International Journal of Pure and Applied Mathematics
Volume 56 No. 3 2009, 345-352

TRINOMIALS $x^6 + Ax + B$ DEFINING SEXTIC FIELDS WITH A PURE CUBIC SUBFIELD

Melisa J. Lavallee[1], Blair K. Spearman[2] §
[1]Department of Mathematics, Statistics and Physics
The Irving K. Barber School of Arts and Sciences
University of British Columbia – Okanagan
3333, University Way, Kelowna, V1V 1V7, BC, CANADA
[1]e-mail: melisa_lavallee@hotmail.com
[2]e-mail: blair.spearman@ubc.ca

Abstract: We give a rational parametrization of irreducible trinomials $x^6 + Ax + B$ in $\mathbb{Q}[x]$ defining sextic fields containing a pure cubic subfield.

AMS Subject Classification: 12F10
Key Words: trinomial, sextic field, pure cubic field

1. Introduction

Let $f(x)$ be a polynomial with rational coefficients and let K denote a field extension of finite degree over $\mathbb{Q}$ the rational numbers. We say that $f(x)$ defines K, if $K = \mathbb{Q}(\theta)$ for some root θ of $f(x)$. In this paper we exhibit a method for determining families of polynomials defining number fields with a subfield condition. Imposing the subfield condition strongly influences the Galois group of the polynomial. A comprehensive survey of the problem of constructing families of polynomials with prescribed Galois group is given in Jensen, Ledet

Received: August 19, 2009

§Correspondence author

and Yui [2]. The mathematics involved in this paper uses only properties of the relative trace of number fields with calculations carried out using *MAPLE*. In spite of the elementary nature of this method, it has an additional useful feature. It often allows for the determination of all polynomials under consideration as is the case in this paper. For our purposes we need to recall the concept of a pure cubic field. A pure cubic field has the form $\mathbb{Q}(\sqrt[3]{m})$ for some integer m which is not a cube. A cubic polynomial with rational coefficients defines a pure cubic field if and only if it is irreducible and its discriminant is of the form $-3d^2$ for some $d \in \mathbb{Q}$. Our main theorem is a simple rational parametrization of all sextic trinomials $x^6 + ax + b$ defining sextic fields with a pure cubic subfield. We prove

Theorem 1. *Let A and B denote nonzero rational numbers such that $f(x) = x^6 + Ax + B$ is irreducible. Then $f(x)$ defines a sextic field containing a pure cubic subfield if and only if there exist rational numbers u and v such that*

$$\begin{aligned} A &= 12u(u^2-1)(u^2-9)(u^2-25)^2v^5, \\ B &= -(u^2-1)(u^2-25)^2(u^2+15)(u^4-30u^2+45)v^6. \end{aligned} \tag{1}$$

In Section 2, a rational parametrization of cubic trinomials $x^3 + ax + b$ defining pure cubic fields is given, along with a general condition for sextic fields to contain a cubic subfield. In Section 3 we prove Theorem 1.

2. Introductory Lemmas

Lemma 2. *Let a and b denote nonzero rational numbers and suppose that $g(x) = x^3 + ax + b$ defines a pure cubic field. Then there exist rational numbers p and q such that*

$$a = -3(p^2 - q^2),\ b = 2p(p^2 - q^2).$$

Proof. Since the discriminant of $g(x)$ must be equal to $-3d^2$ for some rational number d we have

$$-4a^3 - 27b^2 = -3d^2.$$

Using standard methods to parameterize the rational solutions of this equation we obtain solutions

$$(a, b, d) = \left(a, -\frac{4a^3 - 3t^2}{18t}, \frac{4a^3 - 3t^2}{6t}\right),$$

for an arbitrary nonzero rational number t. If

$$(p, q) = \left(\frac{4a^3 - 3t^2}{12at}, \frac{4a^3 + 3t^2}{12at} \right)$$

then

$$x^3 - 3(p^2 - q^2)x + 2p(p^2 - q^2) = x^3 + ax + \frac{4a^3 - 3t^2}{18t} = x^3 + ax + b = g(x)$$

which completes the proof. □

Lemma 3. *Let A and B denote non zero rational numbers and let $f(x) = x^6 + Ax + B$. Suppose that for some root θ of $f(x)$, $\mathbb{Q}(\theta)$ is a sextic extension field of $\mathbb{Q}$ containing a cubic subfield E. Then there exists a root $\theta' \neq \theta$ of $f(x)$ such that $\theta + \theta'$ is a root of an irreducible polynomial $x^3 + ax + b$ defining E.*

Proof. Let $K = \mathbb{Q}(\theta)$ denote the sextic field specified in the statement of the Lemma and E denote its cubic subfield. Since $[K : \mathbb{Q}] = 6$ we must have that $f(x)$ is irreducible. Let $g(x)$ be the minimal polynomial for θ over E. Then $g(x)$ divides $f(x)$ in $E[x]$ and $g(x)$ must have degree equal to $[K : E] = 2$. Since K/E is a separable extension there exists a root $\theta' \neq \theta$ of $g(x)$ (and of $f(x)$) such that $g(x) = (x - \theta)(x - \theta') \in E[x]$ so that $\theta + \theta' \in E$. Since the only proper subfields of E are E and $\mathbb{Q}$, $\theta + \theta'$ is either the root of an irreducible cubic polynomial in $\mathbb{Q}[x]$ or is equal to a rational number. If there was a rational number r such that $\theta + \theta' = r$ then taking the trace of both sides of this equation from K to $\mathbb{Q}$ gives $6r = Tr_{K/\mathbb{Q}}(r) = Tr_{K/\mathbb{Q}}(\theta + \theta') = Tr_{K/\mathbb{Q}}(\theta) + Tr_{K/\mathbb{Q}}(\theta^{\,prime}) = 0 + 0 = 0$ so that $r = 0$. If $r = 0$, we deduce from $\theta + \theta' = 0$ that both θ and $-\theta$ are roots of $f(x)$ so that $f(x) = f(-x)$ by irreducibility of the monic polynomial $f(x)$. This is impossible since $B \neq 0$. Hence $\theta + \theta'$ is the root of an irreducible cubic polynomial. Calculating the trace of $\theta + \theta'$ from E to $\mathbb{Q}$ by using [1, p. 160, Proposition 4.3.2(1)] we determine that $Tr_{E/\mathbb{Q}}(\theta + \theta') = \frac{1}{2} Tr_{K/\mathbb{Q}}(\ \theta + \theta') = 0$ by the argument earlier in the proof. Thus $\theta + \theta'$ is the root of an irreducible cubic trinomial of the form $x^3 + ax + b$. □

3. Proof of Theorem

Proof. We begin by supposing that $f(x) = x^6 + Ax + B$ defines a sextic field K containing a pure cubic subfield. Let θ be a root of $f(x)$ such that $K = \mathbb{Q}(\theta)$. By Lemma 2 there exists a root $\theta' \neq \theta$ of $f(x)$ such that $\theta + \theta'$ is a root of an irreducible cubic trinomial as characterized in Lemma 1. Before using Lemma 1 we must find a polynomial whose coefficients are a function of

A and B and which has $\theta + \theta'$ as a root. Such a polynomial can be calculated from $f(x)$ by using resultants [1, p. 157] or [3]. We calculate this polynomial, denoted by $t(x)$ using

$$t(x) = \sqrt{\frac{\text{Resultant}((f(x-X), f(X))}{2^6 f(x/2)}}. \tag{2}$$

MAPLE gives this polynomial as

$$t(x) = x^{15} - 10Ax^{10} - 26Bx^9 - 12A^2x^5 + 18ABx^4 - 27B^2x^3 - A^3. \tag{3}$$

By Lemma 1 there exist nonzero rational numbers p and q such that the minimal polynomial over $\mathbb{Q}$ of $\theta + \theta'$ is the cubic polynomial $g(x)$ given by

$$g(x) = x^3 - 3(p^2 - q^2)x + 2p(p^2 - q^2).$$

At this point it is convenient to apply scaling in order to simplify the algebraic calculations. If we scale the roots of $f(x)$ by $x \to x/c$ then $f(x)$ becomes $x^6 + c^5Ax + c^6B$ and $g(x)$ becomes $x^3 - 3(p^2 - q^2)c^2x + 2p(p^2 - q^2)c^3$. We choose $c = 1/p$ then set $z = q/p$. Summarizing, we assume that by scaling if necessary, for $f(x) = x^6 + Ax + B$, we have $t(x)$ as given in (3) and $g(x) = x^3 + 3(z^2 - 1)x - 2(z^2 - 1)$ for some rational number z. Finally, when convenient we may write $g(x) = x^3 + 3rx - 2r$ where $r = z^2 - 1$. We note that irreducibility of $g(x)$ requires $r \neq 0$, that is $z \neq \pm 1$. The minimal polynomial of $\theta + \theta'$, namely $g(x)$ must divide $t(x)$. We formally divide $t(x)$ by $g(x) = x^3 + 3rx - 2r$ using *MAPLE* and equate each of the coefficients of x^2, x and the constant term to zero. This gives us the following three equations

$$\begin{aligned} &6r(4A^2 + (9B + 135r^3 - 60r^2)A + 6r^2(39B + 81r^3 - 20r^2)) = 0, \\ &r(108rA^2 + (-36B - 2160r^3 + 80r^2)A - 81B^2 + 234r^2(9r - 4)B \\ &\qquad + 3r^4(729r^2 - 1620r + 80)) = 0, \\ &A^3 - 72r^2A^2 + 1080r^4A - 2r(-27B^2 + 26r^2(27r - 4)B \\ &\qquad + r^4(729r^2 - 1080r + 16)) = 0. \end{aligned} \tag{4}$$

