADA