ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 30, Number 1, Spring 2000

PURE QUINTIC FIELDS DEFINED BY TRINOMIALS

BLAIR K. SPEARMAN AND KENNETH S. WILLIAMS

ABSTRACT. Pure quintic fields which can be defined by a trinomial $X^5 + aX + b$ or $X^5 + aX^2 + b$, where a and b are nonzero rational numbers, are characterized. Using this characterization it is shown that the only pure quintic field $Q(p^{1/5})$ (p a prime) which can be defined by a trinomial is $Q(2^{1/5}) = Q(\theta)$, where θ is the unique real root of $x^5+100x^2+1000 = 0$.

1. Introduction. Let Q denote the field of rational numbers, and let K be a quintic extension of Q, that is, $[K : Q] = 5$. The quintic field K is said to be defined by a trinomial if there exist $a, b \in Q\backslash\{0\}$ such that there is a root θ of $x^5+ax+b = 0$ or $x^5+ax^2+b = 0$ such that $K = Q(\theta)$. Clearly if K is defined by a trinomial, then the corresponding trinomial $X^5 + aX + b$ or $X^5 + aX^2 + b$ is irreducible in $Q[X]$. The quintic field K is called a pure field if $K = Q(z^{1/5})$ for some rational number z which is not a fifth power in Q and $z^{1/5}$ denotes the real fifth root of z. In this paper we are interested in quintic fields defined by trinomials which are pure fields, see Theorems 3.1 and 4.1. Our approach is based upon the characterization of solvable quintic trinomials given in [6]. General solvable quintics are treated by Dummit [2]. We show that the only pure quintic field $Q(p^{1/5})$, p a prime, which can be defined by a trinomial is $Q(2^{1/5}) = Q(\theta)$, where θ is the unique real root of $x^5 + 100x^2 + 1000 = 0$, see Theorem 5.2.

2. Solvable quintic fields defined by $X^5 + aX + b$. Throughout this section we assume that a and b are nonzero rationals such that the

Received by the editors on April 9, 1998, and in revised form on September 9, 1998.
1991 AMS *Mathematics Subject Classification.* Primary 12D05, 12E10, 11R21, 11R29, 11R32.
Key words and phrases. Pure quintic fields, solvable quintic trinomials.
The research of the first author was supported by a Natural Sci. and Engrg. Research Council of Canada grant.
The research of the second author was supported by Natural Sci. and Engrg. Research Council of Canada grant A-7233.

quintic trinomial $X^5 + aX + b$ is both irreducible and solvable. It is shown in [6] that there exist rationals $\varepsilon(= \pm 1), c(\geq 0)$ and $e(\neq 0)$ such that

$$a = \frac{5e^4(3 - 4\varepsilon c)}{c^2 + 1}, \qquad b = -\frac{4e^5(11\varepsilon + 2c)}{c^2 + 1}. \tag{2.1}$$

Moreover, $x^5 + ax + b = 0$ has exactly one real root [6, p. 989], which we denote by x_0. We set, see [6, equations (14), (15), (16)],

$$D = c^2 + 1, \tag{2.2}$$

$$\begin{cases} v_1 = \sqrt{D} + \sqrt{D - \varepsilon\sqrt{D}}, & v_2 = -\sqrt{D} - \sqrt{D + \varepsilon\sqrt{D}}, \\ v_3 = -\sqrt{D} + \sqrt{D + \varepsilon\sqrt{D}}, & v_4 = \sqrt{D} - \sqrt{D - \varepsilon\sqrt{D}}, \end{cases} \tag{2.3}$$

$$u_1 = \left(\frac{v_1^2 v_3}{D^2}\right)^{1/5}, \quad u_2 = \left(\frac{v_3^2 v_4}{D^2}\right)^{1/5}, \tag{2.4}$$

$$u_3 = \left(\frac{v_2^2 v_1}{D^2}\right)^{1/5}, \quad u_4 = \left(\frac{v_4^2 v_2}{D^2}\right)^{1/5},$$

$$\omega = e^{2\pi i/5}. \tag{2.5}$$

Then the roots of $x^5 + ax + b = 0$ are x_0, x_1, x_2, x_3, x_4, where

$$x_j = e(\omega^j u_1 + \omega^{2j} u_2 + \omega^{3j} u_3 + \omega^{4j} u_4), \quad j = 0, 1, 2, 3, 4, \tag{2.6}$$

see [6, equation (13)].

Lemma 2.1. *For $j = 0, 1, 2, 3, 4$,*

$$x_j = e\left(\omega^j u_1 + \omega^{2j}\left(\frac{\varepsilon D^{1/2}}{v_1}\right)u_1^2 + \omega^{3j}\left(\frac{D}{v_1 v_3}\right)u_1^3 + \omega^{4j}\left(\frac{-\varepsilon D^{3/2}}{v_1^2 v_3}\right)u_1^4\right).$$

Proof. The lemma follows immediately from (2.6) on noting the

following relations

$$\left(\frac{u_2}{u_1^2}\right)^5 = \frac{v_3^2 v_4}{D^2}\frac{D^4}{v_1^4 v_3^2} = \frac{v_1 v_4 D^2}{v_1^5} = \frac{\varepsilon D^{5/2}}{v_1^5},$$
$$\left(\frac{u_3}{u_1^3}\right)^5 = \frac{v_2^2 v_1}{D^2}\frac{D^6}{v_1^6 v_3^3} = \frac{v_2^2 D^4}{v_1^5 v_3^3} = \frac{D^5}{v_1^5 v_3^5},$$
$$\left(\frac{u_4}{u_1^4}\right)^5 = \frac{v_4^2 v_2}{D^2}\frac{D^8}{v_1^8 v_3^4} = \frac{v_4^2 v_1^2 v_2 v_3 D^6}{v_1^{10} v_3^5} = \frac{-\varepsilon D^{15/2}}{v_1^{10} v_3^5},$$

where we have made use of the relations $v_1 v_4 = \varepsilon\sqrt{D}$, $v_2 v_3 = -\varepsilon\sqrt{D}$. □

We leave it to the reader to give the x_j, $j = 0, 1, 2, 3, 4$, as polynomials in each of u_2, u_3, u_4 analogously to Lemma 2.1.

