JP Jour. Algebra, Number Theory & Appl. **6**(1) (2006), 117-127

SOLVABLE BRIOSCHI QUINTICS OVER $\mathbb{Q}$

MICHELE ELIA
Dipartimento di Elettronica, Politecnico di Torino
Corso Duca degli Abruzzi 24, 10129 *Torino, Italy*

Abstract

A Brioschi quintic is a form of the general quintic whose coefficients are integer polynomial functions in a single variable. Viewed as an algebraic curve, it is a smooth, irreducible curve admitting of a rational parametric representation. Thus Brioschi quintics solvable by radicals with one rational root are numerous, however, irreducible quintics may also be solvable by radicals. In this paper, solvable Brioschi quintics with rational coefficients are described in full. Remarkably, any Brioschi quintic with integer coefficients is unsolvable by radicals.

1. Introduction

A Brioschi quintic

$$B_5(x, Z) = x^5 - 10Zx^3 + 45Z^2x - Z^2 \tag{1}$$

is a form of the general quintic that depends on a single parameter Z. The study of Brioschi quintics was primarily motivated by numerical computation of their roots via modular functions [1, 8, 9]. This intriguing way to solve quintics is now obscured by efficient numerical methods for computing the roots of any polynomial using the power of today's computers. Nevertheless, the solution of quintics by radicals still deserves considerable attention for theoretical and aesthetical reasons. Notably, the problem has been settled for Bring-Jerrard quintics with integer

2000 Mathematics Subject Classification: 12E05, 12E10.

Keywords and phrases: quintic, Galois group, Diophantine equations.

Received October 17, 2005

coefficients, [6, 11]. However, Brioschi quintics are unsolvable when Z is an integer, whereas with rational coefficients they may be either reducible or irreducible and if solvable, then their Galois group is isomorphic to the Frobenius group.

2. Irreducible Brioschi Quintics

Let $\mathrm{Gal}(p(x)|\mathbb{Q})$ denote the Galois group of a polynomial $p(x)$ over $\mathbb{Q}$. Any irreducible quintic $B_5(x, Z)$ is unsolvable by radicals, if $\mathrm{Gal}(B_5(x, Z)|\mathbb{Q})$ is the symmetric group S_5, whereas it is solvable, if $\mathrm{Gal}(B_5(x, Z)|\mathbb{Q})$ is either the cyclic group $\mathcal{C}_5$ of order 5, or the dihedral group $\mathcal{D}_5$ of order 10, or the Frobenius (metacyclic) group $\mathcal{F}_{20}$ of order 20. Although any quintic can be transformed into some Brioschi quintic, the special form of Brioschi quintic coefficients, when constrained to be rational, fixes their Galois groups.

Theorem 1. *If $B_5(x, Z)$ is irreducible over the field of rational $\mathbb{Q}$, then $\mathrm{Gal}(B_5(x, Z)|\mathbb{Q})$ is isomorphic either to the symmetric group S_5 or to the Frobenius group $\mathcal{F}_{20}$.*

Proof. Since the discriminant $\Delta = 5^5 Z^8 (1728Z - 1)^2$ of $B_5(x, Z)$ with respect to x is not a perfect square over $\mathbb{Q}$ when Z is rational, $\mathrm{Gal}(B_5(x, Z)|\mathbb{Q})$ cannot be a subgroup of the alternating group $\mathcal{A}_5$ [5, p. 397]. Thus the Galois group of a solvable Brioschi quintic is necessarily isomorphic to $\mathcal{F}_{20}$.

If Z is transcendental over $\mathbb{Q}$, then any $B_5(x, Z)$ is irreducible over the transcendental extension field $\mathbb{Q}(Z)$, and its Galois group is S_5. Irreducibility is immediately assessed by a specialization principle [12, 15], since $B_5(x, 1)$ is easily checked to be irreducible modulo 19. The proof that $B_5(x, Z)$ is unsolvable makes use of Theorem 3, whose proof requires a criterion for checking when an irreducible quintic is solvable over $\mathbb{Q}$. To this aim, a theorem [2, 5, 13] will be used, which is quoted from [5, p. 389], in a form specialized to Brioschi quintics, without proof.

Theorem 2. *The irreducible quintic* $B_5(x, Z)$, $Z \in \mathbb{Q}$ *is solvable by radicals if and only if the polynomial*

$$\begin{aligned} q_{20}(x, Z) = {} & x^6 + 360Z^2x^5 + 54000Z^4x^4 \\ & + (6480000Z^6 - 1250Z^5)x^3 \\ & + (583200000Z^8 - 225000Z^7)x^2 \\ & + (18662400000Z^{10} - 2700000Z^9 - 3125Z^8)x \\ & + 186624000000Z^{12} + 108000000Z^{11} - 109375Z^{10} \end{aligned} \tag{2}$$

has a rational root. If this is the case, then the sextic $q_{20}(x, Z)$ *factors into the product of a linear polynomial and an irreducible quintic.*

Since a Brioschi quintic is irreducible when Z is transcendental over $\mathbb{Q}$, (1) defines an algebraic curve in the (x, Z)-plane, which turns out to be a smooth irreducible curve which is isomorphic to $\mathbb{P}^1$ (curve of genus 0). Thus it admits of a one-parametric representation with rational functions, and a classical theorem of algebraic geometry states that over $\mathbb{Q}$ it is isomorphic to either a line or a plane conic [4, p. 4] and [10, Theorem 16, p. 417]. Since (1) is a quadratic polynomial in Z, the following representation is immediately obtained by requiring that the discriminant $\Delta_Z = -4(20x - 1)x^5$ be a perfect square:

$$\begin{cases} x = \dfrac{q^2}{20q^2 + 1} \\ Z = \dfrac{q^5}{(5q - 1)(20q^2 + 1)^2}. \end{cases} \tag{3}$$

Furthermore, by setting $20q^2 + 1 = p$, an isomorphism with a plane conic (parabola) is obtained

$$\begin{cases} x = \dfrac{q^2}{p} \\ Z = \dfrac{q^5}{(5q - 1)p^2} \end{cases} \Leftrightarrow \begin{cases} q = \dfrac{-Z}{x^2 - 5Z} \\ p = \dfrac{Z^2}{x(x^2 - 5Z)^2}. \end{cases}$$

Since not every rational Z is given by (3) with a rational q, the characterization of all solvable quintics with rational Z is not entirely trivial. The following theorem is a completion of a theorem given in [14, p. 449], and characterizes, using the same terminology as [14], the parametric family of solvable irreducible Brioschi quintics.

Theorem 3. *If $B_5(x, Z)$, $Z \in \mathbb{Q}$ is irreducible over $\mathbb{Q}$ and can be solved by radicals, then*

$$Z = \frac{5 - q}{(q^2 + 12q + 40)(q^2 - 6q + 4)^2}, \tag{4}$$

with $q \in \mathbb{Q}$. Conversely, if Z is given by (4), then $B_5(x, Z)$ is always solvable by radicals, but it is irreducible if and only if $q \neq 5 + \frac{1}{25m^5 + 25m^4 + 15m^3 + 5m^2 + m}$ for some $m \in \mathbb{Q}$.

Proof. Let $B_5(x, Z)$ be irreducible and solvable by radicals. Theorem 1 implies that two rational numbers t and Z exist such that $q_{20}(t, Z) = 0$. The substitution $x = tZ^2 - 60Z^2$ does not change the rational character of the roots of (2), and the resulting sextic in t,

$$Q_{20}(t, Z) = (-9331200000t + 2160000t^3 + 233280000000 + t^6)Z^2 + (10800000t - 270000000 - 1250t^3)Z - 3125t + 78125 \tag{5}$$

is a quadratic equation in Z. For any rational root t of $Q_{20}(t, Z)$, Z is rational if and only if discriminant $\Delta_Z = 12500(t + 100)t^6$ is a square, that is, $t + 100 = 5q^2$ with $q \in \mathbb{Q}$. Substituting $t = 5q^2 - 100$ in (5), and solving for Z, both roots are given as a function of q ($-q$ gives the second root), as

$$Z = \frac{5 - q}{(q^2 + 12q + 40)(q^2 - 6q + 4)^2}. \tag{6}$$

Then $Q_{20}(t, Z)$ splits as

$$Q_{20}(t, Z) = \frac{(t + 100 - 5q^2)Q_{20}^{(5)}(t, Z)}{(q^2 + 12q + 40)^2(q^2 - 6q + 4)^4}$$

with

$$Q_{20}^{(5)}(t, Z) = (q-5)^2 t^5 + 5(q^2-20)(q-5)^2 t^4 + 25(q-5)^2(q^2-20)^2 t^3 + 125(q-5)(q+5)(q^2-20)^3 t^2 + 625(q-5)(q+5)(q^2-20)^4 t - 15625(q^2-20)^5,$$

where quintic $Q_{20}^{(5)}(t, Z)$ is irreducible over $\mathbb{Q}$. Conversely, if Z is of the form (6), then $Q_{20}(t, Z)$ splits into a linear factor and quintic $Q_{20}^{(5)}(t, Z)$. Thus $B_5(x, Z)$ is always solvable, although, to a reducible $Q_{20}^{(5)}(t, Z)$ corresponds a reducible $B_5(x, Z)$. The factorization of $Q_{20}^{(5)}(t, Z)$ is clarified, if the substitutions are done in the order $q = k + 5$, $\theta = 5t(k^2 + 10k + 5)$, and $k = 1/z$, which does not alter the degrees of factors of $Q_{20}^{(5)}(t, Z)$, obtaining $Q(\theta, z) = \theta^5 + \theta^4 + \theta^3 + (1+10z)\theta^2 + (1+10z)\theta - 5z^2$. This polynomial defines an algebraic curve admitting of the following parametric rational representation

$$\begin{cases} \theta = 5m^2 \\ z = 25m^5 + 25m^4 + 15m^3 + 5m^2 + m \end{cases} \qquad m \in \mathbb{Q}.$$

Then $Q(\theta, z)$ splits into $\theta - 5m^2$ and a quartic factor, which turns out to be always irreducible when z is rational: first, let the z denominator be taken prime with 3. Then z mod 3 is either 0, 1 or 2, and the three decompositions

$$\begin{cases} \theta(\theta^4 + \theta^3 + \theta^2 + \theta + 1) & z = 0 \bmod 3 \\ (\theta^4 + \theta^2 + 2\theta + 1)(\theta + 1) & z = 1 \bmod 3 \\ (\theta^4 + \theta^2 + \theta + 1)(\theta + 1) & z = 2 \bmod 3 \end{cases}$$

show that quartic factors of $Q(\theta, z)$ are irreducible. Second, let the z denominator be divisible by 3^m, writing $z_0/3^m$ for z, with the z_0 denominator prime with 3, after some simplification we get

$$Q(\theta, z) = 9^m\theta^5 + 9^m\theta^4 + 9^m\theta^3 + 9^m\theta^2 + 10 \cdot 3^m\theta^2 z_0 + 9^m\theta + 10 \cdot 3^m\theta z_0 - 5z_0^2$$

which may be split into irreducible polynomials necessarily of the forms $(3^m\theta^3 + 3^m b\theta^2 + 3^m c\theta + u_1)$ and $(3^m\theta^2 + 3^m a\theta + u_0)$, with u_0 and u_1 units modulo 3, as a simple argument modulo 3^m shows. The proof is completed by observing that the coefficient of θ^3 in the product is $3^m(u_0 + 3^m ab + 3^m c)$ and cannot be equal to the coefficient 3^{2m} of z^3, since u_0 is a unit modulo 3.

Theorem 4. *Any Brioschi quintic $B_5(x, Z)$, with integer $Z \neq 0$, is irreducible over $\mathbb{Q}$, and its Galois group is S_5.*

Proof. The condition $Z \neq 0$ excludes the trivial case $B_5(x, 0) = x^5$. If $B_5(x_0, Z)$ splits over $\mathbb{Q}$, then either at least one linear factor or two irreducible factors occur

$$B_5(x, Z) = (x - x_0)(x^4 + x_0x^3 + Bx^2 + Cx + D), \tag{7}$$

$$B_5(x, Z) = (x^2 + Ax + B)(x^3 - Ax^2 + Cx + D), \tag{8}$$

with $x_0, A, B, C, D \in \mathbb{Z}$ by a theorem of Gauss'.

Factorization (7) is easily excluded, since $B_5(x_0, Z) = 0$ has an integer solution Z if and only if its discriminant Δ_Z is a square integer, namely $-20x_0^2 + x_0 = w^2$. But, writing this equation as $80w^2 + (40x_0 - 1)^2 = 1$, it is clear that the only integer solution is $w = x_0 = 0$, giving $Z = 0$, which is excluded by hypothesis. Factorization (8) is excluded as follows. Comparing the coefficients of equal x powers on both sides of (8), produces the system

$$\begin{cases} B + C - A^2 = -10Z, & BC + AD = 45Z^2, \\ D + A(C - B) = 0, & BD = -Z^2. \end{cases} \tag{9}$$

Substituting $C = -B + A^2 - 10Z$ and $D = A(2B - A^2 + 10Z)$, computed from the first two equations, in the other two equations, then A, B and Z satisfy the following system:

$$\begin{cases} B(-B + A^2 - 10Z) + A^2(2B - A^2 + 10Z) = 45Z^2, \\ BA(2B - A^2 + 10Z) = -Z^2. \end{cases}$$