We will solve these equations for A and B. Notice that if $A = -26r^2$ then substituting for A into the first equation in (4) would yield

$$-672r^5(27r - 37) = 0$$

or equivalently

$$-672(z^2 - 1)^5(27z^2 - 64) = 0$$

which has no rational solutions except $z = \pm 1$ which are not allowed as stated earlier in this proof. Therefore we may solve the first equation in (4) for B giving

$$B = \frac{-4A^2 + (-135r^3 + 60r^2)A + 6r^4(-81r + 20)}{9(A + 26r^2)}. \tag{5}$$

We substitute B into the second equation in (4) giving

$$\frac{4r^2FG}{(A+26r^2)^2} = 0, \tag{6}$$

where

$$\begin{aligned} F &= 3A^2 - 5r^2A - 1323r^5 - 345r^4, \\ G &= 9A^2 + 12r(15r+8)A + 4r^3(81r+32). \end{aligned} \tag{7}$$

We have already seen that $r \neq 0$ so we conclude that if (6) holds then either $F = 0$ or $G = 0$. Suppose first that $F = 0$. Viewing this equation as a quadratic in A we see that its discriminant must be equal to a perfect square in $\mathbb{Q}$. This discriminant is equal to

$$49r^4(324r + 85)$$

or

$$49(z^2-1)^4(324z^2 - 239).$$

Using standard parametrization methods we find that

$$z = \frac{w^2 + 239}{36w}. \tag{8}$$

Substituting $r = z^2 - 1$, then the equation for z given in (8) into $F = 0$ using (7) and solving for A gives two solutions for A in terms of w. Since the second solution is equivalent to the first under the transformation $w \to -w$, we may choose the first solution which is given by

$$A = \frac{(7w^2 + 10w - 1673)(w^2 - 36w + 239)^2(w^2 + 36w + 239)^2}{2^{10}3^9w^5}. \tag{9}$$

Substituting $r = z^2-1$, then the equation for z from (8) and finally the equation for A from (9) into (5) gives B as

$$\begin{aligned} B = -\big(&5(w^4 - 16w^3 - 594w^2 + 3824w + 57121) \\ &\times(w^2 - 36w + 239)^2(w^2 + 36w + 239)^2\big)\left(2^{12}3^{11}w^6\right)^{-1}. \end{aligned} \tag{10}$$

These values of A and B given in (9) and (10) do not satisfy the third equation (4) so we do not consider them further. Next we turn to the equation $G = 0$. Again viewing this equation as a quadratic in A we see that its discriminant must be equal to a perfect square in $\mathbb{Q}$. This discriminant is equal to

$$2^8 3^2 r^2(r+1)(9r+4)$$

or

$$2^8 3^2 (z^2-1)^2(9z^2 - 5).$$

Using standard parametrization methods we find that

$$z = -\frac{u^2+5}{6u} \tag{11}$$

for some nonzero rational number u. Substituting $r = z^2 - 1$, then the equation for z given in (11) into $G = 0$ using (7) and solving for A gives the following solutions for A in terms of v

$$\begin{aligned} A &= -\frac{u^8 - 60u^6 + 1134u^4 - 6700u^2 + 5625}{648u^4}, \\ A &= -\frac{9u^8 - 268u^6 + 1134u^4 - 1500u^2 + 625}{648u^4}. \end{aligned} \tag{12}$$

Since the second solution is equivalent to the first under the transformation $u \to 5/u$, we may choose the first solution from (12). Substituting $r = z^2 - 1$, then the equation for z from (11) and finally the first equation for A from (12) into (5) gives B as

$$B = -\frac{u^{12} - 66u^{10} + 1035u^8 + 10580u^6 - 298425u^4 + 708750u^2 - 421875}{2^6 3^6 u^6}. \tag{13}$$