Lemma 2.2. *If $u_j^5 \in Q$ for some $j = 1, 2, 3$ or 4, then $D = m^2$ for some positive rational m.*

Proof. We assume that $u_1^5 \in Q$. The argument is similar if u_2^5, u_3^5 or $u_4^5 \in Q$. If $D = m^2$ for some positive rational m, we are finished. Thus, we may suppose that $D \neq m^2$ for any nonzero rational m and so $Q(\sqrt{D + \sqrt{D}})$ is a cyclic quartic field with unique quadratic subfield $Q(\sqrt{D})$. Hence, $1, \sqrt{D}, \alpha, \beta$ are linearly independent over Q, where

$$\alpha = \sqrt{D + \varepsilon\sqrt{D}}, \qquad \beta = \sqrt{D - \varepsilon\sqrt{D}}.$$

Now, by (2.3) and (2.4),

$$\begin{aligned} D^2 u_1^5 = v_1^2 v_3 &= (\sqrt{D} + \beta)^2(-\sqrt{D} + \alpha) \\ &= -2D\sqrt{D} + \varepsilon\sqrt{D} + 2cD + 2D\alpha - 2D\beta - \varepsilon\sqrt{D}\alpha \in Q. \end{aligned}$$

But

$$\sqrt{D}\alpha = \varepsilon\alpha + c\beta$$

so

$$(\varepsilon D + 2cD) - 2D\sqrt{D} + (2D - 1)\alpha - (2D + \varepsilon c)\beta \in Q.$$

This contradicts that $1, \sqrt{D}, \alpha, \beta$ are linearly independent over Q as the coefficient of $\sqrt{D}$ is nonzero. □

Lemma 2.3. *If $u_j^5 \in Q$ for some $j = 1, 2, 3$ or 4, then $D = m^2$ and $m^2 + m = n^2$ for some positive rationals m and n.*

Proof. We assume that $u_1^5 \in Q$. The proof is similar if u_2^5, u_3^5 or $u_4^5 \in Q$. By Lemma 2.2 we have $D = m^2$ for some positive rational m. Suppose $m^2 + m \neq n^2$ for any rational n. By (2.3) and (2.4), we have

$$\begin{aligned} D^2 u_1^5 = v_1^2 v_3 &= (m + \sqrt{m^2 - \varepsilon m})^2(-m + \sqrt{m^2 + \varepsilon m}) \\ &= m\Big((-2m^2 + \varepsilon m + 2cm) + (2m - \varepsilon)\sqrt{m^2 + \varepsilon m} \\ &\qquad - 2m\sqrt{m^2 - \varepsilon m}\Big) \in Q, \end{aligned}$$

so that

$$(2m - \varepsilon)\sqrt{m^2 + \varepsilon m} - 2m\sqrt{m^2 - \varepsilon m} \in Q. \tag{2.7}$$

If $c = 0$, then $D = 1 = m^2$ so $m = 1$ and (2.7) becomes

$$(2 - \varepsilon)\sqrt{1 + \varepsilon} - 2\sqrt{1 - \varepsilon} \in Q,$$

which is impossible for $\varepsilon = \pm 1$. If $c \neq 0$, then $D = m^2 \neq 1$ so $m \neq \pm\varepsilon$ and

$$\sqrt{m^2 - \varepsilon m} = \frac{c}{m + \varepsilon}\sqrt{m^2 + \varepsilon m}$$

so that (2.7) yields

$$\frac{2m^2 - 2cm + \varepsilon m - 1}{m + \varepsilon}\sqrt{m^2 + \varepsilon m} \in Q.$$

As

$$(m^2 - m)(m^2 + m) = m^2 c^2 \neq 0$$

and

$$m^2 + m \neq n^2 \quad \text{for any rational } n,$$

we deduce that

$$m^2 - m \neq l^2 \quad \text{for any rational } l.$$

Hence $\sqrt{m^2+\varepsilon m}$ is irrational and thus

$$2m^2 - 2cm + \varepsilon m - 1 = 0.$$

We have

$$c = \frac{2m^2+\varepsilon m-1}{2m}$$

so

$$\left(\frac{2m^2+\varepsilon m-1}{2m}\right)^2 + 1 = m^2,$$

that is,

$$4\varepsilon m^3 + m^2 - 2\varepsilon m + 1 = (m+\varepsilon)(4\varepsilon m^2 - 3m + \varepsilon) = 0.$$

As

$$4\varepsilon m^2 - 3m + \varepsilon = \varepsilon\left\{\left(2m - \frac{3\varepsilon}{4}\right)^2 + \frac{7}{16}\right\} \neq 0$$

we must have $m = -\varepsilon$. This gives $c^2 = m^2 - 1 = 1 - 1 = 0$, contradicting $c \neq 0$. Hence $m^2 + m = n^2$ for some rational n. As m is positive, we can take n to be positive. □

We remark that, if $D = m^2$ and $m^2 + m = n^2$ for some positive rationals m and n, then $m \neq \pm 1$, $D \neq 1$ and $c \neq 0$.