The resultant with respect to B yields an integer Diophantine equation connecting A and Z,

$$(3600A^2 - 80A + 1)Z^4 + (100A^4 - 40A^3)Z^3$$

$$+ (-165A^6 + 11A^5)Z^2 + 30A^8Z - A^{10} = 0. \tag{10}$$

Evidently $A^3 \mid Z^4$ and, a fortiori, $A \mid Z^2$. Thus, dividing each term in (10) by A^4,

$$3600\left(\frac{Z^2}{A}\right)^2 + 100Z^3 - 165A^2Z^2 - 80\frac{Z^4}{A^3} + 30A^4Z$$

$$- 40\frac{Z^3}{A} - A^6 + 11AZ^2 + \frac{Z^4}{A^4} = 0,$$

it is seen that $A \mid Z$. Substituting $Z = zA$ in (10), the resulting equation shows immediately that $A^2 \mid z^4$, thus $A \mid z^2$, and certainly $A \mid z^3$. Then, dividing by A^3, the resulting expression

$$(3600A^2 - 80A + 1)\frac{z^4}{A^3} + (-40 + 100A)\frac{z^3}{A} + (11 - 165A)z^2 + 30A^2z - A^3 = 0$$

shows that $A^3 \mid z^4$ and, together with $A \mid z^2$, implies $A^4 \mid z^6 \Rightarrow A^2 \mid z^3$. Thus, dividing again by A, the final expression shows that $A \mid z$. Finally, the quadratic equation for A, obtained by setting $z = Ay$,

$$(3600y^4 + 100y^3 - 165y^2 + 30y - 1)A^2 + (-40y^3 - 80y^4 + 11y^2)A + y^4 = 0,$$

admits of an integer solution only if the discriminant Δ_A is a perfect square, but

$$\Delta = -125(16y^2 + 4y - 1)(-1 + 2y)^2y^4$$

is not positive for any integer y, hence A cannot be an integer. Since $B_5(x, Z)$ is irreducible for any given Z, by Theorem 3 its Galois group is $\mathcal{F}_{20}$, if Z admits of a representation (4) for some rational q. Setting

$q = \dfrac{5u+v}{u}$, with u and v relatively prime integers, the expression

$$Z = -\frac{vu^5}{(125u^2+22uv+v^2)(-u^2+4uv+v^2)^2}$$

shows that no rational q gives an integer Z: in the last expression the numerator is relatively prime with the denominator, unless v is a power of 5. If v is a power of 5, after simplification a non-integer is still obtained. This completes the proof.

3. Reducible Brioschi Quintics

In the previous section it was shown that Brioschi quintics over $\mathbb{Z}$ are irreducible and unsolvable by radicals. On the other hand, equations (3) show that Brioschi quintics over $\mathbb{Q}$ are reducible, in particular they trivially split into a linear factor, which may have multiplicity greater than 1. The linear factor has multiplicity greater than 1 if and only if the discriminant $3125Z^8(1728Z-1)^2$ with respect to x is zero. This occurs only for $Z = 0$, which is trivial, and $Z = 1/1728$, to which corresponds the factorization

$$B_5\left(x, \frac{1}{1728}\right) = \left(x^2+\frac{1}{8}x+\frac{1}{216}\right)\left(x-\frac{1}{24}\right)^3.$$

To complete the factorization of $B_5(x, Z)$, it remains to settle the splitting into a pair of irreducible factors of degree 2 and 3, respectively. To this aim, it is convenient to perform the substitutions $x = \dfrac{X}{W}$ and $Z = \dfrac{T}{W}$, which do not change the irreducible character of the factors. Comparing the coefficients of equal X powers on both sides of

$$X^5 - 10WTX^3 + 45W^2T^2X - W^3T^2 = (X^2 - aX + b)(X^3 + aX^2 + cX + d)$$

the following system is obtained

$$\begin{cases} c = -b + a^2 - 10WT, & bc - ad = 45W^2T^2 \\ d = a(-b+c) = a(-2b + a^2 - 10WT), & bd = -W^3T^2. \end{cases}$$

The equation $d = a(-b + c)$ shows that $a \neq 0$, for otherwise $d = 0$ contradicts the assumption $Z \neq 0$. Using the first two equations to eliminate d and c, the system

$$\begin{cases} 45W^2T^2 - (-10b + 10a^2)WT + a^4 + b^2 - 3ba^2 = 0 \\ W^3T^2 - 10baWT + ba^3 - 2b^2a = 0 \end{cases}$$

is obtained, thus W is computed as a root of their resultant with respect to T,

$$\begin{aligned} R(W) &= W^4[(a^8 + b^4 - 6ba^6 - 6b^3a^2 + 11b^2a^4)W^2 \\ &\quad + (80b^4a + 450b^2a^5 - 90a^7b - 530b^3a^3)W \\ &\quad - 8100b^3a^4 + 3600b^4a^2 + 2025b^2a^6] \\ &= W^4r(W). \end{aligned}$$