The pair (A, B) given by the first equation in (12) and equation (13) satisfy all three equations in (4) so we have indeed found all rational solutions to (4) and hence the set of trinomials $x^6 + Ax + B$ that we seek. To obtain the final values of A and B as stated in the theorem we introduce a scaling factor $x \to x/(-6uv)$ and factor, yielding

$$\begin{aligned} A &= 12u(u^2-1)(u^2-9)(u^2-25)^2v^5, \\ B &= -(u^2-1)(u^2-25)^2(u^2+15)(u^4-30u^2+45)v^6. \end{aligned}$$

Conversely we show that if $f(x) = x^6 + Ax + B$ is irreducible and the nonzero rational numbers A and B are given by (1), then $f(x)$ defines a sextic field containing a pure cubic subfield. For convenience, by scaling if necessary we may assume that $v = 1$. Let θ denote a root of $f(x)$ and set $K = \mathbb{Q}(\theta)$. Since $f(x)$ is irreducible we have $[K : \mathbb{Q}] = 6$. We will give explicitly a polynomial $g(x)$ defining the pure cubic subfield of K. Define $g(x)$ by

$$g(x) = x^3 + 3(u^2-1)(u^2-25)x + 12u(u^2-1)(u^2-25). \tag{14}$$

Let α denote a root of $g(x)$. Define the quadratic polynomial $q(x)$ in $\mathbb{Q}(\alpha)[x]$ by

$$\begin{aligned} q(x) = (u^2+5)x^2 &\\ - (u^2+5)\alpha x + 10\alpha^2 + 2(u^3 - 25u)\alpha - (u^2-1)(u^2-15)(u^2-25). & \end{aligned}$$

A *MAPLE* calculation shows that

$$\text{Resultant}(f(x), q(x), x)) = -g(\alpha)\, h(\alpha) = 0,$$

where

$$h(\alpha) = (u^2 - 25)^2(u^2 + 5)(R\alpha^2 + S\alpha + T)$$

and

$$\begin{aligned} R =& 66000u^6 - 4170000u^4 + 3150000u^2 - 1350000, \\ S =& -120u(u^{12} - 40u^{10} + 825u^8 + 600u^6 - 200125u^4 + 370000u^2 \\ & - 208125), \\ T =& u^{18} - 75u^{16} + 2880u^{14} - 69000u^{12} + 1100250u^{10} - 18711750u^8 \\ & amp; + 210245000u^6 - 159150000u^4 - 17971875u^2 - 18984375. \end{aligned}$$

Therefore there exists a conjugate θ' of θ over $\mathbb{Q}$ such that $q(\theta') = 0$. Next we evaluate the field extension degrees $[\mathbb{Q}(\theta', \alpha) : \mathbb{Q}]$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Note that

$$[\mathbb{Q}(\theta', \alpha) : \mathbb{Q}] = [\mathbb{Q}(\theta', \alpha) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 2 \cdot 3 = 6, \tag{15}$$

since θ' satisfies a quadratic polynomial over $\mathbb{Q}(\alpha)$ and α is the root of a cubic polynomial in $\mathbb{Q}[x]$. However

$$[\mathbb{Q}(\theta', \alpha) : \mathbb{Q}] = [\mathbb{Q}(\theta', \alpha) : \mathbb{Q}(\theta')][\mathbb{Q}(\theta') : \mathbb{Q}] \geq 1 \cdot 6 = 6 \tag{16}$$

since $[\mathbb{Q}(\theta') : \mathbb{Q}] = [K : \mathbb{Q}] = 6$. Combining (15) and (16) gives the following equalities.

$$\begin{aligned} &[\mathbb{Q}(\theta', \alpha) : \mathbb{Q}] = 6 = [\mathbb{Q}(\theta') : \mathbb{Q}], \\ &[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3. \end{aligned} \tag{17}$$

It follows that the cubic polynomial $g(x)$ is irreducible and $\mathbb{Q}(\alpha)$ is a cubic subfield of $\mathbb{Q}(\theta')$. It is easily checked that the discriminant of $g(x)$ is equal to -3 times a square so that $\mathbb{Q}(\alpha)$ is a pure cubic field. Finally, since $\mathbb{Q}(\theta')$ is isomorphic to the field $K = \mathbb{Q}(\theta)$, K contains a pure cubic subfield as well, which completes the proof. □

A typical polynomial in this family has Galois group isomorphic to "6T11" in *MAPLE* or 2wrS(3).

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag (2000).

[2] C.U. Jensen, A. Ledet, N. Yui, *Generic Polynomials, Constructive Aspects*

of the Inverse Galois Problem, Mathematical Sciences Research Institute Publications, Cambridge University Press (2002).

[3] L. Soicher, M. Comp. Sci. Thesis, Concordia University, Montréal (1981).