Lemma 2.4. *If $u_j^5 \in Q$ for some $j = 1, 2, 3$ or 4, then $v_1, v_2, v_3, v_4, u_1^5, u_2^5, u_3^5, u_4^5 \in Q$.*

Proof. By Lemma 2.3 there exist positive rationals m and n such that

$$D = m^2, \qquad m^2 + m = n^2.$$

Then

$$(m^2 - m)(m^2 + m) = m^2(m^2 - 1) = m^2(D - 1) = m^2c^2$$

so that

$$m^2 - m = (mc/n)^2.$$

Hence there exist nonnegative rationals r and s such that

$$m^2 + \varepsilon m = r^2, \qquad m^2 - \varepsilon m = s^2.$$

Thus, by (2.3), we have

$$v_1 = m + s \in Q, \qquad v_2 = -m - r \in Q,$$
$$v_3 = -m + r \in Q, \qquad v_4 = -m - s \in Q.$$

Finally, from (2.4), we deduce that

$$u_1^5, u_2^5, u_3^5, u_4^5 \in Q. \qquad \square$$

3. Pure quintic fields defined by $X^5 + aX + b$. We begin by proving the following result.

Lemma 3.1. *Let $a, b \in Q\backslash\{0\}$, and suppose that $X^5 + aX + b$ is irreducible and solvable in $Q[X]$. Let x_0 be the unique real root of $x^5 + ax + b = 0$. Then the following hold.*

(i) *$Q(x_0)$ is pure if and only if $u_1^5, u_2^5, u_3^5, u_4^5 \in Q$.*

(ii) *If $Q(x_0)$ is pure, then $Q(x_0) = Q(u_j)$, $j = 1, 2, 3, 4$.*

Proof. Suppose first that $u_1^5, u_2^5, u_3^5, u_4^5 \in Q$. Then, by Lemma 2.3, there exist positive rationals m and n such that

$$D = m^2, \qquad m^2 + m = n^2.$$

Thus, by Lemma 2.1, we have

$$x_0 = e\left(u_1 + \left(\frac{\varepsilon m}{v_1}\right)u_1^2 + \left(\frac{m^2}{v_1 v_3}\right)u_1^3 - \left(\frac{\varepsilon m^3}{v_1^2 v_3}\right)u_1^4\right),$$

and, by Lemma 2.4, $v_1 \in Q$ and $v_3 \in Q$. Hence,

$$x_0 \in Q(u_1).$$

As $u_1^5 \in Q$, $[Q(u_1) : Q] = 1$ or 5. Now x_0 is a root of the irreducible quintic $X^5 + aX + b$ so $[Q(x_0) : Q] = 5$. Since $Q(x_0) \subseteq Q(u_1)$, we must

have $[Q(u_1) : Q] = 5$ and $Q(x_0) = Q(u_1)$. By a similar argument we have $Q(x_0) = Q(u_2) = Q(u_3) = Q(u_4)$. Thus $Q(x_0)$ is a pure field. This completes the proof of (i) in one direction. We now prove (i) in the other direction. Assertion (ii) then follows from the above proof.

Now we suppose that $Q(x_0)$ is a pure field, and we show that $u_1^5, u_2^5, u_3^5, u_4^5 \in Q$. We set

$$M = Q(x_0, x_1, x_2, x_3, x_4)$$

the splitting field of $X^5 + aX + b$. As $x_4 = -x_0 - x_1 - x_2 - x_3$, we see that

$$M = Q(x_0, x_1, x_2, x_3).$$

Further, as $Q(x_0)$ is a pure field, we have $\omega \in M$, where ω is defined in (2.5). Also as $Q(x_0)$ is a pure field its Galois group is solvable and so must be isomorphic to the Frobenius group F_{20} or the dihedral group D_5 of order 10 [6, p. 990]. In the latter case, M does not contain a quartic subfield, contradicting that $Q(\omega) \subseteq M$. Hence the Galois group must be F_{20} and the subfield structure of M given in [8, p. 16] shows that M contains a unique quartic subfield which must be $Q(\omega)$. Indeed, $Q(\omega)$ contains all the elements of M of degree 1, 2 or 4 over Q.

Taking $j = 0, 1, 2, 3$ in (2.6), we obtain

$$\begin{aligned} u_1 + u_2 + u_3 + u_4 &= x_0/e, \\ \omega u_1 + \omega^2 u_2 + \omega^3 u_3 + \omega^4 u_4 &= x_1/e, \\ \omega^2 u_1 + \omega^4 u_2 + \omega u_3 + \omega^3 u_4 &= x_2/e, \\ \omega^3 u_1 + \omega u_2 + \omega^4 u_3 + \omega^2 u_4 &= x_3/e. \end{aligned}$$

The determinant of the coefficient matrix of this system of four linear equations in u_1, u_2, u_3, u_4 is

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ \omega & \omega^2 & \omega^3 & \omega^4 \\ \omega^2 & \omega^4 & \omega & \omega^3 \\ \omega^3 & \omega & \omega^4 & \omega^2 \end{vmatrix} = -5\sqrt{5} \neq 0.$$

Hence, by Cramer's rule, we see that

$$u_1 = \frac{\begin{vmatrix} x_0/e & 1 & 1 & 1 \\ x_1/e & \omega^2 & \omega^3 & \omega^4 \\ x_2/e & \omega^4 & \omega & \omega^3 \\ x_3/e & \omega & \omega^4 & \omega^2 \end{vmatrix}}{-5\sqrt{5}} \in Q(\omega, x_0, x_1, x_2, x_3) = M(\omega) = M,$$

and similarly $u_2, u_3, u_4 \in M$. Thus, $Q(u_1^5) \subseteq M$ and so as $[M : Q] = 20$ we have

$$[Q(u_1^5) : Q] = 1, 2, 4, 5, 10 \text{ or } 20.$$

Now, by (2.3) and (2.4), we see that

$$u_1^5 \in Q\Big(\sqrt{D - \sqrt{D}}, \sqrt{D + \sqrt{D}}\Big)$$

so that

$$[Q(u_1^5) : Q] = 1, 2, 4 \text{ or } 8.$$

Hence,

$$[Q(u_1^5) : Q] = 1, 2 \text{ or } 4.$$

But, as we have already noted, all the elements of M of degree 1, 2 or 4 over Q belong to $Q(\omega)$. Thus,