Since $W = 0$ is excluded, a rational W is obtained if the discriminant of $r(W)$ is a perfect square, which amounts to requiring that a and b satisfy the Diophantine equation $-5(a^2 - 4b)(4a^2 - b) = u^2$. From its one-parametric solution [3], the following rational Z is obtained

$$Z = \frac{(5q^2 + 10q - 4)^5}{1728(1 + 5q^2)(1 + 5q^2)^2(5q^2 + 25q + 11)^2} \quad q \in \mathbb{Q}. \tag{11}$$

For example, $q = -2/5$ yields $Z = \dfrac{-1}{147}$ and the quintic

$$\begin{aligned} B\left(x, \frac{-1}{147}\right) &= x^5 + \frac{10}{147}x^3 + \frac{5}{2401}x - \frac{1}{21609} \\ &= \left(x^2 - \frac{1}{7}x + \frac{1}{21}\right)\left(x^3 + \frac{1}{7}x^2 + \frac{2}{49}x - \frac{1}{1029}\right). \end{aligned}$$

The polynomial $B_5(x, Z)$ may split into a linear factor and a pair of 2-degree polynomials. This occurs if and only if Z admits both representations (3) and (11) at the same time. For example, $q = -11/73$ in (3), and $q = -73/110$ in (11) yield the same $Z = 161051/7686016128$,

and the quintic

$$B_5(x, Z) = x^5 - \frac{805255}{3843008064}x^3 + \frac{129687123005}{6563871546652901376}x - \frac{25937424601}{59074843919876112384}$$

factors as

$$\left(x - \frac{121}{7749}\right)\left(x^2 + \frac{1707552}{62487936}x + \frac{14641}{62487936}\right)\left(x^2 - \frac{1428768}{122000256}x + \frac{14641}{122000256}\right).$$

This completes the characterization of solvable Brioschi quintics over the rational field. As a simple application, let us find every Brioschi quintic that, in the isomorphism with a conic curve, corresponds to a point (q, p) with integer coordinates which satisfy the further condition of p being a square integer. Coordinates q and p are expressed in terms of Fibonacci and Lucas numbers, specifically $q = F_{6n}/4$ and $p = L_{6n}^2/4$. These quintics are always solvable by radicals.

References

[1] B. Berndt, B. Spearman and K. Williams, Commentary on an unpublished lecture by G. N. Watson on solving the quintic, Math. Intelligencer 24(4) (2002), 15-33.

[2] W. E. H. Berwick, The condition that a quintic equation should be solvable by radicals, Proc. London Math. Soc. (2) 14 (1915), 301-307.

[3] R. D. Carmichael, Diophantine Analysis, Dover, New York, 1959.

[4] J. W. S. Cassels, Lectures on Elliptic Curves, Cambridge University Press, Cambridge, 1995.

[5] D. S. Dummit, Solving solvable quintics, Math. Comp. 57(195) (1991), 387-401.

[6] M. Elia and P. Filipponi, Equations of the Bring-Jerrard form, the golden section and square Fibonacci numbers, Fibonacci Quart. 36(3) (1998), 282-286.

[7] E. Galois, Écrits et Mémoires Mathématiques d'Évariste Galois, R. Borgne and J. P. Azra, eds., Gauthier-Villars, Paris, 1962.

[8] R. B. King, Beyond the Quartic Equation, Birkhäuser, Basel, 1996.

[9] F. Klein, The Icosahedron and the Solution of Equations of the Fifth Degree, Dover, New York, 1956.

[10] J. Kollar, Which are the simplest algebraic variety?, Bull. Amer. Math. Soc. 38(4) (2001), 409-433.

[11] S. Rabinowitz, The factorisation of $x^5 \pm x + n$, Math. Mag. 61(3) (1988), 191-193.

[12] J. P. Serre, Topics in Galois Theory, Jones and Bartlett Publishers, Boston, 1992.

[13] J. Shurman, Geometry of the Quintic, Wiley, New York, 1997.

[14] B. K. Spearman, Solvable Brioschi resolvents, AAECC 13 (2003), 447-452.

[15] B. L. van der Waerden, Modern Algebra, Vol. 2, Ungar, New York, 1966.

■