$$u_1^5 \in Q(\omega).$$

If $u_1 \in Q(\omega)$, each summand in the expression for x_0 given in Lemma 2.1 has degree a power of two so that x_0 could not be a quintic irrationality. Hence, $u_1 \notin Q(\omega)$. Thus, by [3], Theorem 10(b), p. 214], $Q(\omega, u_1)$ is cyclic over $Q(\omega)$ of degree five. Now

$$[Q(\omega, u_1) : Q] = [Q(\omega, u_1) : Q(\omega)][Q(\omega) : Q] = 5 \times 4 = 20 = [M : Q]$$

and

$$Q(\omega, u_1) \subseteq M,$$

so that $M = Q(\omega, u_1)$. Thus the Galois group of $M/Q(\omega)$ is cyclic of order five and the conjugates of u_1 over $Q(\omega)$ are $\omega^j u_1$, $j = 0, 1, 2, 3, 4$. Let ϕ be the automorphism of $M/Q(\omega)$ such that

$$\phi(u_1) = \omega u_1.$$

Now by [6, p. 989], we have

$$\sqrt{D} = -\frac{\varepsilon}{u_1 u_4} \in M.$$

But all the elements of M of degree 1, 2 or 4 over Q are contained in $Q(\omega)$, so

$$\sqrt{D} \in Q(\omega).$$

Thus

$$u_1u_4 = -\frac{\varepsilon}{\sqrt{D}} \in Q(\omega),$$

and so

$$\phi(u_1u_4) = u_1u_4.$$

Hence,

$$\phi(u_4) = \frac{u_1u_4}{\phi(u_1)} = \frac{u_1u_4}{\omega u_1} = \omega^4 u_4.$$

Further, by [6, equation (24), p. 989], we have

$$v_1 = Du_1^2u_3 \in M$$

and, by (2.3), we see that v_1 is of degree 1, 2 or 4 over Q. hence,

$$v_1 \in Q(\omega).$$

Thus,

$$\phi(v_1) = v_1,$$

and so

$$\phi(u_1^2u_3) = \phi\left(\frac{v_1}{D}\right) = \frac{v_1}{D} = u_1^2u_3.$$

Hence,

$$\phi(u_3) = \frac{u_1^2u_3}{\phi(u_1)^2} = \frac{u_1^2u_3}{\omega^2u_1^2} = \omega^3 u_3.$$

Now, by [6, equation (23), p. 989], we have $u_1u_2u_3u_4 = -1/D$, so that $\phi(u_1u_2u_3u_4) = u_1u_2u_3u_4$, and thus

$$\phi(u_2) = \frac{u_1u_2u_3u_4}{\phi(u_1)\phi(u_3)\phi(u_4)} = \frac{u_1u_2u_3u_4}{(\omega u_1)(\omega^3u_3)(\omega^4u_4)} = \omega^2 u_2.$$

Hence we have shown that

$$\phi(u_j) = \omega^j u_j, \qquad j = 1, 2, 3, 4.$$

Next, since $Q(x_0)$ is pure, there exists $z \in Q$, z is not equal to the fifth power in Q, such that $Q(x_0) = Q(z^{1/5})$. A simple degree argument shows that $M = Q(\omega, z^{1/5})$. Clearly, $\phi(z^{1/5}) = \omega^j z^{1/5}$ for some $j = 0, 1, 2, 3, 4$. Certainly $j \neq 0$ as ϕ is not the identity

isomorphism. Let k be the unique integer such that $0 < k < 5$ and $jk \equiv 1 \pmod 5$. We have

$$\phi(z^{k/5}) = (\omega^j z^{1/5})^k = \omega z^{k/5}.$$

Hence, replacing the generator z of $Q(z^{1/5})$ by z^k, if necessary, we can suppose that

$$\phi(z^{1/5}) = \omega z^{1/5}, \qquad Q(x_0) = Q(z^{1/5}).$$

Thus,

$$\phi(z^{j/5}) = \omega^j z^{j/5}, \quad j = 1, 2, 3, 4.$$

As $x_0 \in Q(z^{1/5})$, there exist rationals A, B, C, D, E such that

$$x_0 = A + Bz^{1/5} + Cz^{2/5} + Dz^{3/5} + Ez^{4/5}.$$

Hence, by (2.6), we have

$$e(u_1 + u_2 + u_3 + u_4) = A + Bz^{1/5} + Cz^{2/5} + Dz^{3/5} + Ez^{4/5}.$$

Applying the automorphism ϕ j times to both sides of this equation, we obtain

$$\begin{aligned} e(\omega^j u_1 + \omega^{2j} u_2 + \omega^{3j} u_3 + \omega^{4j} u_4) \\ = A + B\omega^j z^{1/5} + C\omega^{2j} z^{2/5} \\ + D\omega^{3j} z^{3/5} + E\omega^{4j} z^{4/5}, \quad j = 0, 1, 2, 3, 4. \end{aligned}$$

Summing these equations for $j = 0, 1, 2, 3, 4$, we see that $A = 0$. Then the equations with $j = 0, 1, 2, 3$ can be written as

$$(eu_1 - Bz^{1/5}) + (eu_2 - Cz^{2/5}) + (eu_3 - Dz^{3/5}) + (eu_4 - Ez^{4/5}) = 0,$$

$$\begin{aligned} \omega(eu_1 - Bz^{1/5}) + \omega^2(eu_2 - Cz^{2/5}) \\ + \omega^3(eu_3 - Dz^{3/5}) + \omega^4(eu_4 - Ez^{4/5}) = 0, \end{aligned}$$

$$\begin{aligned} \omega^2(eu_1 - Bz^{1/5}) + \omega^4(eu_2 - Cz^{2/5}) \\ + \omega(eu_3 - Dz^{3/5}) + \omega^3(eu_4 - Ez^{4/5}) = 0, \end{aligned}$$

$$\omega^3(eu_1 - Bz^{1/5}) + \omega(eu_2 - Cz^{2/5}) + \omega^4(eu_3 - Dz^{3/5}) + \omega^2(eu_4 - Ez^{4/5}) = 0.$$

The determinant of the coefficient matrix of this system of four linear equations in the four quantities $eu_1 - Bz^{1/5}, eu_2 - Cz^{2/5}, eu_3 - Dz^{3/5}, eu_4 - Ez^{4/5}$ is, as already noted earlier, nonzero. Hence,

$$eu_1 - Bz^{1/5} = eu_2 - Cz^{2/5} = eu_3 - Dz^{3/5} = eu_4 - Ez^{4/5} = 0.$$

Thus

$$u_1^5, u_2^5, u_3^5, u_4^5 \in Q. \qquad \square$$

We are now ready to prove our main result.

Theorem 3.1. (i) *If r is a rational $\neq 0, \pm 1$, then*

$$Q((r^3(r+1)(r-1)^4)^{1/5})$$

is a pure quintic field, which is defined by the trinomial $X^5 + aX + b$, where

$$a = -\frac{80r(r^2-1)(r^2+r-1)(r^2-4r-1)}{(r^2+1)^4}, \tag{3.1}$$

$$b = -\frac{32r(r^2-1)(r^4+22r^3-6r^2-22r+1)}{(r^2+1)^4}. \tag{3.2}$$

(ii) *Let $a, b \in Q\backslash\{0\}$, and suppose that $X^5 + aX + b$ is irreducible in $Q[x]$. Let x_0 be a real root of the equation $x^5 + ax + b = 0$, so that $Q(x_0)$ is a quintic field. If $Q(x_0)$ is a pure field, then*

$$Q(x_0) = Q((r^3(r+1)(r-1)^4)^{1/5})$$

for some rational $r \neq 0, \pm 1$.

Proof. (i) Let r be a rational $\neq 0, \pm 1$. Define $a, b \in Q\backslash\{0\}$ by (3.1) and (3.2). Since a and b are invariant under the transformations

$r \to -1/r$, $r \to ((r-1)/(r+1))$ and $r \to ((1+r)/(1-r))$, we may suppose that $r > 1$. Set

$$c = \left| \frac{(r^2+2r-1)(r^2-2r-1)}{4r(r^2-1)} \right|, \tag{3.3}$$

and

$$\varepsilon = e = \operatorname{sgn}\left(\frac{(r^2+2r-1)(r^2-2r-1)}{4r(r^2-1)} \right). \tag{3.4}$$

We note that $\varepsilon = \pm 1$, $c \geq 0$ and $e \neq 0$. Then a simple calculation shows that

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

and

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

Next we observe that

$$D = c^2 + 1 = \frac{(r^2+1)^4}{2^4 r^2 (r^2-1)^2} \neq \frac{125}{4}$$

so that $c \neq 11/2$. Now suppose that $c = 3/4$ so that $c^2 + 1 = 25/16$. Thus $(r^2+1)^2/(r(r^2-1)) = \pm 5$ and so $r^4 \mp 5r^3 + 2r^2 \pm 5r + 1 = 0$, which is impossible with r rational. Hence $c \neq 3/4$. Thus, by [9, Proposition 4], $X^5 + aX + b$ is irreducible in $Q[x]$. Moreover, $X^5 + aX + b$ is solvable by [6, p. 987]. Let x_0 be the unique real root of $x^5 + ax + b = 0$.

Next we note that

$$D = m^2, \quad m = \left| \frac{(r^2+1)^2}{4r(r^2-1)} \right| \tag{3.5}$$

and that

$$m^2 \pm m = \left(\frac{(r^2+1)(r^2+2r-1)}{4r(r^2-1)} \right)^2 \quad \text{or} \quad \left(\frac{(r^2+1)(r^2-2r-1)}{4r(r^2-1)} \right)^2.$$

Then, by the proof of Lemma 2.4, we see that $u_j^5 \in Q$, $j = 1, 2, 3, 4$. Hence, by Lemma 3.1, $Q(x_0)$ is a pure quintic field and $Q(x_0) = Q(u_j)$, $j = 1, 2, 3, 4$.

Appealing to (2.3), (3.4) and (3.5), we obtain Table 1.

TABLE 1.

	Case A $r > 1+\sqrt{2}$	Case B $1+\sqrt{2} > r > 1$
$\sqrt{D}$	$+(r^2+1)^2/(4r(r^2-1))$	$+(r^2+1)^2/(4r(r^2-1))$
ε	$+1$	-1
$\sqrt{D-\varepsilon\sqrt{D}}$	$+(r^2+1)(r^2-2r-1)/(4r(r^2-1))$	$+(r^2+1)(r^2+2r-1)/(4r(r^2-1))$
$\sqrt{D+\varepsilon\sqrt{D}}$	$+(r^2+1)(r^2+2r-1)/(4r(r^2-1))$	$-(r^2+1)(r^2-2r-1)/(4r(r^2-1))$
v_1	$+(r^2+1)/(2(r+1))$	$+(r^2+1)/(2(r-1))$
v_2	$-(r^2+1)/(2(r-1))$	$-(r^2+1)/(2r(r-1))$
v_3	$+(r^2+1)/(2r(r+1))$	$-(r^2+1)/(2(r+1))$
v_4	$+(r^2+1)/(2r(r-1))$	$-(r^2+1)/(2r(r+1))$

From Table 1 and (2.4), we see that

$$u_1^5 = \frac{v_1^2 v_3}{D^2} = \left(\frac{2}{r^2+1}\right)^5 r^3(r+1)(r-1)^4, \quad \text{in Case A.}$$

$$u_2^5 = \frac{v_3^2 v_4}{D^2} = \left(-\frac{2}{r^2+1}\right)^5 r^3(r+1)(r-1)^4, \quad \text{in Case B.}$$

Hence $Q(x_0) = Q((r^3(r+1)(r-1)^4)^{1/5})$. Thus $Q((r^3(r+1)(r-1)^4)^{1/5})$ is a pure quintic field defined by X^5+aX+b, where a and b are defined in (3.1) and (3.2).

(ii) Let $a, b \in Q\backslash\{0\}$, and suppose that $X^5 + aX + b$ is irreducible in $Q[x]$. Let x_0 be a real root of the equation $x^5 + ax + b = 0$, so that $Q(x_0)$ is a quintic field. Suppose that $Q(x_0)$ is a pure field. Then $X^5 + aX + b$ is both irreducible and solvable in $Q[x]$, and there exist rationals $\varepsilon(= \pm 1), c(\geq 0)$ and $e(\neq 0)$ such that (2.1) and (2.2) hold. By Lemma 3.1 we have $u_j^5 \in Q$ and $Q(x_0) = Q(u_j)$, $j = 1, 2, 3, 4$, where the u_j are defined in (2.4). Then, by Lemma 2.3, $D = m^2$ and $m^2+m = n^2$ for some positive rationals m and n. Hence $c^2+1 = m^2$. By the remark just before Lemma 2.4 we have $c \neq 0$. Clearly $(m-c)(m+c) = 1$, so there exists $t \in Q\backslash\{0\}$ such that

$$m - c = t, \qquad m + c = 1/t.$$

Hence,

$$m = \frac{t^2+1}{2t}, \qquad c = \frac{1-t^2}{2t}. \tag{3.6}$$

As $m > 0$ and $c > 0$, we see that $0 < t < 1$. Next $m^2 + m = n^2$ gives

$$\left(\frac{t^2+1}{2t}\right)^2 + \left(\frac{t^2+1}{2t}\right) = n^2$$

so that

$$t^2 + 1 = \left(\frac{2tn}{t+1}\right)^2,$$

that is,

$$t^2 + 1 = s^2,$$

where $s = 2tn/(t+1)$. As above, from the equation $t^2 + 1 = s^2$, we obtain

$$s = \frac{r^2+1}{2r}, \qquad t = \frac{1-r^2}{2r}, \tag{3.7}$$

for some $r \in Q\backslash\{0\}$. As $r \to -1/r$ and $s \to -s$ in (3.7) preserves (3.7), we may suppose that $r > 0$. As $0 < t < 1$ and $r > 0$, we see that

$$1 > r > \sqrt{2} - 1. \tag{3.8}$$

From (3.6) and (3.7), we deduce that

$$c = \frac{1}{4}\frac{(r^2+2r-1)(r^2-2r-1)}{r(r^2-1)} \tag{3.9}$$

and

$$\sqrt{D} = m = -\frac{1}{4}\frac{(r^2+1)^2}{r(r^2-1)}. \tag{3.10}$$

We now consider two cases depending upon the value of ε ($= 1$ or -1). We make use of (3.10) to calculate v_1, v_2, v_3, v_4 from (2.3) and then u_1, u_2, u_3, u_4 from (2.4), see Table 2.

TABLE 2.

ε	1	-1
$\sqrt{D-\varepsilon\sqrt{D}}$	$-(r^2+1)(r^2+2r-1)/(4r(r^2-1))$	$(r^2+1)(r^2-2r-1)/(4r(r^2-1))$
$\sqrt{D+\varepsilon\sqrt{D}}$	$(r^2+1)(r^2-2r-1)/(4r(r^2-1))$	$-(r^2+1)(r^2+2r-1)/(4r(r^2-1))$
v_3	$(r^2+1)/(2(r+1))$	$-(r^2+1)/(2r(r+1))$
v_4	$(r^2+1)/(2r(r+1))$	$-(r^2+1)/(2(r+1))$
u_2^5	$(2/(r^2+1))^5 r^3(r+1)(r-1)^4$	$(-(2r^2/(r^2+1)))^5(1/r)^3((1/r)+1)((1/r)-1)^4$

Finally, from Table 2, we see that

$$Q(x_0) = Q((r'^3(r'+1)(r'-1)^4)^{1/5})$$

for $r' = r(\neq 0, \pm 1)$ or $r' = 1/r(\neq 0, \pm 1)$. □

Remark. The rational number r in part (ii) of Theorem 3.1 can be chosen to satisfy $r > 1$ since $Q((r^3(r+1)(r-1)^4)^{1/5}) = Q((s^3(s+1)(s-1)^4)^{1/5})$ for $s = -(1/r)$, $((r-1)/(r+1))$ and $((1+r)/(1-r))$.

Example 3.1. Taking $r = 2$ in Theorem 3.1, we see that the pure quintic field $Q(24^{1/5})$ is defined by the trinomial

$$X^5 + \frac{96}{5}X - \frac{192}{5},$$

or equivalently $(X \to 2X/5)$ by

$$X^5 + 750X - 3750.$$

Example 3.2. Taking $r = 3$ in Theorem 3.1, we see that the pure quintic field $Q(1728^{1/5}) = Q(12^{1/5})$ is defined by the trinomial

$$X^5 + \frac{1056}{125}X - \frac{26688}{625},$$

or equivalently $(X \to 2X/5)$ by

$$X^5 + 330X - 4170.$$

4. Pure quintic fields defined by X^5+aX^2+b. Let $a, b \in Q\backslash\{0\}$, and suppose that $X^5 + aX^2 + b$ is irreducible in $Q[X]$. Let x_0 be a real root of the equation $x^5 + ax^2 + b = 0$, so that $Q(x_0)$ is a quintic field. Suppose that $Q(x_0)$ is a pure field. Then $X^5 + aX^2 + b$ is both irreducible and solvable in $Q[X]$. It was shown in [7] that there are

essentially only five solvable irreducible quintic trinomials of the form $X^5 + aX^2 + b$. They can be taken to be

$$X^5 + 5X^2 + 3, \tag{4.1}$$

$$X^5 + 5X^2 - 15, \tag{4.2}$$

$$X^5 + 25X^2 + 300, \tag{4.3}$$

$$X^5 + 100X^2 + 1000, \tag{4.4}$$

$$X^5 + 250X^2 + 625. \tag{4.5}$$

Each of these polynomials has one real root which we denote by x_0. As $X^5 + aX^2 + b$ defines a pure quintic field, its Galois group must be F_{20}. This eliminates the polynomials (4.1)–(4.3) as their Galois group is D_5. For polynomial (4.4) we have $x_0 = 2^{3/5} - 2^{4/5} - 2^{6/5} - 2^{7/5}$ [7, p. 756] so that $Q(x_0) \subseteq Q(2^{1/5})$. However, $[Q(x_0) : Q] = [Q(2^{1/5}) : Q] = 5$ so that $Q(x_0) = Q(2^{1/5})$. Hence $X^5 + 100X^2 + 1000$ defines the pure quintic field $Q(2^{1/5})$. We now show that the polynomial (4.5) does not define a pure quintic field. We make use of the following three results.

Proposition 4.1 [11]. *If K is a pure quintic field, then $K = Q(z^{1/5})$, where z is a rational integer not divisible by the fifth power of any prime and $z \neq 0, \pm 1$, and the discriminant $d(K)$ of K is given by*

$$d(K) = 5^3 n^4 \quad \text{or} \quad 5^5 n^4,$$

where $n = \prod_{p|z} p \neq 1$.

Proposition 4.2 [4, pp. 60–61]. *Let θ be an algebraic integer, and let $K = Q(\theta)$. If the minimal polynomial over Q of θ is Eisensteinian with respect to the prime p, then the index $\operatorname{ind}\theta$ of θ in K is not divisible by p and the powers of p dividing the discriminant $d(\theta)$ of θ and the discriminant $d(K)$ of K are the same.*

Proposition 4.3 [10, Theorem 2]. *Let θ be a root of the irreducible polynomial $X^n + AX^s + B \in Z[X]$, where $1 \leq s < n$. Then the discriminant of θ is given by*

$$d(\theta) = (-1)^{n(n-1)/2} m^n B^{s-1} \cdot ((n')^{n'} B^{n'-s'} + (-1)^{n'-1}(n' - s')^{n'-s'}(s')^{s'} A^{n'})^m,$$

where

$$m = \gcd(n, s), \qquad n = mn', \qquad s = ms'.$$

We are now ready to prove that (4.5) does not define a pure field.

Proposition 4.4. *The polynomial* $f(X) = X^5 + 250X^2 + 625$ *does not define a pure quintic field.*

Proof. Let x_0 denote the unique real root of $f(X)$, and set $K = Q(x_0)$ so that K is a quintic field. We suppose that K is a pure field. Now set

$$g(X) = \frac{X^5}{5^4} f\left(\frac{5}{X}\right) = X^5 + 10X^3 + 5.$$

Let θ be the unique real root of $g(X)$ so that $Q(\theta) = K$. By Proposition 4.3 we have

$$d(\theta) = 5^7 \cdot 59^2.$$

Now $(\operatorname{ind}\theta)^2 d(Q(\theta)) = d(\theta)$ so we have

$$d(K) = \frac{5^7 \cdot 59^2}{(\operatorname{ind}\theta)^2}.$$

Since $g(X)$ is five-Eisenstein, by Proposition 4.2, we have $5 \nmid \operatorname{ind}\theta$. Hence,

$$d(K) = \begin{cases} 5^7 & \text{if } \operatorname{ind}\theta = 59, \\ 5^7 \cdot 59^2 & \text{if } \operatorname{ind}\theta = 1. \end{cases} \tag{4.6}$$

As K is a pure quintic field, we deduce from (4.6) and Proposition 4.1 that

$$d(K) = 5^7, \qquad n = 5, \qquad \operatorname{ind}\theta = 59, \tag{4.7}$$

and

$$z = 5^t, \quad t = 1, 2, 3 \text{ or } 4.$$

Thus $K = Q(z^{1/5}) = Q(5^{1/5})$. Therefore, K is also defined by $X^5 - 5$. Since $X^5 - 5$ is also five-Eisenstein, by Proposition 4.2, the power of

5 dividing $d(K)$ is the same as the power of 5 in the discriminant of X^5-5. However, this latter discriminant is 5^9, which contradicts (4.7). Hence, X^5+250X^2+625 does not define a pure quintic field. □

From the remarks at the beginning of this section and Proposition 4.4, we obtain the following result:

Theorem 4.1. *The only pure quintic field defined by a trinomial* X^5+aX^2+b, $a,b \in Q\backslash\{0\}$, *is* $Q(2^{1/5})$, *which is defined by* X^5+100X^2+1000.

5. $Q(p^{1/5})$ defined by a trinomial. In this section we show that the pure quintic field $Q(p^{1/5})$, where p is a prime, cannot be defined by a trinomial X^5+aX+b, where $a,b \in Q\backslash\{0\}$. We make use of the following result.

Proposition 5.1 [1, 5]. *The only integral solutions of* $x^5+y^5=2z^5$ *with* $xyz \neq 0$ *are* $(x,y,z)=(\lambda,\lambda,\lambda)$, $\lambda \in Z\backslash\{0\}$.

We are now ready to prove the following result.

Theorem 5.1. *Let* θ *be the unique real root of the solvable irreducible trinomial* X^5+aX+b, $a,b \in Q\backslash\{0\}$. *Then* $Q(\theta) \neq Q(p^{1/5})$ *for any prime* p.

Proof. Suppose that $Q(\theta)$ is a pure field. Then, by Theorem 3.1 (ii), we have

$$Q(\theta)=Q((r^3(r+1)(r-1)^4)^{1/5})$$

for some rational number $r \neq 0, \pm 1$. We set $r=x/y$, where x and y are integers with $\gcd(x,y)=1$ and $y>0$. As $r \neq 0$ we have $x \neq 0$ and as $r \neq \pm 1$ we have $x \neq \pm y$. Then

$$Q(\theta)=Q((x^3(x+y)(x-y)^4y^2)^{1/5}).$$

If $Q(\theta)=Q(p^{1/5})$ for some prime p, we must have

$$x^3(x+y)(x-y)^4y^2=p^iv^5, \quad \text{where } i=1,2,3 \text{ or } 4, \quad v \neq 0, \quad v \in Z. \tag{5.1}$$

We obtain a contradiction by showing that (5.1) cannot hold. We treat two cases according to whether x and y are of opposite parity or not.

Case 1. x and y are of opposite parity. In this case $x, y, x+y, x-y$ are pairwise prime and hence p^i divides exactly one of these numbers. By unique factorization the rest of the factorizations of these numbers are into fifth powers. We treat four subcases.

Subcase 1a. $x = p^iA^5$, $y = B^5$, $x+y = C^5$, $x-y = D^5$, for nonzero integers A, B, C and D. These equations imply that $C^5 + (-D)^5 = 2B^5$. As C, D, B are nonzero, by Proposition 5.1, we have $(C, -D, B) = (\lambda, \lambda, \lambda)$ for some nonzero integer λ. Hence $C = -D$ which implies $x = 0$, a contradiction.

Subcase 1b. $x = A^5$, $y = p^iB^5$, $x+y = C^5$, $x-y = D^5$, for nonzero integers A, B, C and D. These equations imply that $C^5 + D^5 = 2A^5$. As C, D and A are nonzero, by Proposition 5.1, we have $(C, D, A) = (\lambda, \lambda, \lambda)$ for some nonzero integer λ. Hence $C = D$ which implies that $y = 0$, a contradiction.

Subcase 1c. $x = A^5$, $y = B^5$, $x+y = p^iC^5$, $x-y = D^5$, for nonzero integers A, B, C and D. These equations imply that $A^5 + (-B)^5 = D^5$, which contradicts Fermat's last theorem.

Subcase 1d. $x = A^5$, $y = B^5$, $x+y = C^5$, $x-y = p^iD^5$, for nonzero integers A, B, C and D. These equations imply that $A^5 + B^5 = C^5$, which contradicts Fermat's last theorem.

Case 2. x and y are of the same parity. As x and y are of the same parity and coprime, x and y must both be odd. It follows that $x, y, (x+y)/2, (x-y)/2$ are pairwise prime and hence p^i exactly divides one of these numbers. By unique factorization the rest of the factorizations of these numbers are into fifth powers. Again we treat four subcases.

Subcase 2a. $x = p^iA^5$, $y = B^5$, $(x+y)/2 = C^5$, $(x-y)/2 = D^5$, for nonzero integers A, B, C, D. These equations imply that $C^5 + (-D)^5 = B^5$, which contradicts Fermat's last theorem.

Subcase 2b. $x = A^5$, $y = p^iB^5$, $(x+y)/2 = C^5$, $(x-y)/2 = D^5$, for

nonzero integers A, B, C, D. These equations imply that $C^5+D^5 = A^5$, which contradicts Fermat's last theorem.

Subcase 2c. $x = A^5$, $y = B^5$, $(x+y)/2 = p^iC^5$, $(x-y)/2 = D^5$, for nonzero integers A, B, C, D. These equations imply that $A^5+(-B)^5 = 2D^5$. Hence, by Proposition 5.1, we have $(A, -B, D) = (\lambda, \lambda, \lambda)$ for some $\lambda \in Z\backslash\{0\}$. Hence $A = -B$ and so $x = -y$, a contradiction.

Subcase 2d. $x = A^5$, $y = B^5$, $(x+y)/2 = C^5$, $(x-y)/2 = p^iD^5$ for nonzero integers A, B, C, D. These equations imply that $A^5 + B^5 = 2C^5$. Hence, by Proposition 5.1, we have $(A, B, C) = (\lambda, \lambda, \lambda)$ for some $\lambda \in Z\backslash\{0\}$. Hence $A = B$ and so $x = y$, a contradiction.

This completes the proof that $Q(\theta) \neq Q(p^{1/5})$ for any prime p. □

Finally, from Theorems 4.1 and 5.1, we have the following result.

Theorem 5.2. *The pure quintic field $Q(p^{1/5})$, where p is a prime, can only be defined by a trinomial of the form $X^5 + aX + b$ or $X^5 + aX^2 + b$, where $a, b \in Q\backslash\{0\}$, if $p = 2$, in which case it is defined by $X^5 + 100X^2 + 1000$.*

REFERENCES

1. P. Dénes, *Über die Diophantische Gleichung $x^l + y^l = cz^l$*, Acta Math. **88** (1952), 241–251.

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

3. S. Lang, *Algebra*, Addison Wesley Publ. Co., Reading, Mass., 1971.

4. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer, New York, 1989.

5. K.A. Ribet, *On the equation $a^p + 2^\alpha b^p + c^p = 0$*, Acta Arith. **79** (1997), 7–16.

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

7. ———, *On solvable quintics $X^5 + aX + b$ and $X^5 + aX^2 + b$*, Rocky Mountain J. Math. **26** (1996), 753–772.

8. B.K. Spearman, L.Y. Spearman and K.S. Williams, *The subfields of the splitting field of a solvable quintic trinomial $X^5 + aX + b$*, J. Math. Sci. **6** (1995), 15–18.

9. ———, *Quadratic subfields of the splitting field of a dihedral quintic field trinomial $x^5 + ax + b$*, New Zealand J. Math. **26** (1997), 293–299.

10. R.G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **12** (1962), 1099–1106.

11. J. Westlund, *On the fundamental number of the algebraic number-field* $k(\sqrt[p]{m})$, Trans. Amer. Math. Soc. **11** (1910), 388–392.

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, Ontario, Canada K1S 5B2
E-mail address: williams@math.carleton.ca